Vrij Gesteld

171.

In "Vrij Gesteld" geeft een lid van de redactie of een gastauteur zijn eigen mening, kritiek of commentaar op een fiscaal item dat hem of haar is opgevallen. Er is ook ruimte voor kritiek hierop.

Fiscale algoritmen, profilering en het recht op privéleven

I. Inleiding

Nieuwe technologieën dringen door tot in alle hoeken van onze samenleving. Ook de belastingadministraties maken steeds vaker gebruik van een brede waaier van digitale middelen en data-analyse met het oog op een betere naleving van de belastingwetgeving[1]. Een studie van de OESO toont dat meer dan 35 belastingadministraties *data scientists* in dienst hebben om door middel van data-analyse te voorspellen welke belastingplichtigen een verhoogde kans op frauderen vertonen en dus bij voorkeur gecontroleerd moeten worden[2]. De data die hiervoor gebruikt worden blijven toenemen. Zo kan in Frankrijk de belastingadministratie sinds kort data van publiek beschikbare digitale bronnen (zoals sociale netwerken) integreren zijn data-analyse[3]. Ook in België wordt data-analyse gebruikt en kan hiertoe data van de verschillende administraties gekoppeld worden[4].

Het gebruik van data-analyse en *big data* brengt ook uitdagingen met zich mee. Zo moeten de fundamentele rechten van de belastingplichtigen gerespecteerd worden, inclusief het recht op privéleven. Dat deze rechten geen holle woorden zijn ondervond de Nederlandse staatssecretaris voor Financiën. Hij moest zijn ontslag indienen naar aanleiding van de *SyRI*-zaak. De Nederlandse belastingadministratie had met onethische data-analyse en etnische profilering het recht op privéleven en het recht op non-discriminatie van belastingplichtigen geschonden. Mensen met een niet-Nederlandse nationaliteit uit achterstandswijken bleken veel meer kans te hebben dat hun aangifte werd gecontroleerd. Deze zaak kreeg heel wat media-aandacht, zowel in Nederland[5] als in het buitenland[6], en toont dat de fundamentele rechten van de belastingplichtige meer aandacht behoeven.

II. SyRI

Waarover gaat de *SyRI*-zaak? SyRI staat voor "Systeem Risico Indicatie" en werd door de Nederlandse overheid ingevoerd als instrument tegen fraude op het terrein van uitkeringen, toeslagen en belastingen[7]. SyRI is een predictief model geleerd met behulp van data-analyse algoritmen en profilering om fraudeurs op te sporen. De staatssecretaris kon het instrument inzetten na een uitgebreide, bij wet bepaalde procedure en op verzoek van bepaalde overheidsinstanties, namelijk de belastingdienst, de gemeenten, het Uitvoeringsinstituut Werknemersverzekeringen, de Sociale Verzekeringsbank, de Immigratie- en Naturalisatiedienst en toezichthouders, zoals de Inspectie Sociale Zaken en Werkgelegenheid.

De data die binnen SyRI werden gebruikt, was heel uitgebreid aangezien alle hierboven genoemde overheidsinstanties een samenwerkingsverband konden aangaan om hun gegevens uit te wisselen met het oog op de data-analyse. De data omvatten bijvoorbeeld fiscale gegevens, arbeidsgegevens, eerder opgelegde bestuurlijke boetes, gegevens over het bezit en het gebruik van onroerende en roerende goederen, handelsgegevens, huisvestingsgegevens, geboortedatum, geslacht, inburgeringsgegevens, onderwijsgegevens, pensioengegevens, schuldenlastgegevens, uitkerings-, toeslagen- en subsidiegegevens en zorgverzekeringsgegevens[8].

