

This item is the archived peer-reviewed author-version of:

Waarom krijg ik fiscale controle? Naar meer transparantie bij de geautomatiseerde besluitvorming bij de fiscale overheid

Reference:

De Raedt Sylvie, Martens David, Brughmans Dieter.- Waarom krijg ik fiscale controle? Naar meer transparantie bij de geautomatiseerde besluitvorming bij de fiscale overheid

Tijdschrift voor fiscaal recht - ISSN 2031-8219 - 604(2021), p. 607-612

To cite this reference: <https://hdl.handle.net/10067/1809680151162165141>

Waarom krijg ik fiscale controle? Naar meer transparantie bij de geautomatiseerde besluitvorming door de fiscale overheid

I. Inleiding

Het is intussen algemeen bekend dat de federale fiscale administratie belastingplichtigen selecteert voor controle op basis van een datamining systeem dat centraal wordt georganiseerd. In een dergelijk systeem wordt door een algoritme op geautomatiseerde wijze de samenhang onderzocht tussen een groot aantal gegevens dat de fiscale administratie ter beschikking heeft, om er een wiskundig “model” mee te creëren, dat moet toelaten het risico op fraude bij belastingplichtigen te detecteren. Dit voorspellend model wordt dan toegepast op een deel of het geheel van de te controleren populatie. De belastingplichtigen die het meest overeenstemmen met het fraudeprofiel dat door het algoritme wordt bepaald, worden geselecteerd voor controle.

Dit systeem bestaat wellicht naar schatting minstens al zo'n 18 jaar¹, doch mist tot op vandaag transparantie, zowel ten aanzien van de burger in het algemeen, als ten aanzien van de individuele belastingplichtige die erdoor wordt getroffen. Op 6 april 2021 werd er een opvallend wetsvoorstel ingediend dat tracht tegemoet te komen aan een deel van het probleem.² Het beoogt meer transparantie over het gebruik van algoritmes door de overheid door een aanpassing van de wet openbaarheid bestuur van 1994. Nochtans zijn daarmee niet alle uitdagingen opgelost en blijft de vraag open hoever de transparantie moet reiken en hoe ze technisch moet worden ingevuld.

II. De mysterieuze kindertijd van de fiscale datamining

Hoewel fiscale datamining dus zeker al sinds 2003 bestaat, heeft het geduurd tot 2012 alvorens er een spoor over datamining terug te vinden was in wetgeving.

De eerste (10) jaren waren er over deze datamining alleen een paar parlementaire vragen, enkele vermeldingen in de jaarverslagen van de FOD Financiën en andere onrechtstreekse bronnen. Deze bronnen leverden weinig informatie op. Zo bleef het onduidelijk welke gegevens door de fiscale administratie werden aangewend voor datamining. Of wat de rol was van de individuele belastingambtenaar in de beslissing om een belastingplichtige die door het voorspellingsmodel was geselecteerd, ook effectief te controleren.

III. De tienerjaren: noch mossel noch vis

Met de wet van 3 augustus 2012 wilde de wetgever de verwerking van persoonsgegevens door de FOD Financiën in overeenstemming brengen met de wet verwerking persoonsgegevens van 8 december 1992, zijnde de Belgische dataproductiewet uit het pre-“GDPR3”-tijdperk. Op dat moment was er wel een richtlijn inzake de bescherming van de persoonsgegevens (richtlijn nr. 95/46) die de verwerker van persoonsgegevens een reeks verplichtingen oplegde. Een aantal daarvan hielden verband met het transparantiebeginsel dat vrij centraal staat in het persoonsgegevensbeschermingsrecht. Zowel de richtlijn nr. 95/46 als de GDPR beschouwen transparantie als een aspect van het “eerlijk” verwerken van persoonsgegevens (art. 6, 1., a) van de richtlijn nr. 95/464 en art. 5, 1., (a) GDPR). Het beginsel wordt geconcretiseerd in enerzijds de plicht

voor de verwerker van persoonsgegevens om de betrokkenen te informeren en anderzijds het recht van de betrokkene om deze informatie af te dwingen via o.m. een inzage-recht.

Je zou dus verwachten dat een wet die de verwerking van persoonsgegevens binnen de FOD Financiën in overeenstemming wil brengen met het persoonsgegevensbeschermingsrecht, transparantie zou creëren, ook ten aanzien van datamining als bijzondere vorm van verwerking van persoonsgegevens.

