Slimme technieken als antwoord op de Financial Economic Crime crisis

1 Inleiding

Financiële instellingen spelen een belangrijke rol bij de bestrijding van financieel-economische criminaliteit (FEC). In de rol van poortwachter zijn zij verantwoordelijk voor het herkennen, rapporteren of zelfs weren van ongebruikelijk gedrag. Door toegenomen verwachtingen vanuit de toezichthouder[1] als ook de samenleving[2] wordt de druk op de financiële sector om FEC te beheersen steeds groter.

Als reactie daarop hebben veel financiële instellingen zeer omvangrijke initiatieven opgestart met als doel om (nog) meer ongebruikelijke transacties en cliënten te detecteren. De invulling van deze projecten is doorgaans het opschalen van de bestaande *anti-money laundering* (AML) en sanctieteams of het inrichten van omvangrijke projectteams. De trend is duidelijk: er wordt meer en meer personeel aangetrokken om de risico's te mitigeren. In een recent artikel wordt beschreven dat bij een van de Nederlandse

Met de alsmaar toenemende investeringen, zonder dat duidelijk is welke inspanningen nodig zijn om de risico's goed te mitigeren, kan worden gesteld dat de compliance op het gebied van FEC zich in een crisis bevindt

[1] DNB, 'Toezicht Vooruitblik 2020', dnb.nl.
[2] L. Essers, 'Banken willen witwasaanpak: samen miljarden transacties controleren', RTL Nieuws 13 september 2019, rtlnieuws.nl.

grootbanken inmiddels een tiende van het volledige werknemersbestand bezig is met het doorlichten van cliënten en het speuren naar financiële criminaliteit.[3] Met de alsmaar toenemende investeringen, zonder dat duidelijk is welke inspanningen nodig zijn om de risico's goed te mitigeren, kan worden gesteld dat de compliance op het gebied van FEC zich in een crisis bevindt.

Kunstmatige intelligentie, vaak aangeduid met de Engelstalige term *artificial intelligence* (AI), is het vermogen van een computer om taken uit te voeren die voorheen voorbehouden waren aan intelligente wezens: de mens. Deze algoritmes bleven veelal binnen de muren van de universiteit. Echter, in toenemende mate weten de wetenschappelijke technieken zich te bewegen richting onze tastbare samenleving. Zo ook als toepassing bij het bestrijden van FEC.

Een mogelijke oplossing voor de huidige crisis op het gebied van FEC-compliance zou kunnen liggen in het opzetten van een (volledig) andere inrichting van de poortwachtersfunctie. AI zou daar een grote rol bij kunnen spelen. Maar wat kan er allemaal met AI en wat zijn de voordelen van het inzetten van deze technieken? Is AI een noodzaak om het hoofd te bieden aan de crisis waar financiële instellingen mee worstelen? In dit artikel zetten wij een aantal technieken uiteen die geschikt zijn om te gebruiken bij de bestrijding van FEC en maken wij duidelijk hoe deze waarde toe kunnen voegen. Vanwege de grote toegevoegde waarde van deze technieken voor transactiemonitoring en sanctiescreening diepen wij deze onderwerpen verder uit. Ook zullen wij aandacht besteden aan de nadelen en risico's van het gebruik van AI in het kader van FEC-compliance.

2 FEC-compliance in crisis

Financiële instellingen vervullen de belangrijke rol van poortwachter tot ons financieel stelsel. Deze verantwoordelijkheid is vastgelegd in de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). In dat kader voeren financiële instellingen cliëntonderzoek uit en monitoren zij de relatie met als doel om witwassen en terrorismefinanciering te voorkomen. In aanvulling daarop zijn financiële instellingen en een aantal andere partijen op grond van de Sanctiewet 1977 (Sanctiewet) verplicht om maatregelen te treffen ter naleving van ingestelde sancties. De Nederlandsche Bank (DNB) stelt dat het cruciaal is dat financiële instellingen hun poortwachtersfunctie adequaat inrichten om FEC tegen te gaan. Niet alleen DNB heeft hoge verwachtingen van financiële instellingen, ook vanuit de samenleving zijn de verwachtingen hoog gespannen.