Binnen predictieve modellen zoals SyRI worden de aldus beschikbare data gestructureerd en gekoppeld, om vervolgens geanalyseerd te worden. Eerst wordt een risicoprofiel opgesteld met historische trainingdata. Van deze data is geweten in hoeverre er sprake is van fraude. Een algoritme bekijkt in deze data welke combinaties van karakteristieken vaker voorkomen bij fraudeurs dan bij niet-fraudeurs. Op basis daarvan wordt een score berekend; voor elke persoon in de

1. Intra-European Organisation of Tax Administrations (IOTA), *Impact of Digitalisation on the Transformation of Tax Administrations*, 2018, www.iota-tax.org/sites/default/files/publications/public_files/impact-of-digitalisation-online-final.pdf.
2. www.oecd.org/tax/use-of-digital-technologies-set-to-increase-tax-compliance.htm.
3. FR: Conseil constitutionel, Besl. n° 2019-796 DC van 27 december 2019, overw. 75.
4. Wet van 3 augustus 2012 houdende bepalingen betreffende de verwerking van persoonsgegevens door de Federale Overheidsdienst Financiën in het kader van zijn opdrachten (*BS* 24 augustus 2012); S. De Raedt, *De draagwijdte van het recht op privéleven bij de informatie-inzameling door de fiscale administratie*, Gent, Larcier, 2017, 194; S. De Raedt, "The Impact of the GDPR for the Belgian Tax Authorities", *RDTI* 2018, 66-67, 129-143.
5. Bv. www.nos.nl/artikel/2321704-anti-fraudesysteem-syri-moet-van-tafel-overheid-maakt-inbreuk-op-priveleven.html; www.nos.nl/nieuwsuur/artikel/2307132-vn-rapporteur-zeer-bezorgd-over-nederlands-opsporingssysteem-voor-uitkeringsfraude.html en www.nos.nl/artikel/2326828-donner-meer-slachtoffers-kinderopvangaffaire-moeten-worden-gecompenseerd.html.
6. Ook in België, zie www.standaard.be/cnt/dmf20200707_97637135. UK: www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules; www.techcrunch.com/2020/02/06/blackbox-welfare-fraud-detection-system-breaches-human-rights-dutch-court-rules/.
7. Art. 8 wet SUWI.
8. Art. 5, a., 1., derde lid besluit SUWI.

trainingdata wordt nagegaan hoeveel van deze factoren aanwezig zijn. De exacte weging van deze factoren en het bepalen vanaf welk punt iemand als mogelijke fraudeur wordt aangeduid, gebeurt op basis van deze trainingdata. Typisch wordt hier gebruik gemaakt van optimalisatiealgoritmen die als het ware kleine draaitjes geven aan de knoppen (de weging van de factoren) en bekijken wanneer het model een betere respons geeft in de zin dat de risico score meer consistent wordt met de gekende situatie (al dan niet fraude) in de trainingdata. Het model beweegt langzaam maar zeker naar een lokaal optimale situatie.

Zo vindt het algoritme correlaties (bv. tussen "fraudeur" en "plotse toename van het banktegoed"[9]). De reden waarom er een correlatie is, blijft echter onduidelijk. Vervolgens kan het aldus "getrainde" algoritme worden ingezet om de risico-indicatoren en scores toe te passen op nieuwe data. De *SyRI*-wetgeving voorzag ook dat het risicomodel op basis van een evaluatie kon worden aangepast en dat nieuwe risicomodellen met nieuwe indicatoren konden worden ontwikkeld. Het risicomodel en de risico-indicatoren werden niet openbaar gemaakt. Fraudeurs zouden hun gedrag daar immers op kunnen afstemmen.

In de praktijk gaf SyRI meer risicomeldingen voor welbepaalde (probleem)wijken en mensen met niet-Nederlandse nationaliteit. Algoritmen kunnen inderdaad (ongewilde) discriminerende effecten hebben. Deze discriminerende effecten kunnen het gevolg zijn van historische bias die in de data aanwezig is; mogelijk werden mensen uit bepaalde wijken in het verleden vaker geviseerd bij controles wat resulteert in een hoger aantal positieve gevallen in deze wijken. Het algoritme wordt dan mogelijk misleid door de oververtegenwoordiging van deze wijken in de data. Bovendien kan een systeem als SyRI dit effect in de toekomst nog verder versterken doordat meer controles in het verleden leiden tot nog meer controles in de toekomst, wat de representativiteit van de data verder ondermijnt. Zonder de nodige transparantie in de ontwikkeling van risicomodellen zoals SyRI is het echter onmogelijk om te garanderen dat met deze zelf-versterkende effecten voldoende rekening wordt gehouden.