De richtlijn nr. 95/46 verbodt ook geautomatiseerde verwerkingen van persoonsgegevens als basis voor individuele besluiten (art. 15 richtlijn nr. 95/46). Dit verbod is gebaseerd op de gedachte dat beslissingen ten aanzien van een individu niet uitsluitend kunnen worden genomen op basis van geautomatiseerde processen, zonder tussenkomst van een natuurlijk persoon. Het moet wel gaan om een besluit waaraan rechtsgevolgen zijn verbonden voor dat individu of dat individu "in aanmerkelijke mate treft". Dat besluit moet bovendien worden genomen louter op grond van een geautomatiseerde gegevensverwerking, zonder enige substantiële menselijke tussenkomst. Er is sprake van een substantiële menselijke tussenkomst wanneer door toedoen van de mens ook andere elementen dan de resultaten van het geautomatiseerde beslissingsproces in overweging worden genomen bij de besluitvorming.⁵ Ten slotte moet het gaan over een beslissing waarbij van de betrokken persoon bepaalde aspecten van zijn persoonlijkheid worden geëvalueerd, zoals beroepsreputatie, kredietwaardigheid of betrouwbaarheid. Een beslissing om een bepaalde persoon te controleren omdat hij voldoet aan een bepaald fraudeprofiel is een dergelijke persoonlijkheidsevaluatie, die bovendien rechtsgevolgen meebrengt voor het individu (met name een reeks meewerkverplichtingen aan de controle), of dit individu minstens "in aanmerkelijke mate treft". Dit soort beslissingen was (en is) dus verboden als zij zonder substantiële menselijke tussenkomst worden gemaakt op basis van een geautomatiseerd proces.

De richtlijn nr. 95/46 liet wel toe dat de lidstaten uitzonderingen maken op dit verbod. Maar dan moet er wel een wet zijn die deze geautomatiseerde beslissingen toelaat én moeten er in deze wet maatregelen zijn omschreven ter bescherming van de gerechtvaardigde belangen van de betrokkene (art. 15, 2., b) van de richtlijn nr. 95/46). In de Belgische wet verwerking persoonsgegevens werd destijds verduidelijkt dat deze maatregelen er minstens in moeten bestaan dat aan de betrokkene de mogelijkheid wordt geboden om op nuttige wijze zijn standpunt naar voor te brengen (art. 12bis, tweede lid van de wet verwerking persoonsgegevens). Dit laatste is uiteraard maar mogelijk indien er transparantie is over het selectieproces naar het betrokken individu toe. De richtlijn voorziet ook dat wanneer er dan al sprake is van geautomatiseerde besluitvorming, de betrokkene steeds recht heeft op een "mededeling van de logica die ten grondslag ligt aan de automatische verwerking van hem betreffende gegevens" (art. 12, a) van de richtlijn nr. 95/46).

Van een wet die de verwerking van persoonsgegevens bij de FOD Financiën in overeenstemming wil brengen met het persoonsgegevensbeschermingsrecht zou je verwachten dat er wordt getracht een wettelijke basis te geven aan het geautomatiseerde selectieproces voor fiscale controles (in de mate dat er geen substantiële menselijke tussenkomst is voor deze selectie), en dat deze wettelijk grondslag gepaard gaat met maatregelen ter bescherming van de belangen van de betrokkenen, inbegrepen transparantie over dit automatisch selectieproces naar de betrokken individuen. De wet van 3 augustus 2012 stelt op dat vlak teleur. Hij draagt maar weinig bij aan de transparantie inzake fiscale datamining.

In een artikel 5 werd enkel bepaald dat de FOD Financiën de persoonsgegevens die zij heeft verzameld met het oog op het uitvoeren van zijn wettelijke opdrachten, kan samenvoegen met het oog op de oprichting van een zogenaamd "datawarehouse". Dit datawarehouse moet de FOD

Financiën – nog steeds volgens dit artikel 5 – in staat stellen “gerichte controles uit te voeren op basis van risico-indicatoren” en “analyses uit te voeren op relationele gegevens afkomstig van verschillende administraties en, of diensten van de FOD Financiën”. In § 2 van artikel 5 wordt daarnaast bepaald dat de verwerking, waar mogelijk, moet geschieden op gecodeerde persoonsgegevens en dat de decoding enkel geschiedt wanneer het risico bestaat van het plegen van een inbreuk op een wet of een reglementering waarvan de toepassing behoort tot de opdrachten van de FOD Financiën.

Een dergelijke bepaling kwalificeert niet echt als een duidelijke en uitdrukkelijke wet die als grondslag kan dienen van een geautomatiseerd beslissingsproces inzake selectie van belastingplichtigen voor fiscale controle. Alleen de verwijzing naar de decoding van de gegevens wijst impliciet wel op de toepassing van opgestelde fraudeprofielen op concrete belastingplichtigen ten aanzien van wie dan een geautomatiseerde beslissing tot controle wordt genomen. Of is er nog menselijke tussenkomst? De wet is hier niet duidelijk. Met wat goede wil kunnen we dus hoogstens stellen dat er een impliciete wettelijke grondslag is voor selectie van belastingplichtigen voor controle op basis van een voorspellingsmodel.

