

Artikel

Risico's op witwassen via virtuele valuta in Nederland geregeld?

Mr. L.M. de Zeeuw en drs. R. Bastiaan RA*

1. Inleiding

12 Door het Europees Parlement en de Raad van de Europese Unie (EU) is op 19 april respectievelijk 14 mei 2018 wetgeving aangenomen om witwassen en terrorismefinanciering te voorkomen ten aanzien van wisselplatforms voor virtuele valuta¹ en aanbieders van bewaarportemonnees. Deze wetgeving is een wijziging van de vierde anti-witwasrichtlijn, ook wel de vijfde anti-witwasrichtlijn genoemd.² De afspraken maken deel uit van een grotere set aan maatregelen van de EU tegen financiële criminaliteit en belastingontduiking. Recent is het Nederlandse wetsvoorstel ter implementatie van de vijfde anti-witwasrichtlijn (hierna: implementatiewet) voorgelegd ter consultatie waarop gereageerd kon worden tot 15 januari jl.³ De meeste bepalingen in

de vijfde anti-witwasrichtlijn dienen op 10 januari 2020 in nationale wet- en regelgeving geïmplementeerd te zijn.

Virtuele valuta gaan gepaard met een hoge mate van anonimiteit en maken het mogelijk om naamloze transacties uit te voeren. De anonimiteit van virtuele valuta maakt het ook mogelijk ze te misbruiken voor criminele doeleinden, zoals witwassen. In dit artikel wordt besproken of de risico's op witwassen via virtuele valuta in Nederland voldoende adequaat kunnen worden beheerst na implementatie van de vijfde anti-witwasrichtlijn in nationale wetgeving. De beantwoording van deze vraag zal mede worden gezien in het licht van de nationale risicoanalyse witwassen (hierna: NRA), waarin het risico op witwassen via virtuele valuta in Nederland als relatief groot wordt aangeduid.⁴

* Mr. L.M. de Zeeuw is accountmanager witwasbestrijding bij het Anti Money Laundering Centre (AMLC), FIOD. Drs. R. Bastiaan RA is projectleider witwasbestrijding bij het Anti Money Laundering Centre (AMLC), FIOD. Dit artikel is op persoonlijke titel geschreven.

1. In dit artikel wordt bij de term virtuele valuta met name gekeken naar cryptocurrency's waarbij gebruik wordt gemaakt van de blockchain-technologie.
2. Richtlijn 2018/843/EG van het Europees Parlement en de Raad van 30 mei 2018 als aanvulling op de richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van Richtlijn 2009/138/EG en 2013/36/EU.
3. Wijziging van de Wet ter voorkoming van witwassen en financieren van terrorisme en de Wet toezicht trustkantoren 2018 in verband met de implementatie van richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van de richtlijn 2009/138/EG van het Europees Parlement en de Raad en tot

wijziging van richtlijn (EU) 2013/36 van het Europees Parlement en de Raad (Implementatiewet wijziging vierde anti-witwasrichtlijn).

4. H.C.J. van der Veen & L.F. Heuts, *National Risk Assessment Witwassen* (Cahier-2017-13), Den Haag: WODC 2017.

Virtuele valuta, zoals *cryptocurrency's*, kunnen worden omschreven als een betaalmiddel dat niet wordt gecontroleerd en niet is uitgegeven of gegarandeerd door een centrale bank.

Bekende voorbeelden van *cryptocurrency's* zijn onder meer bitcoin, ethereum, ripple, monero, litecoin en dash.

Wisselplatforms (*digital asset exchanges*) zijn websites waar je virtuele valuta kunt kopen, verkopen of kunt uitwisselen tegen andere virtuele valuta of regulier geld.

Aanbieders van bewaarportemonnees (*custodian wallet providers*) houden de virtuele valuta voor haar klant en dragen doorgaans zorg voor de beveiliging van tegoeden en transacties.

In paragraaf 2 van dit artikel wordt de NRA voor Nederland behandeld in relatie tot virtuele valuta en in paragraaf 3 wordt het huidige wettelijk kader van witwassen en virtuele valuta besproken waarbij vooruitgebleekt wordt naar de implementatie van de vijfde anti-witwasrichtlijn. Vervolgens worden in paragraaf 4, mede aan de hand van praktische voorbeelden, de uitdagingen na invoering van de vijfde anti-witwasrichtlijn uiteengezet en wordt in paragraaf 5 afgesloten met de conclusie. Op andere voor- en tegenargumenten van regulering van virtuele valuta zoals wenselijkheid en haalbaarheid wordt, anders dan vanuit het oogpunt van witwasbestrijding, niet ingegaan.

2. Nationale risicoanalyse witwassen

2.1. Aanleiding NRA

Het opstellen van een NRA en een risicoanalyse terrorismefinanciering is een van de verplichtingen voor lidstaten die voortvloeit uit de vierde anti-witwasrichtlijn van de EU (hierna: vierde anti-witwasrichtlijn) van 20 mei 2015.⁵ De vierde anti-witwasrichtlijn heeft de derde anti-witwasrichtlijn⁶ en de PEP-richtlijn⁷ vervan-

5. Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad tot intrekking van Richtlijn 2005/60/EG van het Europees Parlement en de Raad en Richtlijn 2006/70/EG van de Commissie (PbEU L 141/73).
6. Richtlijn 2005/60/EG van het Europees Parlement en de Raad van 26 oktober 2005 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme (PbEU L 309/15).
7. Richtlijn 2006/70/EG van de Commissie van 1 augustus 2006 tot vaststelling van uitvoeringsmaatregelen van Richtlijn 2005/60/EG van het Europees Parlement en de Raad wat betreft de definitie van politiek prominente personen en wat betreft de technische criteria voor vereenvoudigde klantenonderzoeksprocedures en voor vrijstellingen op grond van occasionele of zeer beperkte financiële activiteiten (PbEU L 214/29).

gen en heeft de aangepaste aanbevelingen van de *Financial Action Task Force* (FATF) uit 2012 omgezet in Europese regelgeving.⁸

In Nederland zijn de maatregelen uit de vierde anti-witwasrichtlijn op 25 juli 2018 onder meer geïmplementeerd in de Wet ter voorkoming van witwassen en het financieren van terrorisme (Wwft). Hierna wordt de NRA voor Nederland besproken met betrekking tot virtuele valuta.