Aangezien de algoritmen alleen naar correlaties zoeken, kan daarnaast bias ook ongewild ontstaan als louter toevallige correlaties rechtstreeks worden gebruikt bij predictieve modellen. Stel dat in een stad een bepaald type wagen erg populair is bij drugsdealers. Algoritmen zullen dit verband oppikken en vervolgens het bezit van dit type wagen correleren met een verhoogde kans op criminele activiteiten. Het gevolg is dat alle eigenaars van dit type wagen systematisch en disproportioneel vaak foutief als hoog-risico zullen worden gelabeld. Als met een dergelijke bias onvoldoende rekening wordt gehouden, bestaat het risico dat ook bijvoorbeeld een lagere sociaaleconomische status of een immigratieachtergrond foutief meegenomen worden in een veralgemening.

De resultaten van SyRI brachten een aantal organisaties, waaronder het Nederlands Juristen Comité voor de Mensenrechten, en twee burgers ertoe een procedure aan te spannen tegen de Nederlandse Staat. Op 5 februari 2020 oordeelde de rechtbank van Den Haag[10] dat hoewel op algoritme gebaseerde data-analyse moet worden benut in de voorkoming en bestrijding van fraude, in dit geval SyRI in strijd is met het door artikel 8, 2. EVRM gewaarborgde recht op privéleven. Volgens de rechtbank is er geen redelijke verhouding tussen het maatschappelijk belang van SyRI en de inbreuk op het privéleven.

III. Recht op privéleven

In de eerste plaats geeft de rechtbank aan dat ze wel voorstander is van nieuwe technologieën en op algoritmen gebaseerde data-analyse. De rechtbank deelt de opvatting van de staat dat digitale mogelijkheden om bestanden te koppelen en met behulp van algoritmen data te analyseren, mogelijkheden bieden fraude te voorkomen en te bestrijden. De rechtbank vindt ook dat risicomodellen die fraude willen voorspellen, in het belang van het economisch welzijn van het land zijn en daarmee een noodzakelijk en legitiem doel dienen[11].

Niettemin vindt de rechtbank dat de manier waarop SyRI concreet vorm gekregen heeft onvoldoende waarborgen biedt voor het recht op privéleven. Geïnspireerd door het Europees Hof voor de Rechten van de Mens[12] stelt de rechtbank dat Nederland bij de toepassing van nieuwe technologieën een bijzondere verantwoordelijkheid heeft. Deze technologieën laten immers een intensiever gebruik van persoonsgegevens toe en hun bescherming moet daarom worden versterkt. Dergelijke bescherming draagt volgens de rechtbank bij tot het vertrouwen van de burger in de overheid. Dit is belangrijk want zonder vertrouwen zullen burgers minder snel gegevens willen verstrekken of zal daarvoor minder draagvlak bestaan[13]. Deze verantwoordelijkheid voor de bescherming van persoonsgegevens vindt een juridische weerslag in artikel 8 EVRM dat het recht op respect voor het privéleven waarborgt. Dit recht behelst ook het recht op bescherming van persoonsgegevens[14].

Iedereen erkent dat SyRI een inmenging is in het recht op privéleven. De hamvraag is evenwel of deze inmenging kan worden verantwoord. Artikel 8, 2. van het EVRM voorziet dat hiertoe de inmenging (1) bij wet voorzien moet zijn en moet beantwoorden (2) aan een noodzakelijkheidstoets, nl. de inmenging moet in een democratische samenleving noodzakelijk 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

9. NL: *Kamerstukken II*, 2012/13, 33579, 3.
10. NL: Rb. Den Haag 5 februari 2020, nr. C-09-550982-HA ZA 18-388, zie www.uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:865.
11. Overw. 6.4.
12. EHRM 4 december 2008, nrs. 30562/04 en 30566/04, *S. en Marper / Het Verenigd Koninkrijk*, punt 112: "*The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.*"
13. Overw. 6.5. en 6.6.
14. Zie onder meer EHRM 4 december 2008, nrs. 30562/04 en 30566/04, *S. en Marper / Het Verenigd Koninkrijk*, punt 66.

bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen, en (3) aan een proportionaliteitstoets. Volgens de rechtbank voldoet SyRI niet aan deze laatste toets.