Met de doelstellingen om de rol als poortwachter te verbeteren, de wet na te leven en nog meer te voldoen aan de verwachtingen van de maatschappij hebben diverse financiële instellingen veel mensen aangetrokken die ondersteunen bij het onderzoeken van cliënten en ongebruikelijke transacties. Daarbij kan eraan worden getwijfeld of de inspanningen die de financiële instellingen momenteel verrichten wel de beste manier zijn om aan de

[3] 'Wanneer gaan banken kosten CDD aan klanten doorberekenen?',Banken.nl 18 mei 2020, banken.nl.

hooggespannen verwachtingen te voldoen. De genomen maatregelen zijn zeer omvangrijk, maar zijn deze ook echt effectief? De inspanningen zijn nu vooral gericht op het uitbreiden van de menselijke detectie en onderzoekscapaciteit. Het is de vraag of het ontplooien van deze extra activiteiten de beste manier is om de risico's te mitigeren.

Ondertussen neemt het transactieverkeer alsmaar verder toe[4], wat resulteert in meer gegevens die beoordeeld moeten worden waarbij het vinden van de echte ongebruikelijke transacties te vergelijken is met het zoeken naar een speld in een hooiberg. Financiële instellingen zijn daarom hard op zoek naar nog meer analisten die dit werk kunnen uitvoeren.[5]

Daar komt bij dat het jaar 2020 zeer waarschijnlijk voor eenieder anders is uitgevallen dan van tevoren bedacht. Zo ook voor financiële instellingen. Naast alle andere problematiek die er speelt, is sinds de uitbraak van de COVID-19-pandemie het transactiegedrag van de samenleving constant aan verandering onderhevig, onder andere door de steeds wisselende maatregelen. Ook is er een toename van bepaalde (nieuwe) vormen van fraude en misbruik, zoals whatsappfraude.[6] Onverwachte kenteringen in gedrag van zowel de gewone burger als criminelen vragen om een dynamische aanpak met de inherente eigenschap hierop te kunnen acteren.

Ook is er een toename van bepaalde (nieuwe) vormen van fraude en misbruik, zoals whatsappfraude

Logischerwijs is het dan ook de vraag hoe lang de huidige situatie nog houdbaar is en in welke mate de grote investeringen in de uitbreiding van de verschillende teams ook echt voor een betere beheersing van de FEC-risico's zorgen.

3 Wat is AI en welke technieken zijn er?

Sinds de totstandkoming van de eerste computers in het begin van de vorige eeuw is er binnen de universiteiten constant gewerkt aan het steeds slimmer maken van de computers door middel van het ontwikkelen van algoritmes.

De kunst van AI is om met name systemen te bouwen die, net als de mens, kunnen leren van ervaring, voorbeelden of zelfs andere computers. Om deze vaardigheden te kunnen nabootsen zijn er verschillende technieken ontwikkeld. Sommige van deze technieken zijn uiterst geschikt om specifieke afwijkingen ten opzichte van een groep te vinden, terwijl andere technieken juist bedoeld zijn om te leren van eerder door een mens gemaakte keuzes en bij toekomstige situaties een inschatting te maken van welke keuze een mens zou hebben gemaakt. Sommige van deze technieken zijn heel transparant en goed navolgbaar, terwijl andere technieken meer lijken op een *black box*.

[4] SWIFT, 'Double digit growth in SWIFT message volumes as gpi uptake soars', 23 januari 2019, swift.com.
[5] E. Rooijers & J. Leupen, 'Banken betalen vorstelijk om honderden 'Sherlocks' te vinden in een leeggeviste markt', Het Financieele Dagblad 3 januari 2020, fd.nl.
[6] 'Nu al vier keer zoveel meldingen van WhatsApp-fraude als in 2019', Trouw 12 oktober 2020, trouw.nl.

