E. Digitalisatie

Het jaar 2020 werd gekenmerkt door een versnelling van de digitale toegang tot financiële diensten, digitale en contactloze betalingen, e-commerce en het gebruik van digitale infrastructuur, waardoor de consumenten, werknemers en ondernemingen beter gewapend waren om het hoofd te bieden aan de situatie zonder precedent die door de COVID19-pandemie is ontstaan. De veiligheid en de continuïteit van de digitale infrastructuur van de financiële sector zijn aldus nog crucialer geworden en het belang van digitale innovatie als bron van economisch herstel is duidelijker geworden met de snellere ontwikkeling van vormen van consumptie op afstand. In de innovatie op het gebied van digital finance hebben er zich verschillende ontwikkelingen voorgedaan. Voorbeelden hiervan zijn nieuwe bedrijfsmodellen die gebaseerd zijn op innovatieve betaaloplossingen, het streven naar verbetering van de operationele efficiëntie door gebruik te maken van kunstmatige intelligentie, *Machine/Deep Learning* of *Robotic Process Automation*, het verfijnen van de commerciële strategieën met behulp van gegevensanalyse en kunstmatige intelligentie, en het beheer van IT-infrastructuren en de aggregatie van gegevens in de cloud. Deze ontwikkelingen zijn vaak ingegeven door de wil om vooruit te lopen op de verwachte grote veranderingen in de structuur van de markt voor financiële diensten. De rol van de financiële diensten en actoren in de wereldmarkt voor producten en diensten is op mondiaal niveau inderdaad sterk aan het veranderen. Er vindt een geleidelijke verschuiving plaats naar een markt waar voor financiële en niet-financiële diensten gebruik wordt gemaakt van geïntegreerde betaal-, e-commerce- en socialemediaplatforms en van ecosystemen voor samenwerking die deze verschillende dimensies omvatten. Deze ontwikkelingen worden met name vergemakkelijkt door het gebruik van modulaire technologieën die het voor verschillende financiële en niet-financiële actoren mogelijk maken om te communiceren via interfaces (*application programming interfaces – API's*). De initiatieven met betrekking tot *global stablecoins* die betalingen in het kader van dergelijke ecosystemen en platforms zouden vergemakkelijken, nemen steeds duidelijker vormen aan. Zo heeft de Libra Association (omgedoopt tot Diem) in april 2020 een nieuwe versie van haar *white paper* gepubliceerd in een poging om de bezorgdheid van verschillende toezichthoudende instanties, centrale banken en andere betrokken partijen weg te nemen. In april 2020 heeft zij bij de Zwitserse financiële toezichthouder (*Autorité fédérale de surveillance des marchés financiers* – FINMA) een aanvraag ingediend om een vergunning te verkrijgen als betalingssysteem.

Deze ontwikkelingen scherpen nu al bepaalde risico's aan (zoals cyber- en IT-risico's) en leiden tot nieuwe risico's voor de consument, het monetair beleid en de financiële stabiliteit, of zouden op korte tot middellange termijn tot dergelijke nieuwe risico's kunnen leiden. Tegen deze achtergrond heeft de Europese Commissie een digitale strategie gepubliceerd met het oog op de bevordering van digitale innovatie, de totstandbrenging van een eengemaakte digitale markt voor financiële diensten en een Europese ruimte voor financiële data om de toegang tot en het delen van dergelijke data te stimuleren, evenals op een betere beheersing van de risico's die het gevolg zijn van de digitale innovatie. In september 2020 leidde dit tot de eerste wetgevingsinitiatieven op dit gebied, waar de Bank nauw bij betrokken is. Twee van deze initiatieven, die betrekking hebben op operationele veerkracht en cryptoactiva, worden hieronder besproken. Diverse gevolgen van deze ontwikkelingen en van het belang van digital finance, zoals de toename van cyber- en IT-risico's, open banking en de regels voor sterke cliëntauthenticatie die in de tweede richtlijn betreffende betalingsdiensten (Payment Services Directive – PSD2) zijn opgenomen, en de initiatieven met betrekking tot de digitale euro, worden eveneens hieronder behandeld.