De rechtbank laat zich voor de interpretatie van de proportionaliteitstoets van artikel 8, 2. EVRM leiden door het Unierecht. De rechtbank merkt op dat persoonsgegevens ook worden beschermd door artikel 8 van het handvest van de Grondrechten van de Europese Unie en door de algemene verordening gegevensbescherming ("AVG")[15]. De AVG concretiseert de bescherming van de verwerking van persoonsgegevens in een aantal specifiekere beginselen, zoals het transparantiebeginsel, het doelbeginsel, het beginsel van dataminimalisatie en juistheid (art. 5 AVG). De rechtbank overweegt dat de minimumbescherming van het recht op bescherming van het privéleven conform artikel 8 EVRM niet minder ver gaat dan de bescherming in de AVG. Bijgevolg kan artikel 8, 2. EVRM volgens de rechtbank geïnterpreteerd worden met behulp van de verordening[16].

IV. Transparantie over profilering

De AVG vereist in beginsel dat de betrokkene informatie krijgt over de verwerking van zijn persoonsgegevens[17] en het recht heeft om inzage te verkrijgen van die persoonsgegevens alsook informatie over onder meer de identiteit van de verwerkingsverantwoordelijke en de verwerkingsdoeleinden[18]. Dit omvat ook informatie over het bestaan van profilering en het verkrijgen van "nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene"[19]. Mensen hebben ook het recht bezwaar te maken tegen profilering[20] en niet onderworpen te worden aan een zogenaamd "uitsluitend op geautomatiseerde verwerking gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft"[21]. Deze rechten op informatie, inzage of verzet kunnen begrepen worden in de context van bijvoorbeeld profilering door een verzekeringsmaatschappij om de tarieven van een autoverzekering te bepalen, of door een bankinstelling om te bepalen welke financiële producten worden aangeboden aan welbepaalde cliënten.

Bij de verwerking van persoonsgegevens ten behoeve van zaken die het algemene belang raken, zoals de strijd tegen belastingfraude, gelden verscheidene uitzonderingen op deze rechten. Zo kan een belastingadministratie met het oog op fraudebestrijding aan profilering doen zonder dat de betrokkene zich daartegen kan verzetten, in de mate dat de profilering is toegestaan door een (Unierechtelijke of) lidstaatsrechtelijke bepaling[22]. Ook dan echter moet deze bepaling passende maatregelen voorzien ter bescherming van de rechten en vrijheden en de gerechtvaardigde belangen van de betrokkene[23].

In de zaak *SyRI* oordeelde de rechtbank dat er sprake is van zogenaamde "besluitvorming op basis van geautomatiseerde verwerking van persoonsgegevens waaraan voor de betrokkenen rechtsgevolgen zijn verbonden of die de betrokkenen in aanmerkelijke mate treffen". De rechtbank leidt dit onder meer af uit het feit dat een risicomelding over een persoon gedurende 2 jaar kon worden opgenomen in een register, en dat risicomelding volgens de wetgeving ook aan de politie mocht meegedeeld worden[24].

Deze geautomatiseerde besluitvorming was dan wel geregeld door de Nederlandse wetgeving, maar de passende maatregelen ter bescherming van de rechten en vrijheden van de betrokkenen ontbraken volgens de rechtbank. Volgens de rechtbank werd vooral het transparantiebeginsel door de wetgever onvoldoende in acht genomen. De overwegingen bij de AVG verduidelijken dat ook bij profilering en dergelijke geautomatiseerde besluiten informatie moet worden verstrekt aan de betrokkenen[25]. De rechtbank stelt echter vast dat SiRY geen informatie gaf over welke objectieve feitelijke gegevens kunnen leiden tot een risicomelding. In de wetgeschiedenis werden weliswaar een aantal voorbeelden gegeven, zoals "iemand bij wie het banktegoed in een jaar explosief stijgt"[26], maar dat volstaat volgens de rechtbank niet. Verder werd geen informatie gegeven over de werking van het risicomodel, bijvoorbeeld het type algoritme dat werd gebruikt[27]. Terwijl wel een bepaalde menselijke controle op de risicomelding was voorzien, vond de rechtbank het ook problematisch dat de manier waarop de definitieve risicoselectie tot stand kwam niet openbaar werd gemaakt[28].