2.2. Doel NRA

Het opstellen van een NRA betekent het in kaart brengen van de belangrijkste risico's op witwassen. Door deze te identificeren, analyseren en beoordelen moet een lidstaat de eigen nationale risico's inzichtelijk maken.⁹ Het doen van een risicoanalyse heeft als doel het verbeteren van wet- en regelgeving ten aanzien van de bestrijding van witwassen en het stellen van prioriteiten binnen dat kader.¹⁰ Zo kunnen diverse partijen de NRA gebruiken om de eigen risico's (beter) te definiëren en beheersende maatregelen te treffen.¹¹

Deze verplichting is in Nederland een gezamenlijke verantwoordelijkheid van de minister van Financiën en de minister van Justitie en Veiligheid en is thans neergelegd in de Wwft.¹² De ministers hebben in aanloop naar de implementatie van de vierde anti-witwasrichtlijn het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) opdracht gegeven de eerste NRA voor Nederland uit te voeren.

2.3. Grootste witwasrisico's volgens NRA

Deze eerste NRA is op 14 december 2017 door het WODC gepubliceerd en aan de Tweede Kamer voorgelegd.¹³ In de NRA zijn tien risico's met de grootste potentiële impact voor witwassen opgenomen (zie tabel 1). Het begrip 'risico' wordt in de NRA aangeduid als een functie van de factoren dreigingen, kwetsbaarheden en gevolgen. Onder 'gevolgen' verstaat de NRA 'de effecten die optreden als gevolg van witwassen', oftewel de impact. Hierbij kan worden gedacht aan de uitwerking van criminele activiteiten op het financiële systeem, de financiële instituties, de economie en de samenleving.

Het risico van 'witwassen via financiële instellingen (met name banken)' staat bovenaan de lijst van witwasrisico's met de grootste potentiële impact. Het niveau van de potentiële impact is hierbij 71 tot en met 75 (op een schaal van 0 tot 100). Experts beoordelen het risico van misbruik van de diensten van financiële instellingen het grootst vanwege het vele geld dat in deze sector omgaat. De potentiële impact van 'witwassen via virtuele valuta'

8. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (The FATF Recommendations), February 2012.
9. Art. 7 vierde anti-witwasrichtlijn.
10. *Kamerstukken II* 2017/18, 34808 nr. 3, p. 41 en 42 (MvT).
11. *Kamerstukken II* 2017/18, 34808 nr. 3, p. 31 (MvT).
12. Art. 1f en art. 1 lid 1 Wwft.
13. *Kamerstukken II* 2017/18, 31477, 22.

Tabel 1 De tien grootste witwasrisico's volgens experts met de grootste potentiële impact*

Risico	Niveau potentiële impact (schaal van 0-100)
Witwassen via financiële instellingen (met name banken)	71 t/m 75
Witwassen via betaaldienstverleners	
Witwassen via trustkantoren	61 t/m 70
Witwassen via offshore vennootschappen	
Witwassen om verhuuld waarde weg te zetten	
Trade-Based Money Laundering	
Witwassen via fiscaal gedreven/complexe vennootschaps-rechtelijke structuren Witwassen via virtuele valuta	
Witwassen door contant geld vanuit/ naar Nederland te verplaatsen (al dan niet via ondergronds bankieren)	55 t/m 60
Witwassen via (inter)nationale beleggings- en of investerings-constructies om waarde te verplaatsen	

* H.C.J. van der Veen & L.F. Heuts, *National Risk Assessment Witwassen* (Cahier-2017-13), Den Haag: WODC 2017, p. 10.

Tabel 2 Gemiddelde weerbaarheid van het totale beleidsinstrumentarium per risico*

Risico	Type risico	Weerbaarheid (schaal van 0-100)
Witwassen via financiële instellingen (met name banken)	Witwaskanaal	41 t/m 50
Witwassen via betaaldienstverleners	Witwaskanaal	
Witwassen via trustkantoren	Witwaskanaal	
Witwassen via fiscaal gedreven/complexe vennootschaps-rechtelijke structuren	Witwasmethode	31 t/m 40
Witwassen via (inter)nationale beleggings- en/of investerings-constructies om waarde te verplaatsen	Witwasmethode	
Witwassen door contant geld vanuit/naar Nederland te verplaatsen (al dan niet via ondergronds bankieren)	Witwasmethode	
Witwasconstructies om verhuuld waarde weg te zetten	Witwasmethode	21 t/m 30
Witwassen via offshore vennootschappen	Witwasmethode	
Trade-Based Money Laundering	Witwasmethode	
Witwassen via virtuele valuta	Witwasmethode	11 t/m 20

* H.C.J. van der Veen & L.F. Heuts, *National Risk Assessment Witwassen* (Cahier-2017-13), Den Haag: WODC 2017, p. 11.

is in dit kader lager ingeschat op een niveau van 55 tot en met 60.