Binnen de AI worden de technieken vaak ingedeeld in vier groepen[7]: *supervised learning, unsupervised learning, semi-supervised learning en reinforcement learning*. Deze vier groepen kunnen weer verder onderverdeeld worden in subgroepen en specifieke technieken.

Hieronder geven wij een korte beschrijving van deze vier groepen.

De indeling hieronder geeft een algemeen beeld van de verschillende AI-technieken. Echter, niet alle specifieke AI-technieken zijn goed binnen deze indeling te plaatsen. Sommige technieken rusten op meerdere principes. Helaas gaat het te ver om alle mogelijkheden van AI binnen het transactiemonitoring- en sanctiedomein te beschrijven in dit artikel, maar in de volgende paragrafen beschrijven wij wel een aantal voorbeelden.

1

Bij **supervised learning** wordt het algoritme getraind om een toekomstige beoordeling te maken op basis van beoordelingen van historische cases. Voor FEC zou het bijvoorbeeld kunnen gaan om het afhandelen van sanctie-alerts, waarbij wordt beoordeeld of een alert terecht is of een zogenoemde *false positive*. Daarbij wordt het algoritme getraind op basis van de alert-afhandeling die in het verleden is uitgevoerd. Deze techniek kan alleen worden toegepast als er een redelijke hoeveelheid betrouwbare historische informatie beschikbaar is die reeds is beoordeeld.

2

Bij **unsupervised learning** worden geen historische voorbeelden gebruikt om de computer te trainen. Bij deze techniek abstraheert het algoritme patronen of structuren uit de dataset. Met deze techniek wordt de data dan ook gegroepeerd of geclusterd. Vaak wordt deze techniek toegepast als er weinig of geen betrouwbare informatie beschikbaar is over historische cases om te gebruiken als basis voor de training.

3

De middenweg tussen bovengenoemde technieken betreft **semi-supervised learning**, waarbij het algoritme wordt getraind met zowel informatie waarover reeds een beoordeling bekend is als informatie waarover die beoordeling niet bekend is voor het algoritme. Een voorbeeld voor FEC kan zijn dat het algoritme wordt getraind om ongebruikelijke transacties te detecteren, waarbij slechts voor een deel van de transacties is aangegeven of deze al dan niet ongebruikelijk zijn. Deze techniek is een krachtig compromis, waarbij wordt gesteund op kennis uit het verleden, maar tevens de weg vrij is om nieuwe patronen te detecteren.

4

Met behulp van **reinforcement learning** leert het algoritme steeds op basis van de gevolgen van de beslissingen, waarbij wordt bewaakt dat het eind-resultaat de beste uitkomst heeft. Deze techniek steunt heel erg op een *trial and error*-aanpak en wordt daarom naar verwachting minder toegepast binnen FEC waar de ruimte om fouten te mogen maken klein is. Een domein waar deze techniek bijvoorbeeld wel werkt is bij het ontwikkelen van een schaak-computer die tegen zichzelf mag spelen.

[7] A. Dusgupta en A. Nath, 'Classification of Machine Learning Algorithms', International Journal of Innovative Research in Advanced Engineering maart 2016.

4 AML post-event transactiemonitoring

Post-event transactiemonitoring is het proces waarbij achteraf wordt gekeken of er transacties of combinaties van transacties zijn die ongebruikelijk zijn en er hierbij een verwachting is van witwassen en/of terrorismefinanciering.[8] Een bank kan dergelijke transacties melden als ongebruikelijk, maar kan daarnaast ook andere acties ondernemen, zoals het uitvoeren van extra cliëntonderzoek, afscheid nemen van de cliënt of verscherpte monitoring instellen.