Welke informatie vrijgegeven moet worden, is niet duidelijk en voorwerp van discussie. Volgens Working Party 29 eist de AVG niet dat het algoritme volledig vrijgegeven wordt[29]. Bovendien moet niet de specifieke beslissing verduidelijkt wor-

15. Verordening (EU) nr. 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn nr. 95/46/EG (algemene verordening gegevensbescherming) (*OJ* L. 119, 4 mei 2016, p. 1-88).
16. Overw. 6.41.
17. De informatieplicht van de betrokkene ligt eerder in art. 13 en 24 AVG; art. 12 is eerder de algemene bepaling die van toepassing is op alle transparantierechten van de betrokkene (niet alleen de informatieplicht, maar ook het inzagerecht...) Art. 12, 1. AVG.
18. Art. 15 AVG; S. De Raedt, "Het inzagerecht op grond van de GDPR in *fiscalibus*: blij met een dode mus?", *TFR*, 2019/10, nr. 562, 475-477.
19. Art. 13, 2., f), art. 14, 2., g) en art. 15, 1., h) AVG.
20. Art. 21, 1. AVG. Dit bezwaarrecht zit m.i. eerder in 22, 1. AVG.
21. Art. 22, 1. AVG.
22. Art. 22, 2., b) AVG.
23. Art. 14, 5., c) en art. 22, 1., b) AVG.
24. Overw. 6.36 en 6.59.
25. Overw. 71.
26. Overw. 6.87.
27. Overw. 6.89.
28. Overw. 6.94.
29. Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 2017, p. 25.

den, maar wel de "*more general form of oversight*"[30]. Van belang is dat de betrokkene nuttige informatie krijgt over de onderliggende logica van de verwerking (art. 13, 14 en 15 AVG)[31]. Deze informatie moet het voor de betrokkene mogelijk maken om de beslissing te begrijpen[32]. Volgens sommige auteurs is deze interpretatie echter te eng[33].

Hier stelt zich bovendien het zogenaamde *black-box*-probleem. De werking van predictieve modellen zoals SiRY laat niet altijd toe om te begrijpen hoe het algoritme de risico-indicatoren en de scores bepaalt[34]. Zoals hierboven aangehaald zorgen optimalisatiealgoritmen ervoor dat het model langzaam maar zeker naar een lokaal optimale situatie beweegt. Zij passen de scores van de risico-indicatoren stelselmatig aan om ervoor te zorgen dat hun predictieve werking zo consistent mogelijk wordt met de trainingdata. Hoe dit gebeurt is soms moeilijk verklaarbaar. De manieren waarop een model de factoren combineert bepaalt in grote mate de verklaarbaarheid en de complexiteit van deze modellen. Zogenaamde *deep learning*-modellen maken hierbij gebruik van complexe niet-lineaire lagen van berekeningen die na elkaar worden uitgevoerd en die geïnspireerd zijn op de werking van biologische neuronen. "*Deep*" duidt hier op het aantal lagen dat op elkaar gestapeld is. Deze modellen bestaan vaak uit miljoenen kleine rekenstappen die uiteindelijk resulteren in een voorspelling. Net zoals het onduidelijk is waarom de exacte configuratie van neuronen in het menselijke brein in staat is om een bal van een fiets te onderscheiden is het in deze "*deep neural networks*" volledig opaak hoe een beslissing wordt gegenereerd. In de zaak *SyRI* was het onduidelijk of het model als *deep learning* kwalificeerde[35]. Het is wel duidelijk dat de rechtbank vindt dat dergelijke modellen met nog meer omzichtigheid gehanteerd moeten worden, omwille van hun complexiteit. Ook in de *SyRI*-zaak vond de rechtbank dat de uitleg van de staat onvoldoende was om bijvoorbeeld met een eenvoudige beslissingsboom te controleren hoe de risicomeldingen van SyRI tot stand kwamen. Om dit *black-box*-probleem op te lossen, wordt artificiële intelligentie ontwikkeld die de beslissingen van predictieve modellen beoogt te verklaren[36]. Dergelijke modellen kunnen ook bijdragen tot een betere rechtsbescherming.