Naast kwetsbaarheden houdt de NRA ook rekening met het element 'weerbaarheid'. Weerbaarheid ziet op de aanwezigheid van factoren die de dreiging of de gevolgen daarvan juist beperken of zelfs opheffen. De NRA noemt accurate registraties, toezicht, handhaving en opsporing van voldoende capaciteit, kwaliteit en professionaliteit als voorbeelden. De NRA geeft per risico de gemiddelde weerbaarheid weer (zie tabel 2).

In de NRA wordt aangegeven dat de laagste weerbaarheid geldt voor (1) witwasmethoden die niet gereguleerd zijn, (2) methoden met een internationaal component en (3) methoden van witwassen die in relatieve anonimiteit kunnen worden uitgevoerd. Al deze drie elementen zijn van toepassing op virtuele valuta en verklaren de lage inschaling op een niveau van weerbaarheid van 11 tot en met 20 (op een schaal van 0-100).¹⁴ Ofschoon de poten-

14. H.C.J. van der Veen & L.F. Heuts, *National Risk Assessment Witwassen* (Cahier-2017-13), Den Haag: WODC 2017, p. 62.

tiële impact van ‘witwassen via virtuele valuta’ relatief gemiddeld op de lijst staat, wordt deze door een lage weerbaarheid als een groot risico voor witwassen gezien.

Als concreet voorbeeld van witwassen via virtuele valuta wordt in de NRA genoemd dat crimineel vermogen dat wordt omgezet in virtuele valuta, kan worden ingezet ten behoeve van andere criminele activiteiten, zoals de online aanschaf van wapens en drugs.¹⁵ Opgemerkt wordt dat crimineel vermogen dat wordt omgezet in virtuele valuta, om te kwalificeren als witwassen, ook kan worden ingezet voor legale activiteiten.

De risico's van virtuele valuta worden daarnaast beschreven in andere publicaties. Zo noemt het *Nationaal Dreigingsbeeld 2017 Georganiseerde criminaliteit* dat witwassen plaatsvindt door gebruik van cryptocurrency's, waarbij door accounthouders bedragen worden aangehouden zonder bancaire tegenrekening in de analoge wereld.¹⁶ De FATF heeft in 2014 een rapport uitgebracht over virtuele valuta, waarbij wordt omschreven welke verschillende valuta er zijn en welke risico's hieraan gerelateerd zijn.¹⁷ Recentelijk heeft de FATF genoemd dat dienstverleners actief bij Initial Coin Offerings (ICO's) onder de antiwitwaswetgeving zouden moeten worden gebracht.¹⁸ De FATF zegt daarmee ICO's een belangrijk risico te vinden. Daarnaast stipt de OESO aan dat cryptocurrency's en blockchain een uitdaging vormen voor de fiscale transparantie.¹⁹ Een voorbeeld dat het Openbaar Ministerie (OM) noemt is de bitcoin-pinautomaat waarbij contant geld kan worden omgewisseld in bitcoins en andersom.²⁰

3. Wettelijk kader van witwassen en virtuele valuta

3.1. Strafbaarstelling witwassen

In Nederland is witwassen strafbaar gesteld in het Wetboek van Strafrecht (Sr), in de artikelen 420bis e.v. Hoewel de strafbepalingen dateren uit december 2001 hoeven deze niet te worden aangepast in het licht van de opkomst van virtuele valuta. In 2017 veroordeelde de Rechtbank Rotterdam een bitcoinhandelaar voor gewoontewitwassen, omdat werd gehandeld in bitcoins onder omstandigheden die maakten dat moest worden vermoed dat de bitcoins van misdrijf afkomstig waren.²¹ Uit deze en andere uitspraken komt naar voren dat bit-

coins en impliciet ook andere cryptocurrency's vallen onder het bestanddeel ‘voorwerp’.²²

Van de strafbaarstelling en vervolging van witwassen gaat een zekere preventieve werking uit in de vorm van afschrikking en normbevestiging. Echter, dit zal, net als bij de strafbaarstelling van gronddelicten, onvoldoende zijn om de witwasrisico's volledig te beheersen.

3.2. Het voorkomen en melden van witwassen

Naast het primair repressieve strafrecht kent Nederland wetgeving die zich in het bijzonder richt op het voorkomen, het signaleren en het onverwijld melden van witwassen.²³ Deze toezichtwetgeving heeft tot doel witwassen en terrorismefinanciering door middel van het financiële stelsel te voorkomen met preventieve maatregelen.²⁴

De toezichtwetgeving richt zich op dienstverleners en risicovolle sectoren die veelvuldig door plegers van gronddelicten en witwassers worden gebruikt voor onder andere het afstorten, het bewaren en het verplaatsen van criminele gelden, het verhullen van de herkomst en gerechtigheid tot die gelden en voor de aankoop van registergoederen. Ook richt het zich op sectoren die gebruikt worden voor het consumptief besteden van criminele gelden, zoals bij jachtbouwers, garagebedrijven en juweliers.

Voor het bereiken van dit doel zijn in de Wwft banken, andere financiële ondernemingen en natuurlijke personen en rechtspersonen in het kader van specifieke beroepsactiviteiten, als instelling aangewezen om preventieve maatregelen na te leven. De twee belangrijkste verplichtingen in dat kader zijn het verrichten van cliëntenonderzoek (cliëntacceptatie, cliëntidentificatie, transactiemonitoring, herkomstvraag), ook wel *know your customer* (KYC) of *customer due diligence* (CDD) genoemd, alsmede het melden van ongebruikelijke transacties aan FIU-Nederland.²⁵

Deze twee kernverplichtingen zijn door de EU in de vierde anti-witwasrichtlijn bestendigd. De verplichtingen uit de vierde anti-witwasrichtlijn zijn op 25 juli 2018 geïmplementeerd in nationale wetgeving door het

15. H.C.J. van der Veen & L.F. Heuts, *National Risk Assessment Witwassen* (Cahier-2017-13), Den Haag: WODC 2017, p. 49.

16. F. Boerman, M. Grapendaal, F. Nieuwenhuis en E. Stoffers, *Nationaal dreigingsbeeld 2017 Georganiseerde criminaliteit*, mei 2017.