1. Digitale operationele veerkracht

1.1 Verdere toename van cyber- en IT-gerelateerde risico's

De digitale operationele veerkracht van de financiële sector werd tijdens het verslagjaar in belangrijke mate beïnvloed door de COVID-19-pandemie. Sinds maart 2020 vragen (of verplichten) de instellingen hun medewerkers om zoveel mogelijk van thuis uit te werken, wat ongeziene uitdagingen en extra risico met zich meebrengt. Aanvankelijk waren de uitdagingen vooral van operationele aard, zoals de noodzaak om de IT-capaciteit uit te breiden om massaal telewerken mogelijk te maken. Naarmate de pandemie langer aansleept, krijgen de uitdagingen een meer strategisch karakter. Instellingen worden er bijvoorbeeld toe gedwongen te prioriteren tussen lopende en geplande strategische projecten, omdat de huidige omstandigheden vaak niet toelaten om het tempo en de mate van verandering van voor de gezondheidscrisis aan te houden. Massaal telewerken verlaagt weliswaar het gezondheidsrisico, maar doet het inherent IT- en cyberrisico toenemen, bijvoorbeeld omdat het oplossen van een incident bemoeilijkt wordt door de beperktere fysieke aanwezigheid van operatoren, maar ook door het grote aantal bedrijfscomputers dat gelijktijdig vanop afstand via het internet verbinding maakt met de instelling. Dankzij de door de instellingen genomen voorzorgsmaatregelen heeft dit in het verslagjaar gelukkig niet tot al te belangrijke operationele incidenten geleid.

De veiligheid en de continuïteit van de digitale infrastructuur van de financiële sector zijn nog crucialer geworden in 2020

Cyberaanvallen waren in de voorbije jaren hoe dan ook al wereldwijd geëvolueerd tot een dagdagelijkse realiteit. Er wordt ook vastgesteld dat aanvallers de gebruikte technieken en methodes verder aanscherpen, waardoor een deel van de aanvallen steeds gesofisticeerder en krachtiger wordt. Verwacht wordt

dan ook dat het aantal langdurige en doelgerichte cyberaanvallen in de toekomst verder zal toenemen, waarbij de financiële sector logischerwijs één van de potentiële doelwitten blijft. De lijst van wereldwijde cyberaanvallen op financiële instellingen opgesteld door de denktank 'Carnegie Endowment for International Peace' [1] schetst een actueel beeld van de cyberdreigingen voor de sector. In 2020 werden bij gerapporteerde aanvallen bijvoorbeeld gevoelige gegevens zoals kredietaanvragen en kredietkaartnummers ontvreemd, geldautomaatsystemen ontwricht en frauduleuze transacties geïnitieerd via inbraak in serversystemen van banken.

In deze omstandigheden is het voor de financiële instellingen en infrastructuren uitdagend om hun IT-systemen, -data en -diensten adequaat te beveiligen tegen de diverse aanvallen. Omdat cyberdreigingen zeer snel evolueren, moet er meer dan ooit over gewaakt worden dat de defensiecapaciteit van de instellingen en FMI's het mogelijk maakt flexibel in te spelen op veranderende aanvalspatronen. Oplossingen voor het verzamelen van informatie over potentiële bedreigingen, aanvallers en aanvalstypes zijn hierbij essentieel. Verder is het belangrijk dat niet enkel de externe netwerkperimeter van een instelling adequaat wordt beveiligd, maar dat ook de interne maatregelen voldoende fijnmazig zijn en in meerdere 'lagen' worden uitgewerkt. Voor financiële instellingen is het ook nuttig om het risicoprofiel van de cliënt en/of tegenpartij te kennen bij het bepalen van het risico op fraude bij bepaalde transacties. In het kader van particulier bankieren wordt daarvoor gebruikgemaakt van beveiligingsmechanismen die geïntegreerd zijn in de applicatie voor internet- of mobiel bankieren. In de context van de activiteiten van correspondentbanken kan als voorbeeld het Customer Security Programme (CSP) worden genoemd, dat uitgerold werd door SWIFT om financiële instellingen te ondersteunen bij de risicobeoordeling van tegenpartijen in het berichtenverkeer. Dit CSP benadrukt tevens het belang van een frequente reconciliatie van uitgaande transacties, wat toelaat om potentieel frauduleuze activiteiten tijdig te detecteren en waar nodig stop te zetten voor de eindbestemming bereikt wordt.