In de zaak *SyRI* tilt de rechtbank heel zwaar aan dit gebrek aan transparantie, mede omdat het systeem etnische profilering en discriminatie in de hand werkte. Zelfs een rapporteur van de Verenigde Naties had de rechtbank laten weten dat met de inzet van SyRI volgens haar sprake was van een discriminerend en stigmatiserend effect. Hierboven werd toegelicht op welke manier een dergelijke bias inderdaad in een model kan sluipen. Om dit probleem op te lossen en algoritmen binnen ethische grenzen te houden, worden technieken ontwikkeld die ongewenste bias van de modellen expliciet in rekening brengen tijdens het leerproces van het algoritme[37]. Ook de overwegingen bij de AVG verduidelijken dat de proportionaliteitstoets impliceert dat de verwerkingsverantwoordelijke passende wiskundige en statistische procedures hanteert, en geschikte technische en organisatorische maatregelen treft om het risico op fouten te minimaliseren[38]. De wetgever zou de toepassing van dergelijke technieken wettelijk kunnen verplichten met het oog op de rechtsbescherming van de belastingplichtige.

V. Wat nu?

De (nieuwe) Nederlandse staatssecretaris voor Financiën liet weten geen hoger beroep in te dienen tegen deze uitspraak van de rechtbank van Den Haag. De Nederlandse belastingadministratie onderzoekt nu binnen welke grenzen het systeem met algoritmen wel gebruikt kan worden[39]. De zaak *SiRY* illustreert dat het wetgevend kader voor het gebruik van data-analyse ontoereikend is. Ook in België bestaat er een wettelijk kader dat de FOD Financiën de mogelijkheid biedt om, teneinde 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, een zogenaamd "datawarehouse" op te richten dat toelaat processen van datamining en data-matching uit te voeren, met inbegrip van profilering[40]. De Belgische wetgeving voorziet in ieder geval niet in specifieke maatregelen om aan de transparantieverplichtingen van de AVG te voldoen. De vraag rijst evenwel hoever deze transparantie moet gaan. Op dat vlak is er dringend nood aan meer duidelijkheid. Steeds meer belastingadministraties gebruiken immers deze technologie, die mits een legitiem gebruik talrijke voordelen heeft.

Toon Calders[41]
Anne Van de Vijver[42]

30. *Idem*.
31. S. De Raedt, "The Impact of the GDPR for the Belgian Tax Authorities", *RDTI* 2018, 66-67 en 129-143.
32. Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 2017, p. 25.
33. M. Veale en L. Edwards, "Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling", *Computer Law & Security Review* 2018, 34(2), (398) 399-400.
34. The Norwegian Data Protection Authority, *Artificial intelligence and privacy*, 2018, 12.
35. Overw. 6.48 tot 6.51.
36. Bv. T. Vermeire en D. Martens, "Explainable Image Classification with Evidence Counterfactual", www.arxiv.org/abs/2004.07511.
37. Bv. T. Calders, "Fairness-aware data mining", *16e Journées Francophones Extraction et Gestion des Connaissances, EGC 2016*, 2016, Reims, France.
38. Overw. 71.
39. Zie www.rijksoverheid.nl/ministeries/ministerie-van-sociale-zaken-en-werkgelegenheid/documenten/kamerstukken/2020/04/23/kamerbrief-naar-aanleiding-van-vonnis-rechter-inzake-syri.
40. Art. 5, § 1, eerste lid van de wet van 3 augustus 2012.
41. Prof. computerwetenschappen Universiteit Antwerpen, Faculteit Wetenschappen, Departement Computerwetenschappen, Antwerp Tax Academy, DigiTax.
42. Prof. fiscaal recht Universiteit Antwerpen, Faculteit Rechten, Onderzoeksgroep Onderneming en Recht, Antwerp Tax Academy, DigiTax.