Ook wat betreft waarborgen voor een transparante verwerking van persoonsgegevens in het kader van deze datamining, stelt de wet teleur. Artikel 5 bepaalt wel dat elke categorie van gegevens die in het datawarehouse wordt opgenomen, onderworpen is aan een machtiging van het Sectoraal Comité voor de Federale Overheid (orgaan binnen de toenmalige Privacycommissie, dat haar machtigingen publiceert op de website). In 2015 heeft de FOD Financiën een lijst met categorieën persoonsgegevens aan dit Sectoraal Comité overgemaakt en heeft zij een machtiging bekomen om deze categorieën toe te voegen aan (of te behouden in) het datawarehouse (machtiging 2015/8). De lijst bevat vooral veel afkortingen en termen eigen aan de interne werking van de FOD Financiën (zie verwijzing naar lijsten met persoonsgegevens genaamd “TAXI”, “SITRAN”, “LOCO” en “STIRFRAUDE” e.d.m.) en is dus weinig toegankelijk voor het grote publiek.

Als het dan gaat over transparantie ten aanzien van de individuele belastingplichtige die erdoor wordt getroffen, zien we zelfs een tegenovergestelde beweging. Het recht op transparantie dat door de richtlijn wordt gegarandeerd (door onder meer een recht op inzage en een bijhorend recht op toelichting over de logica van de geautomatiseerde beslissing) wordt door de wet van 3 augustus 2012 ingeperkt (zie art. 11 van de wet van 3 augustus 2012, enigszins bijgestuurd door art. 96 van de wet van 17 juni 2013, na kritiek van rechtsleer en Privacycommissie⁶). Het inzagerecht, inbegrepen het recht op toelichting over de logica van de automatische beslissing, kan niet worden ingeroepen gedurende de periode tijdens dewelke de betrokkene het voorwerp uitmaakt van een controle, een onderzoek “of de daarmee verband houdende voorbereidende werkzaamheden” voor zover dit inzagerecht nadelig zou zijn voor de controle.

IV. De puberjaren: even teleurstellend

Na de inwerkingtreding van de GDPR (verordening nr. 2016/679) werd de wet van 3 augustus 2012 aangepast in 2018. De GDPR heeft het principieel verbod op geautomatiseerde besluitvorming van de richtlijn nr. 95/46 behouden en zelfs uitgebreid⁷ (art. 22 GDPR). Het transparantiebeginsel werd in de GDPR versterkt. Zo onder meer voorziet de GDPR dat de betrokkene in geval van geautomatiseerde besluitvorming inzage kan vragen in “de nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene”.

De aanpassing van de wet van 3 augustus 2012 door de wet van 5 september 2018 weerspiegelt dit evenwel niet. Op grond van het aangepaste artikel 5 kan de FOD Financiën nog steeds “gerichte controles uitvoeren op basis van risicoindicatoren” en “analyses uitvoeren op relationele gegevens afkomstig van verschillende administraties en/of diensten van de FOD Financiën”. Daar wordt nu aan toegevoegd dat de FOD Financiën de gegevens die ze in het kader van haar wettelijke opdrachten heeft verzameld, kan “samenvoegen in een datawarehouse waardoor er processen van datamining en datamatching uitgevoerd worden, met inbegrip van profilering in de zin van de artikel 4, 4) van de GDPR”. De begrippen “datawarehouse”, “datamining”, “datamatching” worden daarbij netjes in de wet gedefinieerd. Over de mogelijkheid om individuele beslissingen te nemen op basis van deze processen en de menselijke tussenkomst bij deze beslissingen, wordt evenwel nog steeds met geen woord gerept. Wel wordt opnieuw gesteld dat de verwerking, waar mogelijk, geschiedt op gepseudonimiseerde persoonsgegevens en dat de depseudonimisatie enkel geschiedt wanneer er een risico bestaat tot het plegen van een inbreuk op een wet of een reglementering waarvan de toepassing tot de opdrachten van de FOD Financiën behoort. We hebben vandaag dus nog steeds geen duidelijke en uitdrukkelijke wettelijke grondslag voor het nemen van geautomatiseerde beslissingen inzake de selectie van belastingplichtigen voor controle, hoogstens een impliciete.