De huidige technische oplossingen op het gebied van transactiemonitoring worden al jaren toegepast

De huidige technische oplossingen op het gebied van transactiemonitoring worden al jaren toegepast: er is een database met alle uitgevoerde transacties en hieruit worden enkele selecties gemaakt die kwalificeren als mogelijk ongebruikelijk. Die selecties worden vervolgens handmatig beoordeeld. Die selecties, vaak benoemd als transactiemonitoringregels, zijn gedefinieerd als mitigerende maatregelen voor de risico's zoals benoemd in bijvoorbeeld de Systematische Integriteitsrisicoanalyse (SIRA) van de organisatie. Deze aanpak heeft twee grote nadelen: veel van de alerts uit dergelijke systemen zijn onterecht (zogenaamde *false positives*) en het systeem is niet in staat om al het ongebruikelijke gedrag en vooral het onbekende witwasgedrag te detecteren (zogenaamde *false negatives*). Als een bepaald soort gedrag niet expliciet in de transactiemonitoringregels is verwerkt, levert dit geen melding op. De toepassing van AI biedt mogelijkheden voor beide tekortkomingen aan traditionele transactiemonitoringoplossingen. Om het aandeel onterechte meldingen omlaag te krijgen is het noodzakelijk om meer terechte meldingen te genereren en tegelijkertijd minder onterechte meldingen te maken. Om onbekend gedrag toch te detecteren zijn er specifieke AI-toepassingen die afwijkingen (zogenaamde *outliers*) kunnen detecteren zonder dat de mens de computer exact dient te vertellen waarnaar gezocht moet worden.

Een *random forest classifier*[9] is een voorbeeld van een AI-techniek die gebruikmaakt van *supervised learning* en kan helpen om meer gericht terechte transactie-monitoring-alerts te genereren of gegenereerde *false positives* op een geautomatiseerde wijze af te handelen. Deze techniek leert van trainingsdata, historische alerts, door automatisch beslisbomen te maken om historische terechte meldingen van onterechte meldingen te scheiden. Zodra deze beslisbomen zijn gemaakt, kunnen ze gebruikt worden om het huidige transactiegedrag van cliënten te monitoren. Indien het gedrag van een cliënt, volgens de beslisboom, vergelijkbaar is met een groep van alerts die in het verleden beschouwd zijn als terechte alerts, dan is dat een reden om aan te nemen dat ook voor dat gedrag een alert aangemaakt moet worden. Ook indien het huidige gedrag van de cliënt niet voldoet aan de voorwaarden van de traditionele transactiemonitoringregels. Deze techniek kan ook omgekeerd ingezet worden: als er alerts gegenereerd worden door de traditionele transactiemonitoringregels, maar de beslisboom groepeert deze vooral met historische *false positives*, dan kan er onder bepaalde voorwaarden voor worden gekozen deze alerts automatisch te laten sluiten door het systeem. Hierbij kan het gevolgde pad langs de beslisboom laten zien welke eigenschappen van de transactie of de cliënt eraan bijdragen dat de alert waarschijnlijk een *false positive* betreft. Deze eigenschappen kunnen vervolgens opgenomen worden in de rationale bij het sluiten van de alert. Een beslisboom is ook voor mensen een begrijpelijk concept. De transparante terugkoppeling is ook het grote voordeel van de *random forest classifier*.

Voor het detecteren van *false negatives*, mogelijk ongebruikelijke transacties waarvoor geen alert is gegenereerd, kunnen AI-technieken op het gebied van *anomaly*-detectie een belangrijke rol spelen

[8] DNB, 'Leidraad Wwft en SW', versie december 2019, toezicht.dnb.nl.
[9] 'Random forest', wikipedia, en.wikipedia.org.