17. The Financial Action Task Force, *Virtual Currencies Key Definitions and Potential AML/CFT Risks*, June 2014.

18. Zie fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html (geraadpleegd op 15 november 2018).

19. OECD, *OECD Secretary-General report to G20 Finance Ministers and Central Bank Governors*, Buenos Aires, Argentina, March 2018.

20. 'OM vreesst witwaspraktijken met pinautomaten voor Bitcoins', *Het Financieel Dagblad*, 5 november 2017.

21. Rb. Rotterdam, 19 december 2017, ECLI:NL:RBROT:2017:10225.

22. Zie ook ECLI:NL:RBMNE:2017:5713, ECLI:NL:RBROT:2018:2201, ECLI:NL:RBMNE:2018:1180, ECLI:NL:RBMNE:2018:1183, ECLI:NL:RBMNE:2018:1191 en ECLI:NL:RBROT:2018:4269. In de laatste uitspraak oordeelde de rechter dat het begrip voorwerp in de zin van artikel 420bis en 420ter Sr een autonome strafrechtelijke betekenis toekomt en ruim omschreven is: het omvat alle zaken en vermogensrechten. Ook bitcoins vallen hieronder. Bitcoins zijn immers voor menselijke beheersing vatbare objecten met een waarde in het economische verkeer die voor overdracht vatbaar zijn. Er kan mee betaald worden. Ook zijn ze individueel bepaalbaar: alle bitcoins die ooit zijn gewonnen en alle transacties die ermee worden uitgevoerd, worden in de blockchain bijgehouden.

23. Andere nationale beleidsinstrumentaria om risico's ten aanzien van witwassen en terrorismefinanciering tegen te gaan zijn, volgens de NRA, de Wwft, Sr, Wet toezicht trustkantoren, fiscale wetgeving, Wet toezicht accountantsorganisaties, Wet Bibob en de Handelsregisterwet 2017.

24. *Kamerstukken II* 2011/12, 33238 nr. 3 (MvT).

25. Nationaal is FIU-Nederland volgens de Wwft aangewezen als enige dienst in Nederland bij welke de meldplichtige instellingen hun ongebruikelijke transacties dienen te melden. FIU-Nederland analyseert de gemelde ongebruikelijke transacties. Nadat ongebruikelijke transacties verdacht zijn verklaard, worden deze ter beschikking gesteld aan diverse opsporingsdiensten.

in werking treden van de Implementatiewet vierde anti-witwasrichtlijn,²⁶ alsook het gewijzigde Uitvoeringsbesluit Wwft 2018²⁷ en de Implementatieregeling vierde anti-witwasrichtlijn.²⁸ Hierdoor vallen onder meer alle instellingen uit de Wwft onder een toezichthouder.²⁹ Een uitbreiding van Wwft-instellingen naar bedrijven en dienstverleners die zich specifiek bezighouden met virtuele valuta heeft hiermee echter nog niet plaatsgevonden.

Alle instellingen waarop de Wwft van toepassing is, waren echter altijd al verplicht om ongebruikelijke transacties die zien op virtuele valuta te melden. Banken melden bijvoorbeeld al jarenlang aan FIU-Nederland ongebruikelijke transacties in relatie tot de aan- of verkoop van virtuele valuta waarvan de financiële tegenwaarden op bankrekeningen zichtbaar zijn. Ook een bitcoinhandelaar en de beheerder (*operator*) van een bitcoin-pinautomaat, die zakelijk handelen en bitcoins kopen of verkopen tegen contanten vanaf 10.000 euro, vallen onder het (huidige) instellingsbegrip van de Wwft.

Een uitzondering op de meldplicht van transacties in relatie tot virtuele valuta geldt voor de groep '(rechts)personen die beroeps- of bedrijfsmatig handelen als koper of verkoper van goederen voor zover *betaling van deze goederen in contanten plaatsvindt* voor een bedrag van 10.000 euro of meer'.³⁰ Deze uitzondering vloeit voort uit het instellingsbegrip. De handelaar die

beroeps- of bedrijfsmatig betalingen verricht in virtuele valuta en niet in contanten, kwalificeert niet als instelling. Een juwelier die een sieraad verkoopt ter waarde van € 10.000 of meer en betaald krijgt in bitcoins, heeft voor deze transactie dan ook geen meldplicht. Toenevende acceptatie van virtuele valuta bij deze meldgroep maakt dit tot een witwasrisico met een potentieel relevante impact.

Nederland kent overigens een strafbaarstelling in de Wet op de economische delicten voor het niet-naleven van de verplichtingen uit de Wwft, zoals het niet onverwijld melden van ongebruikelijke transacties en het niet uitvoeren van cliëntenonderzoek.³¹

3.3. Vijfde anti-witwasrichtlijn van de EU

Een jaar na het aannemen van de vierde anti-witwasrichtlijn heeft de Europese Commissie een voorstel gedaan om deze richtlijn te wijzigen. De Commissie heeft enkele doelen verwoord, zoals onder andere het bereiken van een verbetering ten aanzien van virtuele valuta, informatietoegang (bijvoorbeeld van nationale FIU's tot bankgegevens), prepaidkaarten en illegaal contant geld.