De beperking van het inzagerecht, daaronder begrepen het recht om toelichting te krijgen omtrent de logica van de geautomatiseerde beslissing, wordt door de wetgever in 2018 gehandhaafd voor de duur van de controle.

Wat betreft transparantie omtrent de persoonsgegevens die worden gebruikt voor doeleinden van datamining zetten we zowaar zelfs een stap achteruit. Daar waar de vorige versie van artikel 5 nog bepaalde dat de toevoeging van elke categorie van gegevens die in het datawarehouse wordt opgenomen, onderworpen is aan een machtiging van het Sectoraal Comité voor de Federale Overheid, wordt nu bepaald dat enkel de integratie in het datawarehouse van persoonlijke gegevens geleverd door een derde partij onderworpen zijn aan een (te publiceren) beraadslaging van (een nieuw opgericht) Informatieveiligheidscomité.

V. Op naar volwassenheid: de internationale unanimitéit over de nood aan transparantie

Het belang van transparantie bij het nemen van geautomatiseerde beslissingen wordt reeds lange tijd sterk onderstreept door verschillende internationale organisaties. Tegenover de omvangrijke voordelen van een geautomatiseerd beslissingssysteem, dat aan efficiëntie wint door de inzet van zelflerende algoritmes (artificiële intelligentie), staan immers ook risico's van bijvoorbeeld ongewilde discriminatie. Een bekend en sprekend voorbeeld van hoe de goedbedoelde inzet van artificiële intelligentie bij een systeem van geautomatiseerde fraudedetectie volledig verkeerd kan uitpakken, is de Nederlandse SyRI-zaak (Systeem Risico Indicatie), helder toegelicht in TFR, afl. 585.

Dergelijke risico's onderbouwen de oproep van onder meer de Raad van Europa en de Europese Unie om bepaalde ethische standaarden in te bouwen in onder meer de overheidstoepassingen van geautomatiseerde besluitvorming gebaseerd op artificiële intelligentie. Voldoende transparantie vormt daarbij een belangrijke sleutel en draagt bovendien bij tot het vertrouwen in de inzet van artificiële intelligentie bij onder meer overheidsbeslissingen. Hierover kan onder meer worden verwezen naar de recente verklaring van het Comité van ministers van de Raad van Europa over “the risks of computer-assisted or artificial-intelligence-enabled decision making in the field of the social safety net” van 17 maart 2021 en de communicatie van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's van 21 april 2021 met als titel “Fostering a European approach to Artificial Intelligence” naar aanleiding van het

ontwerp van verordening met geharmoniseerde regels inzake artificiële intelligentie. Ook in dit ontwerp van verordening met geharmoniseerde regels inzake artificiële intelligentie van 21 april 2021 staat transparantie centraal. De transparantievereiste wordt bovendien concreter ingevuld en gedifferentieerd in functie van de risico's verbonden aan het gebruik van de AI-toepassing.

VI. Een herontdekking van de wet openbaarheid bestuur

Ook in het wetsvoorstel van 6 april 2021 dat ons opviel, wordt de nood aan transparantie bij het gebruik van algoritmes onderschreven en dit specifiek voor wat betreft het gebruik van algoritmes door de overheid. Het wetsvoorstel tracht deze transparantie in de praktijk te brengen via aanpassingen aan de wet openbaarheid bestuur.

Die benadering is op zich niet nieuw. In een parlementaire vraag van 2005 (toen de fiscale datamining wellicht nog in de kleutertijd zat) werd door mevrouw Pieters reeds pienter opgemerkt dat een belastingplichtige door het gebruik van fiscale datamining, niet langer in de mogelijkheid was om aan zijn belastingambtenaar te vragen hem de criteria mee te delen op grond waarvan hij werd geselecteerd voor controle. De lokale ambtenaar krijgt immers lijsten van geselecteerde belastingplichtigen toegestuurd en hijzelf, noch zijn leidinggevende hebben dus enig inzicht in de reden van selectie.⁸ Mevrouw Pieters zag daar meteen een probleem in voor de openbaarheid van bestuur, gegarandeerd door zowel de Grondwet (art. 32) als de wet openbaarheid bestuur van 1994.