1 Zie https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

Naast cyberrisico brengt de sterke afhankelijkheid van IT-oplossingen in de financiële sector ook andere uitdagingen met zich mee. Traditionele instellingen worden onder druk gezet door innovatieve spelers, toegenomen verwachtingen van cliënten betreffende de aangeboden diensten en beschikbaarheid of door toenemende veiligheidsrisico's (bijvoorbeeld door het gebruik van niet langer ondersteunde "End-of-Life"-software), om hun soms sterk verouderde IT-architecturen op relatief korte termijn te vernieuwen, maar de complexiteit van hun IT-landschap maakt het tot een grote uitdaging om dit op een economisch verantwoorde manier te realiseren. Tevens is het risico van een toenemende afhankelijkheid van derde partijen voor informaticadiensten en van andere gestandaardiseerde informatiesysteemcomponenten sterk aanwezig. Met name cloudoplossingen worden steeds meer en voor steeds belangrijker processen aangewend. Deze ontwikkeling draagt er ook toe bij dat op sectorniveau een beperkt aantal kritieke dienstverleners een alsmaar toenemend concentratierisico voor de financiële industrie vertegenwoordigen. Ook het voldoende uitgebreid testen van ontwikkelde software en hersteloplossingen voor een waaier aan extreme maar plausibele scenario's blijft een belangrijk aandachtspunt.

Het is dan ook van belang dat de bestuursorganen van de financiële actoren over de nodige expertise en informatie beschikken om de risico's op passende wijze te kunnen opvolgen, en dat ze adequate maatregelen opnemen in hun strategische planning om de risico's binnen aanvaardbare perken te houden. Heel wat instellingen geven echter aan dat zij moeilijkheden ondervinden om voldoende mensen aan te werven met de juiste vaardigheden en expertise. Daarnaast dienen alle medewerkers van deze ondernemingen zich bewust te zijn van het cyber- en IT-risico, zodat zij begrijpen hoe deze risico's kunnen optreden en hoe zij verwacht worden te reageren.

1.2 Richtsnoeren en ontwikkelingen op wetgevend vlak

De Bank heeft de afgelopen jaren in belangrijke mate bijgedragen aan de ontwikkeling van een regelgevend kader om de beheersing van cyber- en IT-risico's te verbeteren. De prudentiële circulaire betreffende de verwachtingen van de Bank op het vlak van de operationele bedrijfscontinuïteit en de

beveiliging van systeemrelevante instellingen [1] is nog steeds een belangrijke referentie. Verder draagt de Bank actief bij tot de totstandkoming van een Europees regelgevend kader voor het beheer van cyber- en IT-risico's. In de schoot van de EBA resulteerde dit achtereenvolgens in de publicatie van richtsnoeren voor toezichthouders betreffende de beoordeling van het ICT-risico in het kader van het SREP [2], richtsnoeren met betrekking tot uitbesteding [3] en richtsnoeren met betrekking tot het beheer van ICT- en beveiligingsrisico's [4]. Deze richtsnoeren werden ondertussen allemaal geïntegreerd in het toezichts- en beleidsraamwerk van de Bank. Ook voor verzekeringsondernemingen draagt de Bank bij tot de totstandkoming van een soortgelijk reglementair kader onder de auspiciën van EIOPA. In 2020 werden de richtsnoeren met betrekking tot uitbesteding aan aanbieders van clouddiensten [5] omgezet in een NBB-circulaire, en werden er richtsnoeren met betrekking tot ICT-beveiliging en governance [6] gepubliceerd.

In september 2020 publiceerde de Europese Commissie een voorstel voor een verordening, de zogenaamde "Digital Operational Resilience Act" (DORA). Dit voorstel heeft als doel de risico's die gepaard gaan met de digitale transformatie van de financiële industrie te matigen door strikte en gemeenschappelijk regels op te leggen met betrekking tot ICT-governance en risicobeheer, ICT-incidentrapportering en informatiedeling, veiligheidstests en derdepartijrisico op het vlak van ICT. Deze regels zouden gelden voor een brede waaier aan financiële instellingen, maar ook voor kritieke ICT-leveranciers (third-party providers), bijvoorbeeld aanbieders van clouddiensten, die onderworpen zouden worden aan een vorm van oversight. De Bank speelt als lid van de Belgische delegatie een belangrijke adviserende rol tijdens de besprekingen van de ontwerpteksten op Europees vlak, en zal vermoedelijk ook intensief betrokken worden bij de latere omzetting van de Europese DORA-verordening in technische standaarden.