Deze gewijzigde wetgeving, de vijfde anti-witwasrichtlijn, is aangenomen door het Europees Parlement en de Raad.³² De aanleiding voor deze wijziging was drieërlei. Allereerst de opkomst van technologische diensten die steeds vaker als alternatieve financiële systemen worden gebruikt en de risico's die met deze nieuwe financieringsinstrumenten en betalingsmogelijkheden samenhangen. Ten tweede was er een toenemende verwevenheid van georganiseerde misdaad en terrorisme waar te nemen (zoals de terroristische aanslagen in o.a. Parijs en Brussel). En ten derde was betere samenwerking gewenst tussen verschillende bevoegde autoriteiten, zowel tussen als binnen lidstaten.³³

Onder virtuele valuta wordt volgens de vijfde anti-witwasrichtlijn verstaan: *'een digitale weergave van waarde die noch door een centrale bank, noch door een overheid wordt uitgegeven en evenmin aan een fiduciaire valuta is gekoppeld, maar die door natuurlijke of rechtspersonen als een betaalmiddel wordt aanvaard en kan worden overgedragen, opgeslagen of elektronisch verhandeld.'*³⁴

Waar tot op heden geen aandacht werd besteed aan virtuele valuta in antiwitwaswetgeving, brengt de vijfde anti-witwasrichtlijn daar verandering in. Uit het voorstel volgt dat eronder worden gebracht:

26. Wet van 11 juli 2018 tot wijziging van de Wet ter voorkoming van witwassen en financieren van terrorisme en enige andere wetten in verband met de implementatie van richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2005/60/EG van het Europees Parlement en de Raad en Richtlijn 2006/70/EG van de Commissie (PbEU 2015, L 141), alsmede in verband met de uitvoering van verordening (EU) 2015/847 van het Europees Parlement en de Raad van 20 mei 2015 betreffende bij geldovermakingen te voegen informatie en tot intrekking van Verordening (EG) nr. 1781/2006 (PbEU 2015, L 141) (Implementatiewet vierde anti-witwasrichtlijn).
27. Besluit van 17 juli 2018, houdende nadere regels met betrekking tot uiteindelijk belanghebbenden en politiek prominente personen, het vaststellen van indicatoren voor het melden van ongebruikelijke transacties en tot wijziging van enige andere besluiten in verband met de implementatie van de vierde anti-witwasrichtlijn en de verordening betreffende bij geldovermakingen te voegen informatie (Uitvoeringsbesluit Wwft 2018).
28. Regeling van de Minister van Financiën en de Minister van Justitie en Veiligheid van 13 juli 2018, nr. 2018-0000113969, directie Financiële Markten, tot wijziging van de Uitvoeringsregeling Wet ter voorkoming van witwassen en financieren van terrorisme en enige andere regelingen in verband met de implementatie van de vierde anti-witwasrichtlijn (Implementatieregeling vierde anti-witwasrichtlijn).
29. De groep van *beroeps- of bedrijfsmatige handelende kopers of verkopers*, anders dan die in aangewezen goederen, kende tot voor kort als enige meldgroep geen toezichthouder. Door het aangenomen Aanwijzings- en mandaatbesluit Wwft 2018 is de groep onder het gedelegeerde toezicht van Bureau Toezicht Wwft van de Belastingdienst gebracht. Zie art. 2 Aanwijzings- en mandaatbesluit Wwft 2018 en art. 1a lid 4 onder h Wwft.
30. Na wijziging van de Wwft op 25 juli 2018 vallen ook de aankooptransacties onder de reikwijdte van deze groep en is de transactie-omvang teruggebracht van € 15.000 naar € 10.000 in contanten.

31. Art. 16 Wwft, art. 3 Wwft in verband met art. 1 WED en art. 2 lid 1 WED.
32. Richtlijn 2018/843/EG van het Europees Parlement en de Raad van 30 mei 2018 als aanvulling op de richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van Richtlijn 2009/138/EG en 2013/36/EU.
33. Implementatiewet wijziging vierde anti-witwasrichtlijn van 11 december 2018, p. 1 (MvT), www.internetconsultatie.nl.
34. Richtlijn 2018/843/EG van het Europees Parlement en de Raad van 30 mei 2018 als aanvulling op de richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van Richtlijn 2009/138/EG en 2013/36/EU, p. 33.

- aanbieders die zich in de eerste plaats en professioneel bezighouden met diensten voor het wisselen van virtuele valuta en fiduciaire valuta (d.w.z. munten die als wettig betaalmiddel zijn erkend) ('wisselplatforms voor virtuele valuta');
- portemonneeaanbieders die diensten verlenen voor de bewaring van de credentialen die nodig zijn om toegang te krijgen tot virtuele valuta ('aanbieders van bewaarportemonnees').

Om de aan anonimiteit verbonden risico's te bestrijden, zouden nationale FIU's volgens de Commissie in staat moeten zijn virtuele valuta-adressen te koppelen aan de identiteit van de eigenaar van virtuele valuta. De Commissie maakt niet duidelijk op welke wijze deze opdracht door de FIU's moet worden gerealiseerd. Bovendien zou volgens de Commissie verder onderzocht kunnen worden of gebruikers in staat gesteld kunnen worden zich op vrijwillige basis bekend te maken bij aangewezen autoriteiten.³⁵ Tot slot schrijft de richtlijn voor dat aanbieders van wisselplatforms voor virtuele valuta en aanbieders van bewaarportemonnees geregistreerd moeten worden.

3.4. Implementatiewet wijziging vierde anti-witwasrichtlijn

Op 11 december jl. heeft het ministerie van Financiën samen met het ministerie van Justitie en Veiligheid een publieke consultatie geopend voor de implementatiewet. Hierop kon gereageerd worden tot 15 januari jl. De meeste bepalingen dienen op 10 januari 2020 in nationale wet- en regelgeving geïmplementeerd te zijn.