De vraagstelster duidde ook meteen het belang van transparantie over het selectieproces. Een belastingplichtige moet toch immers kunnen nagaan of er geen sprake is van willekeur. Die vrees voor willekeur was toen ingegeven door de vaststelling dat – op dat moment – nog slechts 3% van de belastingplichtigen aan een grondige controle werden onderworpen. Deze riskeerden dan wel herhaalde controles waardoor het risico ontstaat dat deze belastingplichtigen zich persoonlijk geïsoleerd voelden.⁹

De minister van Financiën antwoordde toen evenwel dat “om evidente redenen er geen nadere inlichtingen en gegevens inzake de gebruikte risicofactoren en methodologie kunnen worden prijsgegeven”. De vraag om inzage te krijgen in het selectieproces zou volgens de minister op grond van artikel 6, § 1, 6° van de wet openbaarheid bestuur kunnen worden afgewezen omdat het belang van de openbaarheid niet opweegt tegen de bescherming van een federaal economisch of financieel belang (hier het fiscaal belang) van de overheid. Met het verlenen van inzage in het selectieproces zou een belastingplichtige immers volgens de minister in de toekomst belastingen kunnen ontwijken.

De toepasselijkheid van artikel 6, § 1, 6° werd door de minister verantwoord door te verwijzen naar een uitspraak van de Raad van State van 2 oktober 1997 (arrest nr. 68.609). Uit dit arrest valt evenwel in wezen iets anders te lezen dan de minister voorhoudt. De Raad van State oordeelde immers dat de wet openbaarheid bestuur weliswaar toelaat dat het recht op inzage in bepaalde omstandigheden wordt beperkt, maar dat de uitzonderingen strikt moeten worden geïnterpreteerd. Zo ook de uitzondering van artikel 6, § 1, 6° wet openbaarheid bestuur. Deze bepaling laat niet toe dat elke inzage die mogelijks repercussies zou kunnen hebben op de financiën van de staat, wordt geweigerd. De Raad van State oordeelde in die zin in het door de minister aangehaalde arrest van 2 oktober 1997, maar ook in een arrest van 18 juni 1997.¹⁰ In het eerste geval ging het over een vennootschap die inzage vroeg van het administratief dossier na de verzending van het bericht van wijziging. De administratie had deze geweigerd omdat de inzage schadelijk zou zijn voor de financiële belangen van de Staat. De Raad van State oordeelde evenwel dat dit in concreto niet was aangetoond.¹¹ In het tweede geval had de fiscale administratie een verzoek om inzage eveneens

afgewezen omwille van het risico voor de financiële belangen van de staat. De belastingplichtige had het verzoek ingediend nadat hij een vraag om inlichtingen had ontvangen omtrent zijn vermeend titularisschap van een rekening bij een verdachte wisselagent. De fiscale administratie argumenteerde dat de belastingplichtige geen legitiem belang had bij deze vraag. Volgens de administratie zou de inzage er enkel op gericht zijn om precies te weten over welke informatie de fiscale administratie beschikt, en vervolgens de belastingen te ontwijken door de elementen die al in het bezit van de administratie zijn proberen te verhullen. Ook hier wees de Raad van State de redenering van de fiscale administratie af bij gebrek aan concrete aanwijzingen van schade voor de staat. Ook in meer recente rechtspraak van de Raad van State zien we dezelfde redenering terug.¹²

VII. Biedt een wijziging van de wet openbaarheid bestuur een oplossing?

Het wetsvoorstel wil meer transparantie bekomen over de aanwending van algoritmes door de overheid op twee fronten.

Vooreerst worden een punt toegevoegd aan artikel 2 van de wet openbaarheid bestuur aangaande de zogenaamde “actieve” openbaarheid van bestuur. In artikel 2 worden een reeks elementen opgesomd waaromtrent de overheid openbaarheid moet verlenen, ook al wordt daar niet om verzocht door de burger. Het zijn openbaarheidsverplichtingen met als doel “een duidelijke en objectieve voorlichting van het publiek over het optreden van de federale administratieve overheden” (aanhef art. 2).

Met name verplicht het aangevulde artikel 2 de overheid – in het hier besproken wetsvoorstel – om online de regels bekend te maken die de belangrijkste algoritmische verwerkingen omschrijven waarvan de openbare besturen bij het vervullen van hun opdrachten gebruik maken, althans wanneer het gaat over algoritmes die geheel of gedeeltelijk de grondslag vormen voor individuele beslissingen. Dit voorstel doet denken aan het algoritmeregister dat bijvoorbeeld in Nederland bestaat voor de stad Amsterdam (www.algoritmeregister.amsterdam.nl/en/ai-register/).

Daarmee samenhangend worden de federale administratieve overheden ook verplicht de effectbeoordeling bekend te maken die ze in overeenstemming met artikel 35 van de GDPR moeten maken. De GDPR verplicht verwerkers van persoonsgegevens inderdaad om in welbepaalde gevallen voorafgaand aan de verwerking een beoordeling uit te voeren van het effect van de beoogde verwerking op de bescherming van de persoonsgegevens. Het gaat hierbij onder meer om de gevallen waarin er geautomatiseerde individuele beslissingen worden genomen waarbij er een persoonlijkheidsevaluatie wordt gemaakt van natuurlijke personen (zoals de mate waarin ze een frauderisicoprofiel hebben).