Voor het detecteren van *false negatives*, mogelijk ongebruikelijke transacties waarvoor geen alert is gegenereerd, kunnen AI-technieken op het gebied van *anomaly*-detectie een belangrijke rol spelen.[10] Dit zijn algoritmes die vergelijkbaar gedrag clusteren. Hierbij wordt uitgegaan van de premisse dat afwijkend gedrag niet per se betekent dat er sprake is van een ongebruikelijke transactie, maar dat het risico hierop wel groter is dan wanneer het gedrag in lijn was met het gemiddelde gedrag in het cluster. Indien iemand ongebruikelijk gedrag vertoont, is de verwachting dat een dergelijk algoritme dit gedrag niet of nauwelijks kan clusteren met bijvoorbeeld andere cliënten, die als groep samen 'normaal gedrag' vertonen. Voor deze cliënten die niet onderdeel zijn van een (groot) cluster kunnen alerts aangemaakt worden.

Naast de hierboven beschreven technieken zijn er nog veel meer manieren om AI in te zetten om de transactiemonitoring nog effectiever te maken. Hierbij kan gedacht worden aan technieken voor het automatisch *tunen* van de in gebruik zijnde *thresholds*. Ook leveren AI-technieken een grote toegevoegde waarde waar het gaat om het onderzoeken van bijvoorbeeld witwasnetwerken. Dergelijke samenwerkingsverbanden zijn met het blote oog moeilijk te doorzien, maar met behulp van AI-technieken, al dan niet grafisch, inzichtelijk te maken. Dit heeft een toegevoegde waarde als de gegevens van verschillende financiële instellingen samengebracht worden, zoals bij Transactie Monitoring Nederland (TMNL).

5 Sanctiefiltering

Zoals wordt gesteld in de Leidraad Financiële Sanctie-regelgeving[11], geldt in Nederland een *principle-based* benadering voor het naleven van de Sanctiewet. Dat wil zeggen dat het doel van de wet duidelijk geformuleerd is: er mogen geen transacties worden uitgevoerd met (rechts) personen genoemd in de sanctieregelgeving, maar de manier waarop een bank daar invulling aan geeft inclusief de interne procedures en controles moet door een financiële instelling zelf worden bepaald.

> Het is gebruikelijk dat Nederlandse banken hun in- en uitgaande transacties tegen de van toepassing zijnde sanctielijsten houden voor ze de transactie verwerken

Het is gebruikelijk dat financiële instellingen hun in- en uitgaande transacties tegen de van toepassing zijnde sanctielijsten houden voor ze de transactie verwerken. Immers, indien dit na het uitvoeren van de transactie plaatsvindt, kan een bank al in overtreding zijn.

Financiële instellingen wereldwijd gebruiken elektronische communicatienetwerken, zoals SWIFT, voor het onderling sturen van berichten. Een voorbeeld van zo'n bericht is het type SWIFT MT103 dat wordt gebruikt voor een eenmalige betaling.[12] Elk berichttype is weer verder opgedeeld in velden, zogeheten *tags*. Zo is er een veld voor het bedrag van de transactie en de naam van de begunstigde. In SWIFT worden in berichten echter nog veel verschillende typen informatie bij elkaar in één veld gestopt, zoals bijvoorbeeld straat en land. Dit kan betekenen dat het veld met adres-informatie Cuba Street, Wellington, Nieuw-Zeeland bij het screenen tegen een sanctielijst een alert kan genereren tegen het land Cuba. Met behulp van *supervised learning* kan een AI-techniek ingezet worden die wordt getraind om te herkennen welk deel van de tekst het adres, de plaats of het land betreft.

De SWIFT-berichttypes in de serie MT700 wordengebruikt voor transacties ten behoeve van handelsfinancieringen, zoals het importeren en exporteren van goederen. Deze transacties worden vaak ondersteund door documenten, zoals vrachtbrieven, die de details van de transactie en

[10] G. Palshikar, M. Apte en S. Baskaran, 'Analytics for Detection of Money Laundering', TACTiCS 2014.
[11] Ministerie van Financiën, 'Leidraad Financiële Sanctieregelgeving', 12 augustus 2020, Rijksoverheid. nl.
[12] SWIFT, 'Standards MT', swift publications november 2019, swift.com.