Op grond van de richtlijn is het noodzakelijk om de Nederlandse wetgeving op verschillende punten aan te passen. In hoofdzaak betreffen deze aanpassingen (1) het onder de integriteitswetgeving brengen van virtuele valuta, (2) het treffen van nadere maatregelen ten aanzien van hoogrisicolanden en (3) het uitbreiden van de samenwerkingsmogelijkheden voor toezichthoudende autoriteiten.³⁶ De belangrijkste aanpassingen voor nationale wetgeving, in relatie tot het onder de integriteitswetgeving brengen van virtuele valuta, worden hieronder kort aangestipt.

Zoals de vijfde anti-witwasrichtlijn voorschrijft zullen de anti-witwasverplichtingen gaan gelden ten aanzien van de wisselplatforms voor virtuele valuta en aanbieders van bewaarportemonnees. Op deze manier worden dergelijke aanbieders verplicht tot het verrichten van cliëntenonderzoek en het melden van ongebruikelijke transacties aan FIU-Nederland.

Opvallend is dat de registratieplicht uit de vijfde anti-witwasrichtlijn in de implementatiewet vorm wordt gegeven als een vergunningplicht. Het is voor het eerst dat binnen de Wwft een vergunningplicht wordt inge-

voerd voor een instelling. Gezien de hoge risico's die samenhangen met de dienstverlening en gelet op de poortwachtersfunctie die deze aanbieders vervullen, is het nodig dat er vooraf een toets kan plaatsvinden of deze aanbieders daadwerkelijk in staat zijn de risico's op terrorismefinanciering en witwassen voldoende te mitigeren.³⁷

De verplichting om een vergunning aan te vragen geldt voor iedere aanbieder die wisseldiensten en bewaarportemonnees beroeps- of bedrijfsmatig in of vanuit Nederland aanbiedt. Zonder een vergunning mogen de diensten niet worden aangeboden. Dit geldt niet alleen voor aanbieders die in Nederland gevestigd zijn, maar ook voor aanbieders die vanuit een andere lidstaat of vanuit een derde land diensten in Nederland aanbieden en zich richten op de Nederlandse markt.

In het wetsvoorstel wordt De Nederlandsche Bank (DNB) aangewezen als Wwft-toezichthouder voor deze aanbieders. De te verlenen vergunning ziet overigens niet zozeer op de activiteiten van de aanbieders zelf, maar op het feit dat de instelling over adequate beheersmaatregelen beschikt om te voldoen aan de Wwft-verplichtingen.³⁸

4. Uitdagingen na invoering vijfde anti-witwasrichtlijn

4.1. Virtuele valuta en algemene uitdagingen

Virtuele valuta maken het mogelijk om op afstand, op ieder moment, vanuit iedere locatie met een internetverbinding, anoniem en buiten het zicht van overheden en financiële instellingen, zonder opgaaf van redenen en het afleggen van verantwoording, wereldwijd (criminele) transacties tussen partijen aan te gaan en financieel af te wikkelen, (criminele) vermogens over te dragen, aan te houden en te besteden. Hoewel transacties in virtuele valuta als de bitcoin voor eenieder zichtbaar zijn op de blockchain, staat anonimiteit en encryptie de koppeling met een identiteit, respectievelijk beslaglegging, in de weg. Transacties zijn zichtbaar, maar partijen en valuta-tegoeden blijven in hoge mate ongrijpbaar.

Nederlandse opsporingsinstanties constateren in toenemende mate dat virtuele valuta bij witwasonderzoeken worden gesignaleerd en hebben hier ook meer aandacht aan besteed. Van de virtuele valuta zijn het vooral bitcoins die de afgelopen jaren in beslag zijn genomen.³⁹ Er is nationaal en internationaal veel aandacht voor de illegale handel op het dark web, het gebruik van virtuele valuta daarbij, alsmede voor personen die criminelen de mogelijkheid bieden hun criminele virtuele valuta om te zetten in (contant) fiatgeld (o.a. euro's en dollars), de

35. Richtlijn 2018/843/EG van het Europees Parlement en de Raad van 30 mei 2018 als aanvulling op de richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van Richtlijn 2009/138/EG en 2013/36/EU, p. 24 en 25.

36. Implementatiewet wijziging vierde anti-witwasrichtlijn van 11 december 2018, p. 1 (MvT), www.internetconsultatie.nl.

37. Implementatiewet wijziging vierde anti-witwasrichtlijn van 11 december 2018, p. 11 (MvT), www.internetconsultatie.nl.

38. Implementatiewet wijziging vierde anti-witwasrichtlijn van 11 december 2018, p. 11 en 12 (MvT), www.internetconsultatie.nl.

39. *Aanhangsel Handelingen II* 2017/18, 793.

zogenaamde *cash-out*.⁴⁰ In 2017 zijn door FIU-Nederland nieuwe witwastypologieën gevalideerd over de aan- en verkoop van virtuele betaalmiddelen.⁴¹

Door het opnemen van wisselplatforms en aanbieders van bewaarportemonnees in de vijfde anti-witwasrichtlijn en de voorgestelde implementatiewet wordt de problematiek van anonimiteit die verbonden is aan bewaarportemonnees (*wallets*) en transacties met virtuele valuta deels, maar niet volledig opgelost. Gebruikers kunnen namelijk ook wallets aanhouden en transacties verrichten zonder betrokkenheid van wisselplatforms of aanbieders van bewaarportemonnees. Dit is inherent aan de onderliggende Blockchaintechnologie die ‘peer-to-peer’ transacties⁴² mogelijk maakt zonder tussenkomst van (gereguleerde) derden. Het mag duidelijk zijn waar de voorkeur van een crimineel naar uitgaat. Andere middelen die worden ingezet om de eigen anonimiteit te vergroten zien op het gebruik van een derde, bijvoorbeeld een katvanger of het gebruik van een bitcoinhandelaar voor de (contante) aan- of verkoop van bitcoins. Daarnaast zijn er technieken die kunnen worden ingezet om de criminele herkomst van bitcoins te verhullen zoals het gebruik van mixing services.⁴³