1 Circulaire NBB_2015_32 van 18 december 2015 betreffende aanvullende prudentiële verwachtingen op het vlak van de operationele bedrijfscontinuïteit en beveiliging van systeemrelevante instellingen.
2 EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP) (mei 2017).
3 EBA Guidelines on outsourcing arrangements (februari 2019).
4 EBA Guidelines on ICT and security risk management (november 2019).
5 EIOPA Guidelines on outsourcing to cloud service providers (februari 2020).
6 EIOPA Guidelines on information and communication technology security and governance (oktober 2020).

1.3 Operationele activiteiten

De beoordeling en de bevordering van de beheersing van cyber- en IT-risico's zijn topprioriteiten voor de Bank en de Europese en internationale samenwerking wordt in dit verband steeds belangrijker. De aandacht gaat hierbij enerzijds uit naar de beveiliging van en het vertrouwen in individuele financiële instellingen of FMI's, en anderzijds naar sectoroverschrijdende beheersingsstrategieën.

De benadering voor de individuele instellingen is tweeledig. Enerzijds dienen de instellingen onderworpen aan prudentieel toezicht eigen vermogen aan te houden ter dekking van hun operationele risico's, waaronder cyber- en IT-risico's. Anderzijds wordt nauw toegezien op de operationele veiligheid en robuustheid van de kritieke processen bij de financiële instellingen en FMI's. De beschikbaarheid, integriteit en vertrouwelijkheid van de IT-systemen en -data staan hierbij centraal. De Bank voerde in 2020 diverse inspectieopdrachten uit (voor banken in het kader van het SSM) om na te gaan of het regelgevend kader wordt nageleefd en of de IT-systemen met betrekking tot het cyber- en IT-risico adequaat worden beheerd. Daarnaast volgt zij deze risico's op bij de financiële instellingen en FMI's in het kader van haar permanente en periodieke toezichtswerkzaamheden. Door de COVID-19-gezondheidscrisis was de Bank genoodzaakt haar aanpak voor deze toezichtsactiviteiten te herzien. Enerzijds werden activiteiten inhoudelijk aangepast aan de nieuwe realiteit, met specifieke aandacht voor COVID-19, anderzijds werd ook de werkwijze aangepast, waarbij waar mogelijk ingezet werd op vergaderingen op afstand en technologische hulpmiddelen.

In 2018 heeft de Bank een raamwerk voor ethische hacking opgezet, namelijk TIBER-BE (Threat Intelligence Based Ethical Red Teaming Belgium). Dit programma is het Belgische onderdeel van een methodologie die werd ontwikkeld door het Eurosysteem, en beoogt via gesofisticeerde tests de cyberweerbaarheid van individuele FMI's en financiële instellingen te verhogen, alsook tot belangrijke inzichten te komen met betrekking tot de cyberbeveiliging van de Belgische financiële sector in zijn geheel. De Bank stimuleert deze oefeningen vanuit haar rol als bewaker van de financiële stabiliteit. Gedurende het rapporteringsjaar werd op de website van de Bank een geactualiseerde versie van het TIBER-BE-raamwerk gepubliceerd, waarin de

methodologie verder wordt verfijnd op basis van ervaringen uit reeds afgeronde tests. De sector blijkt overtuigd te zijn van de deugdelijkheid van de toegepaste methodologie en van de meerwaarde die deze specifieke tests bieden. Het TIBER-BE-team heeft ondertussen ook met succes grensoverschrijdende tests uitgevoerd, in nauwe en goede samenwerking met andere EU-landen die het TIBER-raamwerk geïmplementeerd hebben, alsook met het Verenigd Koninkrijk, waarbij gezocht werd naar synergieën met het soortgelijke CBEST-raamwerk. TIBER-BE opereert nu op kruissnelheid.