> Bij veel compliance-afdelingen wordt het hebben van 90% *false positives* van de alerts als acceptabel gezien

> Daarmee is de inzet van AI de enige serieuze oplossing om de crisis te bestrijden

goederen bevatten. Deze documenten vereisen vaak handmatige screening. Er zijn echter in toenemende mate slimme technieken beschikbaar die dit kunnen verge-makkelijken, bijvoorbeeld *Optical Character Recognition* (OCR).[13] Dit is een techniek om tekst uit een afbeelding of document te digitaliseren. Uit de gedigitaliseerde tekst kunnen vervolgens geautomatiseerd de entiteiten en locaties worden herkend die dan tegen de sanctielijsten kunnen worden aangehouden. OCR kan zowel samenwerken met *supervised* als met *unsupervised* AI-technieken.

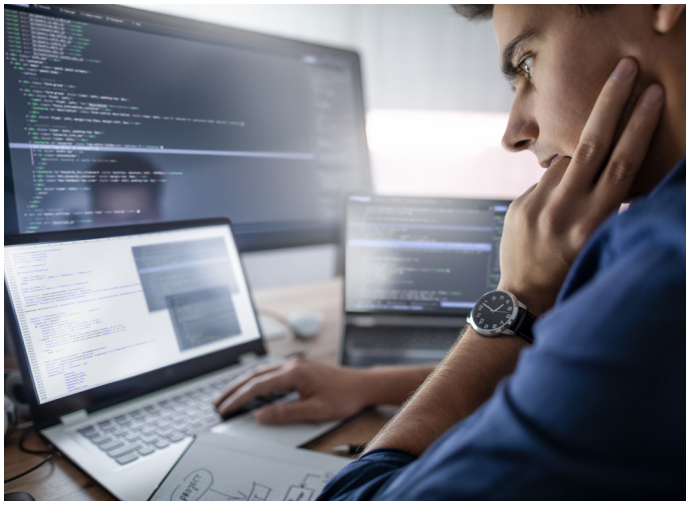
Bij transactiefiltering worden veel alerts gegenereerd die voor het menselijk oog duidelijk *false positives* betreffen. Bij veel compliance-afdelingen wordt het hebben van 90% *false positives* van de alerts als acceptabel gezien.[14] Er is dan ook veel winst te behalen door de alert afhandeling op een intelligentere manier uit te voeren. Zoals in de paragraaf over transactiemonitoring ook al beschreven, kan dat bijvoorbeeld met behulp van *supervised learning*-technieken als *random forest classification*.

Naast de hierboven beschreven technieken kunnen AI-technieken op vele andere manieren een belangrijke rol spelen in het effectiever voldoen aan compliance op het gebied van sancties. Het gaat daarbij bijvoorbeeld om het bewerken en consolideren van sanctielijsten en het automatisch voorstellen van zogenaamde *good guy* of normalisatieregels.

6 Wat zijn de voor- en nadelen van het inzetten van AI?

Enerzijds kan door de inzet van AI een enorme kostenbesparing worden gerealiseerd. De inzet van techniek kan een deel van de activiteit van de vele analisten vervangen. Daarnaast is de techniek in staat om bepaalde activiteiten nauwkeuriger en met een hoger kwaliteitsniveau uit te voeren. Daarmee is de inzet van AI de enige serieuze oplossing om de crisis te bestrijden.

Daar staat tegenover dat de inzet van AI op de korte termijn vraagt om aanvullende inspanningen op andere vlakken. Met name het investeren in de juiste techniek, kennis en ervaring zal een grote kostenpost zijn en vragen om een andere manier van denken en werken. Daar komt bij dat met name het goed inregelen van een model dat gebruikmaakt van intelligente technieken tijd kost en het even duurt voordat de eerste echte resultaten zichtbaar worden.