Daarnaast moeten de federale administratieve overheden, voor elk administratief document met een individuele draagwijdte, aan de persoon over wie een individuele beslissing wordt genomen die geheel of gedeeltelijk op een algoritmische grondslag wordt getroffen, op diens verzoek, op een bevattelijke wijze en mits geen afbreuk wordt gedaan aan bij wet beschermde geheimen, welbepaalde informatie verschaffen. Aangezien het hier gaat over transparantie op verzoek van de betrokkene, hadden we deze toevoeging verwacht bij de artikelen 4 en volgende van de wet openbaarheid bestuur aangaande de passieve openbaarheid. Niettemin wordt deze verplichting toegevoegd aan de verplichtingen van de federale administratieve overheden inzake hun actieve openbaarheid (art. 2).

De informatie die de federale administratieve overheid op verzoek moet verschaffen betreft (1) de mate waarin en de wijze waarop de algoritmische verwerking tot de besluitvorming heeft bijgedragen; (2) de verwerkte gegevens en de bronnen ervan; (3) de op de situatie van de belanghebbende toegepaste verwerkingsparameters en, in voorkomend geval, ook de afweging ervan en (4) de met de verwerking uitgevoerde verrichtingen.

VIII. Makkelijk gezegd dan gedaan: een “counterfactual” oplossing voor de transparantie-uitdaging van de overheid

Of dit wetsvoorstel het nu haalt of niet: over de nood aan transparantie bij het nemen van geautomatiseerde beslissingen, al dan niet ondersteund door artificiële intelligentie, lijkt er unanimititeit te bestaan.

Waar de discussie wellicht zal blijven steken is bij de uitvoering van dit beginsel. Het wetsvoorstel verplicht de overheid tot het bekendmaken van allerhande informatie, waarvan de vraag rijst wat er precies mee wordt bedoeld en hoe ze deze informatie kan verschaffen. Neem nu bijvoorbeeld de informatie over “de op de situatie van de belanghebbende toegepaste verwerkingsparameters en, in voorkomend geval, ook de afweging ervan”. Een algoritme bekijkt in potentieel massaal veel data welke kenmerken en vooral combinaties van kenmerken vaker voorkomen bij fraudeurs dan bij niet-fraudeurs. Deze kenmerken worden door het algoritme gewogen. Het algoritme kan ook zelflerend zijn zodat de beslissing van het geautomatiseerd proces om een belastingplichtige te selecteren als potentiële fraudeur ook door de dataminers niet meer kan worden verklaard. Sommige van dergelijke voorspellingsmodellen vergen immers tientallen of zelfs honderden pagina's om de formule waarmee fraudescores worden berekend, uit te schrijven. Hoe wordt de overheid dan verwacht deze verklaring te geven?

Ook het transparantiebeginsel van het persoonsgegevensbeschermingsrecht doet al jaren vragen rijzen omtrent de praktische toepassing ervan bij geautomatiseerde beslissingen. Hoe moet de overheid voldoende informatie verschaffen opdat de betrokkene inzicht zou hebben in de “logica die aan de grondslag ligt van de geautomatiseerde beslissing”. Juristen doen al jaren suggesties om een betere invulling te geven aan de te verstrekken informatie¹³, doch dit lost het probleem niet op van de geautomatiseerde beslissingen gebaseerd op zelflerende algoritmes die de overheid zelf niet kan verklaren. De toegenomen complexiteit van de voorspellingsmodellen heeft niet enkel in de fiscaliteit de nood aan transparantie aangescherpt. Veel van de huidige voorspellingsmodellen zijn zo complex en grootschalig in het aantal parameters dat toegang tot deze informatie weinig verduidelijking geeft. Vooral de befaamde “deep learning”-modellen, ondervinden een groot gebrek aan mogelijkheid tot uitleggen van beslissingen. Ironisch genoeg, is de oplossing voor dergelijke complexe algoritmes, het ontwikkelen van nieuwe algoritmes. Een heel nieuw domein binnen AI heeft plots veel aandacht gekregen: “Explainable Artificial Intelligence” (XAI). Eén van deze veelbelovende technieken zijn algoritmes die counterfactual verklaringen¹⁴ genereren. Een counterfactual verklaring zal voor een voorspelde beslissing aangeven wat er aan de data veranderd dient te worden, opdat de voorspelling zou veranderen. Bijvoorbeeld: “U wordt onderworpen aan een controle omdat uw jaarlijks inkomen 14.000 EUR is en u eigenaar bent van een woning met een kadastraal inkomen van 2.000 EUR. Indien uw inkomen 18.000 EUR zou zijn geweest als eigenaar van deze woning, dan had deze controle niet plaatsgevonden.”¹⁵ Deze verklaringen zijn verstaanbaar voor personen zonder enige kennis van datamining. Een belangrijk aspect van deze verklaring is dat ze specifiek zijn voor elke voorspelling. Een datamining algoritme neemt beslissingen aan de hand van complexe relaties tussen verschillende criteria. Dit kan ervoor zorgen dat de ene persoon met