De Bank besteedt ook in toenemende mate aandacht aan sectorbrede initiatieven. In het kader van het SSM worden bijvoorbeeld op regelmatige basis transversale analyses uitgevoerd met betrekking tot cyber- en IT-gerelateerde thema's. Zo werd alle significante banken alsook een aantal minder significante banken in 2020 opnieuw gevraagd om een IT-vragenlijst in te vullen die belangrijke informatie verschaft voor het jaarlijkse 'Supervisory Review and Evaluation Process', en die toelaat transversale analyses uit te voeren. Ook een groot aantal verzekeringsondernemingen en beursvennootschappen werd gevraagd soortgelijke informatie te verschaffen met een vergelijkbare doelstelling.

Vanuit haar rol als sectorale autoriteit voor de toepassing van de wet ter beveiliging en bescherming van kritieke infrastructuren (voornamelijk systeemrelevante banken en FMI's), beoordeelt de Bank tevens de doeltreffendheid van controlesystemen bij de kritieke financiële infrastructuren. Eveneens in deze context organiseert en coördineert de Bank sectorbrede crisissimulatieoefeningen, om de Belgische financiële sector voor te bereiden op potentiële operationele incidenten met een systemisch karakter. In het kader van de wet ter beveiliging van netwerk- en informatiesystemen (NIS) fungeert de Bank als sectoraal meldpunt voor grote incidenten in de financiële sector.

2. FinTech

2.1 Sterke cliëntauthenticatie en 'open banking'

De belangrijkste toezichtsactiviteit op het vlak van de betalingen bestond enerzijds in de opvolging van de verscherpte beveiligingseisen voor het elektronisch betaalkaartverkeer in de sector van de onlinehandel en anderzijds in de facilitering van de toegang van FinTech-spelers tot de betaalrekeningsystemen van de kredietinstellingen.

2.1.1 Sterke cliëntauthenticatie: voort te zetten werkzaamheden

De invoering van de regels betreffende sterke cliëntauthenticatie (hierna: 'SCA') in september 2019 leidde tot een aantal implementatieproblemen voor de sector van de online kaartbetalingen (elektronische handel).

Enerzijds dienen de uitgevers van betaalkaarten (vnl. kredietinstellingen) hun procedures voor het authenticeren van betaalkaarten in sommige gevallen aan te passen om in overeenstemming te zijn met deze regels en anderzijds dienen kaarttransacties online als regel nu geauthenticeerd te worden, wat niet altijd gebeurde. Dit laatste vereist de invoering van nieuwe technische protocollen in een complex ecosysteem met talrijke spelers. Deze protocollen maken het authenticeren, evenals het correct gebruik maken van de voorziene wettelijke uitzonderingen op de regel van verplichte sterke cliëntauthenticatie mogelijk en zorgen ervoor dat alle spelers in de sector iedere kaarttransactie correct kunnen authenticeren.

De verscherpte beveiligingseisen voor het elektronisch betaalkaartverkeer en de toegang van FinTech-spelers tot de betaalrekeningsystemen zijn nauwlettend opgevolgd

De aanpassingen die vereist zijn van de kant van de online handelaren om deze protocollen tijdig en volledig te ondersteunen via hun websites, teneinde het authenticeren van kaarttransacties mogelijk te maken, vormen een bijzondere uitdaging voor de sector. Aangezien die Belgische betaalkaarthouders online handel drijven met buitenlandse handelaren in de ons omringende landen, is het migreren naar SCA door deze handelaren tevens een cruciale factor voor het slagen van deze migratie in België.

Teneinde deze migratie in goede banen te leiden en in lijn met de EBA-Opinie ter zake, verleende de Bank reeds in augustus 2019 uitstel van implementatie aan de Belgische betaalkaartindustrie voor de regels inzake SCA en werkte zij in overleg met de sector, onder leiding van Febelfin, een nationaal migratieplan uit. Dit plan werd reeds in mei 2020 op de website van de Bank gepubliceerd. Het nationaal migratieplan koos resoluut voor een graduele overgang naar het volledig toepassen van SCA op iedere kaarttransactie. Tijdens een overgangsperiode zal er een systeem van zogenaamde 'zachte weigeringen' van kaarttransacties worden gehanteerd, wat inhoudt dat een kaarttransactie boven een bepaald bedrag (bijvoorbeeld EUR 1.500) die zou worden aangeboden bij de kaartuitgever door een online handelaar (en diens acquirer) zonder authenticatie van de kaarthouder, geweigerd wordt met de vraag om deze opnieuw door te sturen naar de kaartuitgever maar ditmaal mét authenticatie van de kaarthouder. De kaarthouder zelf merkt helemaal niets van deze 'zachte weigering', tenzij de handelaar de nodige protocollen nog niet heeft geïntegreerd in zijn webshop en de transactie derhalve geheel niet kan doorgaan ('harde weigering'). De drempelbedragen voor de toepassing van deze procedure dalen tijdens de overgangsperiode geleidelijk, totdat op het einde van deze periode volledige overeenstemming met de regels inzake SCA wordt bereikt.