De eerdergenoemde zichtbaarheid van onderlinge transacties staat onder druk door de opkomst van zogenaamde privacy coins en ontwikkelingen waarbij transacties *off-chain* of via een *side-chain* worden verwerkt en vastgelegd.⁴⁴ Privacy coins zijn cryptocurrency’s die een hogere mate van privacy bieden dan bitcoins. Door gebruik te maken van mixing-technieken wordt de link tussen verzender en ontvanger verbroken of wordt een transactie in zijn geheel verborgen. Door gebruik te maken van Tor en I2P kan het IP-adres van de gebruiker afgeschermd worden.⁴⁵ Voorbeelden van populaire privacy-coins zijn dash, monero, verge en z-cash.

Wanneer een transactie met virtuele valuta plaatsvindt via een derde, zoals wisselplatforms, aanbieders van bewaarportemonnees en/of andere (financiële) instellingen,

zal het risico op witwassen daar kunnen worden beheerst, gelet op de (toekomstige) wettelijke verplichtingen, namelijk de inzet van KYC-maatregelen en het verrichten van meldingen aan FIU-Nederland. Enkele voorbeelden waarbij virtueel geld omgewisseld wordt in chartaal of giraal geld en die een risico vormen op witwassen, deels na implementatie van de vijfde anti-witwasrichtlijn, komen hierna aan de orde.

4.2. Praktische voorbeelden

Bij een bitcoin-pinautomaat kan een vorm van KYC plaatsvinden die afhankelijk is van de transactieomvang. In zijn algemeenheid zijn transacties tot € 1.000 à € 2.000 volledig anoniem. Afhankelijk van de instellingen van de bitcoin-pinautomaat vindt identificatie plaats via sms, vingerafdruk en/of een identiteitsbewijs. In dat laatste geval zal de operator, ter plaatse of op afstand, de identiteit van de klant moeten verifiëren wil de transactie doorgang kunnen vinden. Tevens zal de operator de uitkomsten van dit proces moeten documenteren. Een bitcoin-pinautomaat beschikt over de nodige technische voorzieningen om dit alles mogelijk te maken. De operator kan de limieten en de KYC-maatregelen overigens zelf instellen. Uit de concept memorie van toelichting bij de Implementatiewet volgt dat een bitcoin-pinautomaat zal kwalificeren als een wisselplatform voor virtuele valuta.⁴⁶ Degene die een bitcoin-pinautomaat daadwerkelijk in beheer heeft, wordt beschouwd als de aanbieder van de wisseldienst, niet degene die een bitcoin-pinautomaat ter beschikking stelt, zoals een winkeleigenaar waar een dergelijke automaat geplaatst wordt. Dit betekent dat de operator, op basis van de subjectieve indicator, ook transacties onder de € 10.000 dient te gaan melden indien er aanleiding is te veronderstellen dat deze verband houden met witwassen.

Een ander voorbeeld ziet op buitenlandse prepaidkaarten waarbij bitcoins en andere virtuele valuta als tegenwaarde in een betaaltransactie worden gebruikt. Deze kaarten maken het de kaartgebruiker mogelijk vrijwel direct een tegoed aan virtuele valuta te gebruiken bij reguliere (online) aankopen en geldopnamen wereldwijd. Bestedingen kunnen zelfs plaatsvinden bij winkels die geen virtuele valuta accepteren. Kaartuitgevers van buiten de EU noch de lokale verwerkers van de betaaltransacties vallen namelijk onder de anti-witwasrichtlijnen. Dit betekent dat door deze instellingen geen meldingen worden gedaan inzake ongebruikelijke (en verdachte) transacties.

Bij de verkoop van bitcoins aan een (buitenlands) wisselplatform kunnen zowel het wisselplatform als de betrokken (buitenlandse) bankinstelling tot melding overgaan voor zover deze zijn gereguleerd. Ook indien wisselplatforms niet zijn gereguleerd zouden deze KYC-maatregelen dienen te treffen die zijn gekoppeld aan handelslimieten. Het melden aan een FIU vindt dan echter niet plaats.

40. In de fenomeenbeschrijving ‘De bitcoinhandelaar, een faciliterende rol bij de cash-out van criminele verdiensten’, AMLC, 2017, worden enkele mogelijkheden tot een dergelijke cash-out beschreven.

41. S. Visser, ‘Nieuwe witwastypologieën in de strijd tegen witwassen met virtuele betaalmiddelen’, *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 2017, aflevering 4.

42. ‘Peer-to-peer’ transacties zijn transacties die men direct aan een ander kan overmaken, zonder gebruik te maken van een centrale entiteit. Iedereen is met ‘peer-to-peer’ aangesloten op hetzelfde netwerk.

43. ‘De bitcoinhandelaar, een faciliterende rol bij de cash-out van criminele verdiensten’, AMLC, 2017, p. 10.

44. Van *off-chain* is sprake indien transacties tussen twee partijen op een tweede laag plaatsvinden, buiten de blockchain van de virtuele valuta om. Op het moment dat er geen transacties meer tussen beide partijen zullen plaatsvinden wordt het saldo van de transacties geregistreerd op de blockchain. Bij een *side-chain* gaan meerdere partijen op een afzonderlijke blockchain transacties met elkaar aan. Hiervoor worden hun bitcoins eerst omgezet in een equivalent van een valuta dat op de betreffende side-chain wordt gebruikt. Indien een partij weer in bitcoin wil gaan handelen wordt de betreffende valuta weer omgezet in bitcoins.