een jaarlijks inkomen van 14.000 EUR en een woning met een kadastraal inkomen van 2.000 EUR wel gecontroleerd wordt en de andere niet, aangenomen dat ze wat betreft andere criteria verschillen. De verklaring bevat dus louter de informatie die ertoe geleid heeft dat de belastingplichtige in kwestie voor dat betreffende aanslagjaar geselecteerd werd. Een belangrijk extra voordeel is dat de verklaring ook geen inzicht geeft in het voorspellingsmodel zelf, waarmee de belastingplichtige dus ook geen informatie bekommt om de belastingen te ontwijken. Daarmee wordt gehoor gegeven aan het argument van potentieel economisch (fiscaal) verlies van de overheid bij het geven van uitleg over de beslissing. Daarnaast kunnen counterfactual verklaringen de samenwerking tussen belastingambtenaren en het voorspellingsmodel verbeteren. De ambtenaar krijgt inzicht in de logica van het model en hoeft dit niet meer blind te vertrouwen. Een foutieve voorspelling van het model kan mogelijks herkend worden aan de bijhorende verklaring. Verder zal de belastingambtenaar zijn werk efficiënter kunnen uitvoeren. Een counterfactual verklaring geeft aan welke informatie interessant is voor de ambtenaar en kan inzicht geven in het type van fraude dat het algoritme denkt te identificeren.

Ten slotte zijn counterfactual verklaringen ook voor dataminers interessant. Hoewel nieuwe technieken nog volop ontwikkeld en gevalideerd worden, zijn er reeds “open-source” technieken¹⁶ beschikbaar die op eender welk voorspellingsmodel kunnen toegepast worden. Dit geeft een dataminer volledige vrijheid in de keuze van zijn algoritme en verzekert ook dat counterfactual verklaringen relevant blijven bij nieuwe doorbraken in artificiële intelligentie. Daarenboven kunnen counterfactual verklaringen ongewenste vooroordelen in datamining modellen bloot leggen.¹⁷ Wanneer elementen zoals bijvoorbeeld bepaalde steden of bepaalde wijken in steden voorkomen in de verklaringen, is dit een signaal dat het model (ongewilde) discriminerende effecten heeft. Bij deze rode vlag kan een dataminer actie ondernemen en zijn model aanpassen om deze effecten te vermijden.

Hier staan wel enkele uitdagingen tegenover.¹⁸ Zo is het mogelijk dat er voor één voorspelling meerdere verklaringen mogelijk zijn. Kiezen dewelke dan daadwerkelijk getoond wordt aan de belastingplichtige geeft een nieuwe vorm van macht aan de fiscus, waarvoor bepaalde krijtlijnen uitgetekend dienen te worden. Daarnaast vereisen deze verklaringen nog meer algoritmes, namelijk degene die dergelijke verklaringen aanbieden. Duidelijke transparantie omtrent hoe die verklaringen worden gegenereerd en gekozen wordt een bijkomende eis.

IX. Conclusie

De nood aan transparantie is universeel binnen het domein van AI, zeker wanneer beslissingen over individuen worden genomen. De juridische vertaling van dit transparantiebeginsel blijkt een werk te zijn dat niet door juristen alleen kan worden ingevuld. Alle bestaande juridische instrumenten én de nieuwe poging van de indieners van het wetsvoorstel inzake algoritmes gebruikt door de overheid botsen op praktische vraagstukken van implementeerbaarheid. Alleen een samenwerking met andere disciplines zoals datamining en AI lijkt te kunnen leiden tot zinvolle oplossingen. Eén van deze oplossingen zijn de zogeheten counterfactual verklaringen, die de burger in staat stellen om een verklaring te bekomen voor de geautomatiseerde beslissingen die ten aanzien van hem is genomen, en de overheid tegelijkertijd behoedt voor economische schade die zou ontstaan door belastingontduiking.