De Bank volgt de implementatie van dit migratieplan actief op, in samenwerking met de sector, en stuurt indien nodig bij. Zij houdt hierbij rekening met parameters, zoals de ervaring van Belgische kaartuitgevers met het gradueel aanscherpen van de regels voor authenticatie overeenkomstig het migratieplan en de snelheid waarmee online handelaren in het binnen- en buitenland naar de vereiste technische protocollen migreren.

2.1.2 Open Banking: toegang tot betaalrekeningsystemen

Een tweede belangrijke toezichtsactiviteit in 2020 bestond uit het opvolgen van de naleving van de regels omtrent de toegang voor FinTech-spelers tot betaalrekeningen bij kredietinstellingen.

De betalingsdienstenrichtlijn PSD2 voerde immers twee nieuwe categorieën gereguleerde dienstverleners

in, namelijk betalingsinitiatie- en rekeninginformatiedienstverleners (samen *'derde partijen'* genoemd), die na het verkrijgen van respectievelijk een vergunning en een erkenning van de Bank (of een andere bevoegde autoriteit in de EER) het recht hebben om, middels de toestemming van de rekeninghouder(s), respectievelijk een betaling te initiëren op en rekeninginformatie te aggregeren van betaalrekeningen bij kredietinstellingen.

Om dit technisch mogelijk te maken voor deze derde partijen, dienen de kredietinstellingen een technisch toegangskanaal te creëren (*'speciale interface'),* waarvan deze partijen gebruik kunnen maken om hun diensten aan te bieden. De specifieke technische vereisten werden vastgelegd in de technische standaard i.v.m. SCA & CSC[1], die in werking trad op 14 september 2019.

In 2020 stelde de EBA vast dat er nog onduidelijkheid bestond op de markt omtrent de interpretatie van het verbod op het opwerpen van of voorzien in obstakels voor deze derde partijen in de technische werking van deze speciale interface(s). Dit resulteerde in juni 2020 in een EBA-Opinie omtrent obstakels en de verwijdering daarvan.

De Bank onderschreef deze EBA-Opinie en verduidelijkte in een Mededeling dd. 1 juli 2020 dat zij zich op deze EBA-Opinie baseert voor haar interpretatie van het verbod op obstakels voor derde partijen en dat zij verwacht dat kredietinstellingen tegen 31 december 2020 alle obstakels uit hun speciale interface(s) verwijderen. De Bank volgt de verwijdering van deze obstakels actief op bij de kredietinstellingen en verschaft waar nodig nadere technische uitleg.

2.2 De digitale euro

De Europese centrale banken bestuderen de verschillende toekomstscenario's waarin de uitgifte van een digitale euro, een elektronische vorm van centralebankgeld (CBDC), aanbevolen of noodzakelijk is. Voorbeelden van deze toekomstscenario's zijn een sterke afname van cash als betalingsmiddel, een belangrijke toename in het gebruik van niet-gereglementeerde betalingsmiddelen dat resulteert in een significant risico voor de financiële stabiliteit en de consumentenbescherming of een belangrijke toename van het gebruik van digitale munten uitgegeven door buitenlandse centrale banken die de positie van de euro ondermijnt.

In oktober publiceerde de ECB samen met de experts van de 19 nationale centrale banken in het eurogebied een rapport dat de geïdentificeerde toekomstscenario's opsomt en evalueert. Daarnaast bevat het rapport ook enkele basisprincipes voor een eventuele uitgifte. Een digitale euro kan enkel een aanvulling zijn op de bestaande betalingsmiddelen (bijvoorbeeld cash) en mag privé-initiatieven niet ontmoedigen of verdringen. Er werd nog geen beslissing genomen met betrekking tot de uitgifte van een digitale euro.