[13] J. Memon, M. Sami & R. A. Khan, 'Handwritten Optical Character Recognition (OCR): A Comprehensive Systematic Literature Review (SLR)', https://arxiv.org/ pdf/2001.00139.pdf.

[14] A. Swift & D. Dekhtyar-McCarthy, 'Challenging the Status Quo: Sanctions Screening', ACAMS Today 12 december 2019, acamstoday.org.

De exacte werking van AI-technieken is soms moeilijk te doorgronden en de vele instellingen en parameters van deze technieken maken deze oplossingen soms moeilijk beheersbaar voor de compliance officer. Daarmee vraagt de beheerste inzet van AI voor de bestrijding van FEC om specifieke expertise op het snijvlak van techniek en compliance. Deze aanvullende investeringen verdienen zich op de lange termijn zeker terug, doordat met behulp van AI-technieken makkelijker ingesprongen kan worden op een situatie die verandert en minder mankracht nodig zal zijn om de risico's op een meer effectieve manier te beheersen.

Ook spelen ethische afwegingen een rol bij het zorgvuldig implementeren van AI-technieken. Recent hebben we in het nieuws[15] gezien dat de inzet van algoritmen het risico op bijvoorbeeld discriminatie met zich meebrengt. Grip krijgen op de risico's daaromtrent is noodzakelijk om AI-technieken goed en succesvol in te zetten.[16]

Een ander nadeel dat zich voordoet bij AI-technieken is dat de kwaliteit van de brondata een grote rol speelt in de kwaliteit van de resultaten en dat de datakwaliteit bij veel financiële instellingen ruimte heeft voor verbetering. Het kan een uitdaging zijn om voldoende data met de juiste kwaliteit voor de toepassingen bij elkaar te krijgen. Dit geldt bijvoorbeeld voor informatie over de alert afhandeling. Om te kunnen leren van historische voorbeelden is het voor de effectieve inzet van sommige AI-technieken belangrijk om te weten welke alerts als onderzoekswaardig werden beschouwd, welke alerts zijn gemeld en welke alerts oninteressant zijn. Indien onvoldoende detailinformatie beschikbaar is over de alertafhandeling of wordt getwijfeld over de kwaliteit daarvan, kan worden geïnvesteerd om dit soort datalabels alsnog beschikbaar te maken. Dat is een stuk lastiger als het gaat om informatie die niet binnen de financiële instelling aanwezig is, zoals bijvoorbeeld informatie over de cliënt. In dat geval zal de informatie waarschijnlijk in de loop der tijd opgebouwd moeten worden.

De inzet van AI kan de nauwkeurigheid, volledigheid en daarmee de kwaliteit van de uitgevoerde werkzaamheden vergroten. Voor mensen kan het soms (erg) lastig zijn om grote hoeveelheden informatie tegelijk goed te overzien. Denk bijvoorbeeld aan een AML-transactiemonitoringalert die is gegenereerd omdat een cliënt in een maand tijd een uitzonderlijk hoog transactieverkeer laat zien vergeleken met de 12 maanden daarvoor. De transactiemonitoringtool zal aangeven dat er een afwijkend patroon is, welke maand dat betreft en wat het aantal en de omvang van de transacties is. Tevens worden alle transacties voor de betreffende maand getoond. Het kan daarbij soms om honderden transacties gaan, waardoor je je af kunt vragen of een dergelijke alert goed door het menselijk oog beoordeeld kan worden. Een oplossing waarbij AI wordt ingezet, kan de patronen in de honderden transacties in de alert waarschijnlijk beter doorgronden en op die manier tot een meer overwogen beslissing over de alert komen.