David MARTENS20

Dieter BRUGHMANS21

Noten:

1. Zie M. SAINSTRAIN, TIC. Nouveaux standards transactionnels et fiscalité, Planbureau Working paper 15-03, augustus 2003, 41-42 (het hoofdstuk "La technologie au service de l'impôt").
2. Doc. 55-1904/001.
3. "GDPR" is de afkorting voor General Data Protection Regulation (verordening nr. 2016/679 inzake de bescherming van de persoonsgegevens). De afkorting van de Nederlandse benaming: AVG of Algemene Verordening Gegevensbescherming lijkt het in de geschreven taal niet te halen ten voordele van de GDPR.
4. De stelling dat de vereiste van de eerlijke verwerking in wezen verwijst naar de vereiste van een transparante verwerking, blijkt onder meer uit het arrest BARA van het Hof van Justitie (HvJ 1 oktober 2015, C-201/14, BARA , randnrs. 31
5. D. DE BOT, Verwerking van persoonsgegevens, in de reeks "Recht en praktijk", Antwerpen, Kluwer, 2001, 220, randnr. 295.
6. Zelfs voor de totstandkoming van de wet werd er kritiek geformuleerd door de Commissie voor de bescherming van de persoonlijke levenssfeer in advies nr. 11/ 2012 van de Commissie voor de bescherming van de persoonlijke levenssfeer van 11 april 2012 omtrent het voorontwerp van de wet betreffende de verwerking van persoonsgegevens door de FOD Financiën in het kader van zijn bijzondere opdrachten; na de wet: S. DE RAEDT, "Beperking op privacyrechten bij oprichting superdatabank", Fisc.Act. 2012, nr. 30, 1-5; S. DE RAEDT, "De uitschakeling van de privacyrechten tijdens de controle: de wet openbaarheid bestuur is niet steeds de redding", Fisc.Act. 2012, nr. 33, 1-4. Er was ook een tussenkomst van de voorzitter van de Commissie voor de bescherming van de persoonlijke levenssfeer naar aanleiding van de publicatie van de wet van 3 augustus 2012 bij de bevoegde minister (zie hierover verslag namens de Commissie voor Financiën en Begroting van 15 mei 2013, Parl.St. Kamer 2012-13, nr. 53-756/005, 62; advies nr. 32/2012 van de Commissie voor de bescherming van de persoonlijke levenssfeer van 17 oktober 2012 omtrent het amendement bij het wetsontwerp houdende fiscale en financiële bepalingen).
7. Vandaag heeft eenieder op grond van art. 22 GDPR "het recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft". Er is dus geen beperking tot beslissingen die een persoonlijkheidsevaluatie inhouden. Uitzonderingen blijven mogelijk, onder meer wanneer er een Unierechtelijke of lidstaatrechtelijke bepaling is die de automatische besluitvorming toelaat én passende maatregelen voorschrijft ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene (art. 22, 2., b) van de verordening nr. 2016/679). De lidstaten moeten dus zelf invulling geven aan deze mogelijkheid om geautomatiseerde besluitvorming toe te laten.
8. Parl.Vr. nr. 608 van mevrouw Trees Pieters van 20 januari 2005.
9. Parl.Vr. nr. 608 van mevrouw Trees Pieters van 20 januari 2005.

10. RvS 18 juni 1997, nr. 66.860, Matagne.
11. Zie ook RvS 9 februari 1998, nr. 71.688, Brussels Airport Terminal Company NV.
12. RvS 2 juni 2020, nr. 247.694, X.
13. A. SELBST en J. POWLE, "Meaningful information and the right to explanation", *International data Privacy law*, 2017, vol. 7, nr. 4, 233-242 .
14. D. MARTENS en F. PROVOST, "Explaining Data-Driven Document Classifications", *MIS Quarterly* 38.1, 2014, 73-100.
15. Dit is een fictief voorbeeld.
16. Zie bv.: D. BRUGHMANS en D. MARTENS, "NICE: An Algorithm for Nearest Instance Counterfactual Explanations", arXiv preprint arXiv:2104.07411, 2021.
17. S. WACHTER, B. MITTELSTADT en C. RUSSELL, "Counterfactual explanations without opening the blackbox: Automated decisions and the GDPR", *Harv. JL & Tech.*31, 2017, 841.
18. S. BAROCAS, A. SELBST en M. RAGHAVAN., "The hidden assumptions behind counterfactual explanations and principal reason", *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 2020, p. 80-89.
19. Research manager UAntwerpen, Digitax onderzoeksexcellentiecentrum, advocaat.
20. Hoogleraar UAntwerpen, Digitax onderzoeksexcellentiecentrum.
21. Onderzoeker UAntwerpen, Digitax onderzoeksexcellentiecentrum