2.3 Voorstel voor een Europese verordening betreffende markten in cryptoactiva (MiCA)

In september 2020 publiceerde de Europese Commissie een voorstel voor een verordening betreffende markten in cryptoactiva (MiCA). Dit voorstel maakt deel uit van de digitale strategie van de Commissie.

Met deze verordening beoogt zij een kader te scheppen voor cryptoactiva die niet als financiële instrumenten, elektronisch geld, deposito's, gestructureerde deposito's of effectiseringsinstrumenten kwalificeren en voor cryptoactivadiensten die niet onder de bestaande regels vallen.

Het eerste deel van het voorstel bevat regels die betrekking hebben op de aanbieding van bepaalde cryptoactiva en de toelating ervan tot de handel op een handelsplatform op het grondgebied van de Unie evenals op de emittenten van cryptoactiva. Deze regels verschillen naar gelang van de categorie cryptoactiva. In de MiCA worden drie categorieën cryptoactiva onderscheiden : 1° cryptoactiva die worden gedekt door een valuta die een wettig betaalmiddel is en waarvan de emittent een kredietinstelling of een instelling voor elektronisch geld is (*e-money tokens*), 2° activa die worden gedekt door diverse valuta die een wettig betaalmiddel zijn, één of meer grondstoffen of één of meer cryptoactiva of een combinatie van deze activa en die een stabiliseringsmechanisme omvatten (*asset-referenced tokens*), 3° overige cryptoactiva, die niet tot de eerste twee categorieën cryptoactiva behoren. De eerste twee categorieën activa zijn met name

1 Gedelegeerde Verordening (EU) 2018/389 van de Commissie van 27 november 2017 tot aanvulling van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad wat betreft technische reguleringsnormen voor sterke cliëntauthenticatie en gemeenschappelijke en veilige open communicatiestandaarden.

bedoeld voor emittenten van *stablecoins*, terwijl de derde categorie beantwoordt aan de doelstelling van de verordening om een kader te scheppen voor alle cryptoactiva (die niet reeds aan bestaande regelgeving zijn onderworpen), van welke aard ook, die door een emittent zijn uitgegeven. Voor de eerste twee categorieën activa moet de emittent voorafgaandelijk een vergunning hebben verkregen. De MiCA voorziet in de regeling van deze vergunning voor de *asset-referenced tokens,* terwijl ze voor de *e-money tokens* is opgenomen in de richtlijnen die op de betrokken instellingen van toepassing zijn. Voor *asset-referenced tokens* moet het *white paper*[1] voorafgaandelijk worden goedgekeurd, terwijl het *white paper* voor *e-money tokens* voorafgaandelijk ter kennis moet worden gebracht. Voor de categorie van de overige activa daarentegen moet het *white paper* voorafgaandelijk ter kennis worden gebracht en gelden er bepaalde vereisten voor de emittent. De naleving van deze vereisten zou alleen voor deze activa achteraf worden gecontroleerd door de bevoegde autoriteit. Tot slot gelden er gedrags- en transparantieregels en prudentiële vereisten voor de emittenten.

De Europese Commissie heeft een voorstel voor een verordening gepubliceerd om een kader te scheppen voor cryptoactiva

Voor de eerste twee categorieën van activa gelden bijzondere regels wanneer het actief als significant wordt beschouwd op grond van criteria die wijzen op een grotere impact, met name voor de financiële stabiliteit. In dat geval zou de Europese Bankautoriteit voor alle of een deel van de bepalingen van de verordening de bevoegde autoriteit voor deze activa zijn.

Een tweede deel van de verordening bevat regels voor cryptoactivadiensten, zoals de bewaring en de administratie, de exploitatie van een handelsplatform, de uitvoering van orders, enz.

De Bank is nauw betrokken bij de onderhandelingen over dit voorstel in haar hoedanigheid van deskundige bij de Permanente Vertegenwoordiging van België bij de Europese Unie.

1 Het white paper is een document dat door de emittent onder zijn verantwoordelijkheid wordt opgesteld en gepubliceerd en dat de belangrijkste informatie bevat die volgens de MiCA openbaar moet worden gemaakt (bijvoorbeeld met betrekking tot de emittent, het project, het type actief en de rechten op dat actief, of de technologie) om de toekomstige koper van cryptoactiva in staat te stellen met kennis van zaken een aankoopbeslissing te nemen.