Echter, de inzet van AI-technieken kan functioneren als een *black box*. De technieken en de resultaten die daarmee samenhangen zijn soms moeilijk te doorgronden en te interpreteren. Bij de inzet van intelligente technieken om ongebruikelijke transacties te detecteren is het daarom soms niet duidelijk waarom de techniek een bepaalde transactie heeft aangemerkt als mogelijk ongebruikelijk. Terwijl deze achterliggende reden nodig is om de alert goed te kunnen beoordelen. In de wereld van de AI wordt het probleem van deze onnavolgbaarheid herkend, daarom zijn er andere technieken ontwikkeld die de uitkomst trachten te verklaren. Daarmee kan alsnog een indicatie worden gegeven van de kenmerken op basis waarvan de transactie als mogelijk ongebruikelijk is aangemerkt.

De traditionele manier om het risico op FEC te mitigeren is door de risico's die bijvoorbeeld zijn geïdentificeerd in de systematische integriteitsrisico-analyse in kaart te brengen. Daarbij wordt nagedacht over mogelijke risico's en hoe die risico's gemitigeerd kunnen worden. De kracht van AI ligt vervolgens in het detecteren van mogelijke onregelmatige transacties voor nieuwe patronen. Met behulp van AI kunnen we ook op zoek gaan naar de zaken waarvan we niet weten dat we ze niet weten – de grote onbekende. Op die manier kunnen nieuwe scenario's en bijvoorbeeld nieuwe witwaspatronen worden ontdekt, die voor het menselijk oog moeilijk op een andere manier te doorgronden zijn. Voor de risico's die niet zijn geïdentificeerd kunnen financiële instellingen de rol van poortwachter echter veel beter invullen door gebruik te maken van AI.

In de wereld van de AI wordt het probleem van deze onnavolgbaarheid herkend, daarom zijn er andere technieken ontwikkeld die de uitkomst trachten te verklaren

[15] J. Schellevis & W. de Jong, 'Overheid gebruikt op grote schaal voorspellende algoritmes, 'risico op discriminatie'', NOS 29 mei 2019, nos.nl.
[16] M. Kaptein & W. Touw, 'Zo krijgt u zicht op de ethische risico's van algoritmen', Nationaal register 8 september 2020, nationaalregister.nl.

7 Conclusie

De huidige aanpak bij het beheersen van risico's op het gebied van FEC heeft tot een crisis geleid, doordat er een toenemend aantal analisten ingezet moet worden. Om dit proces slimmer en efficiënter te kunnen inrichten is het inzetten van AI onvermijdelijk. Het is niet de vraag of AI van toegevoegde waarde is bij compliancevraagstukken, maar op welke termijn AI zal worden geïmplementeerd.

Hoewel het inzetten van AI onvermijdelijk is, zal dit niet betekenen dat er geen menselijk oog meer aan te pas komt. Analisten blijven gewoon nodig, al is het in veel kleinere aantallen en om, ondersteund door AI, de echt onderzoekswaardige cases te bekijken. Daarnaast is een andere expertise nodig en die ligt op het snijvlak van compliance en techniek.

Het goed inzetten van AI-technieken op het gebied van FEC vraagt naast een bepaalde expertise ook om goede brongegevens en tijd om de algoritmen goed te kunnen trainen. De analisten van vandaag zorgen voor een dataset met historische voorbeelden waarop getraind kan worden. De inzet van AI is niet in alle gevallen de heilige graal, maar het is wel een antwoord op de crisis.

Ieder zijn voordelen – laat de mens doen waar hij goed in is, maar maak ook gebruik van intelligente technieken voor werkzaamheden waar dat betere en efficiëntere resultaten oplevert.

Dit artikel is eerder verschenen in Tijdschrift voor Compliance - december

Meer informatie?

Renske van Hooff

Director KPMG
E vanhooff.renske@kpmg.nl

Jori van Schijndel

Manager KPMG
E vanschijndel.Jori@kpmg.nl

Monica van Santbrink

Senior Consultant KPMG
E vansantbrink.monica@kpmg.nl

kpmg.nl