45. Tor staat voor The Onion Router en is ontwikkeld om het IP-adres van een computer te maskeren bij overdracht van informatie naar een ander IP-adres. De informatie wordt eerst doorgeleid naar andere gebruikers (nodes), alvorens die op de eindbestemming aankomt. I2P staat voor the Invisible Internet Project en is vergelijkbaar met Tor, maar maakt gebruik van een andere techniek.

46. Implementatiewet wijziging vierde anti-witwasrichtlijn van 11 december 2018, p. 4 (MvT), www.internetconsultatie.nl.

4.3. Overige uitdagingen en aanbeveling

Bovenstaande ontwikkelingen maken dat ook andere toezichthouders, naast DNB, betrokken worden bij virtuele valuta. Zo is een belangrijke rol voor de Belastingdienst weggelegd nu particuliere vermogens in toenemende mate in virtuele valuta worden aangehouden en zakelijke transacties decentraal via een blockchain verlopen en in virtuele valuta worden verricht.⁴⁷ Parallel aan de afbraak van het bankgeheim in Europese landen de afgelopen tien jaar, loopt de opkomst van de virtuele valuta. Net als de langdurige strijd tegen het bankgeheim en tegen verborgen vermogens aangehouden op (onbekende) buitenlandse bankrekeningen, zal het een uitdaging zijn voor belastingdiensten wereldwijd hier zicht op te krijgen, en, gelijk aan de buitenlandse bankrekeningen, deze informatie ook met elkaar te delen.

Een laatste uitdaging die blijft bestaan, ook na implementatie van de vijfde anti-witwasrichtlijn in nationale wetgeving, is het risico op witwassen bij een toenemende acceptatie van virtuele valuta bij de groep van '(rechts)personen die beroeps- of bedrijfsmatig handelen als koper of verkoper van goederen'.⁴⁸ Deze groep kwalificeert niet als instelling onder de Wwft als betalingen plaatsvinden in virtuele valuta en niet in contanten voor een bedrag van € 10.000 of meer. Het toezicht op basis van de Wwft is daardoor niet van toepassing en er bestaat geen wettelijke verplichting voor het uitvoeren van cliëntenonderzoek alsook het melden van ongebruikelijke transacties. Om die reden is het wenselijk dit instellingsbegrip uit te breiden met een tegenwaarde in virtuele valuta, zodat het risico adequater kan worden beheerst.

5. Conclusie

Concluderend kan worden gesteld dat voor het beheersen van witwasrisico's bij virtuele valuta uitdagingen blijven bestaan ten aanzien van de huidige Wwft en ten aanzien van de situatie na implementatie van de vijfde anti-witwasrichtlijn in nationale wetgeving.

Door het omzetten van de vijfde anti-witwasrichtlijn in nationale wetgeving zullen in de nabije toekomst wisselplatforms en aanbieders van bewaarportemonnees onder de antiwitwaswetgeving worden gebracht. Daarnaast zal er een vergunningplicht in de Wwft worden opgenomen voor deze nieuwe instellingen en is DNB als Wwft-toezichthouder aangewezen. Dit is onder meer van belang voor het kunnen beheersen van de witwasrisico's via wisselplatforms en aanbieders van bewaarportemonnees en voor de behoefte die zal bestaan, bij deze toekomstige poortwachters, aan duidelijke richtlijnen om adequaat aan de nieuwe verplichtingen te kunnen voldoen.

Hoewel deze ontwikkelingen een eerste stap zijn in het beheersen van witwasrisico's bij virtuele valuta, en van strafbaarstelling van witwassen en vervolging een zekere preventieve werking uitgaat, zijn er ook situaties geschetst die niet (volledig) onder de antiwitwaswetgeving vallen en waardoor de risico's van witwassen via virtuele valuta onvoldoende kunnen worden gemitigeerd.

Dit wordt mede veroorzaakt doordat, ook na (zelf)regulering, in de praktijk voldoende risico's overblijven, zoals het gebruik van valse identiteiten, het smurfen van transacties,⁴⁹ het niet melden van ongebruikelijke transacties en het gebrek aan actieve uitwisseling van verdachte transacties in internationaal verband. Een en ander is tevens inherent aan de blockchain, maar met name gerelateerd aan geldgedreven criminaliteit. Opsporingsdiensten en het OM dienen zich dan ook ervan bewust te zijn dat zij een actieve en voorname rol moeten blijven vervullen in het zelf signaleren van witwassen via virtuele valuta, zowel binnen de infrastructuur van virtuele valuta zelf als bij de omzetting van virtuele valuta naar (contant) fiatgeld en andersom. Deze risico's rechtvaardigen de inschaling qua kwetsbaarheid en weerbaarheid ook na implementatie van de vijfde anti-witwasrichtlijn.

Tot slot is gezien het internationale karakter van virtuele valuta een geïntegreerde internationale benadering nodig om een effectieve aanpak te bewerkstelligen. Nederland heeft aangegeven een voortrekkersrol te willen vervullen binnen de Europese en internationale aanpak van virtuele valuta.⁵⁰

47. *Handelingen II* 2017/18, 33.

48. Art. 1a lid 4 sub i Wwft.

49. Het smurfen van transacties houdt in het opknippen van een transactie (bedrag) in kleinere hoeveelheden geld om onder een meldgrens te blijven.

50. *Kamerstukken II* 2017/18, 32013, 168.