



Servizio studi del Senato

Note su atti dell'Unione europea



NOTA N. 83

PROPOSTE EUROPEE IN MATERIA DI PAGAMENTI E FINANZA DIGITALE

La presente Nota illustra il Pacchetto sulla finanza digitale proposto il 24 settembre 2020 dalla Commissione europea. Del pacchetto fanno parte la strategia in materia dei pagamenti al dettaglio (paragrafo 2), la strategia in materia di finanza digitale (paragrafo 3) e quattro proposte legislative (paragrafo 6). Il Pacchetto è stato oggetto dei lavori del Consiglio economia e finanza (ECOFIN) a partire dal successivo meeting di ottobre sino all'ultima videoconferenza del 16 aprile 2021 (paragrafo 4). Nel mese di marzo u.s. è stato raggiunto un accordo sulle Conclusioni del Consiglio sulla strategia in materia di pagamenti al dettaglio (paragrafo 5).

1. Introduzione

Il 24 settembre 2020 la Commissione europea ha presentato un "[Pacchetto sulla finanza digitale](#)". Del pacchetto fanno parte **due comunicazioni strategiche in materia di [finanza digitale](#) e [pagamenti al dettaglio](#)**, nonché **tre proposte di regolamento** sulle cripto-attività, su un regime "pilota" per **infrastrutture di mercato basate sulla tecnologia dei registri distribuiti** (tra le quali rientra la *blockchain*) e sulla **resilienza digitale operativa del settore finanziario più una proposta di direttiva** volta ad **adeguare e coordinare la normativa esistente** rispetto alle modifiche introdotte dai precedenti atti.

Il pacchetto è volto a ridurre la frammentazione del mercato, promuovere la concorrenza e favorire l'innovazione contenendone i rischi legati alla stabilità finanziaria, alla protezione dei consumatori e all'antiriciclaggio.

Secondo la Commissione "**il futuro della finanza è digitale**". La crisi sanitaria ha accelerato i processi già in atto, per cui una quota sempre maggiore dei servizi di pagamento, finanziamento e investimento avviene tramite tecnologie digitali. Sostenere la transizione digitale nell'UE è una priorità chiave per la Commissione, come stabilito nella comunicazione di febbraio 2020 ("[Plasmare il futuro digitale dell'Europa](#)") e più di recente nell'ambito del [piano per la ripresa](#).

2. Pagamenti al dettaglio

La **strategia in materia di pagamenti al dettaglio** prevede 4 ambiti di obiettivi e azioni:

1. **soluzioni di pagamento sempre più digitali e istantanee di portata paneuropea**: nel novembre del 2020 è scaduto il periodo di esenzione temporanea stabilito dal regolamento che istituisce l'area unica dei pagamenti in euro (*Single Euro Payments Area* [SEPA](#)) per il soddisfacimento dei requisiti di adesione allo **schema per i pagamenti istantanei** in euro

sviluppato dal [Consiglio europeo per i pagamenti \(SCT Inst\)](#). Un **pagamento istantaneo** è un trasferimento elettronico al dettaglio con **accredito dei fondi sul conto del beneficiario in pochi secondi anziché in uno o più giorni lavorativi**. La Commissione intende esaminare il numero di prestatori di servizi di pagamento nonché il numero di conti in grado di inviare e ricevere bonifici istantanei SEPA e, su tale base, **decidere se è opportuno proporre una normativa che imponga l'adesione dei prestatori di servizi di pagamento allo schema SCT Inst** entro la fine del 2021. La Commissione intende valutare inoltre l'opportunità di imporre l'adesione da parte di tutti i portatori di interessi alla totalità o a una parte delle funzionalità aggiuntive dello schema SCT Inst che potrebbero comprendere anche eventuali *standard* futuri per i codici QR. Nel contesto del **riesame della direttiva sui servizi di pagamento (PSD2)**, la Commissione intende valutare il livello di **tutela dei consumatori** che effettuano pagamenti istantanei in relazione, ad esempio, al diritto ai rimborsi e alle commissioni applicate. Saranno esaminate inoltre, se del caso in collaborazione con la Banca centrale europea (BCE) e o l'Autorità bancaria europea (ABE), le misure per far fronte a rischi specifici, quali il rischio di liquidità, il riciclaggio di denaro, il finanziamento del terrorismo e i reati "presupposto" associati. Entro la fine del 2023 la Commissione intende esaminare la fattibilità dello sviluppo di un'"etichetta" per le **soluzioni di pagamento paneuropee**; modalità per **facilitare la diffusione delle specifiche europee per i pagamenti con carta senza contatto (CPACE)** e sostenere la **modernizzazione dei dispositivi dei commercianti dell'UE** per l'accettazione dei pagamenti, consentendo ad esempio ai registratori di cassa di emettere ricevute elettroniche. La Commissione intende inoltre fornire orientamenti, se necessario, per garantire che le soluzioni di pagamento istantaneo e i rispettivi modelli di *business* siano conformi alle norme dell'UE in materia di concorrenza. Al fine di **facilitare l'interoperabilità transfrontaliera e nazionale**, la Commissione intende esaminare, in stretta collaborazione con l'ABE, le modalità per **promuovere l'uso dell'identità elettronica** e delle soluzioni basate su servizi fiduciari, sfruttando l'ulteriore potenziamento del [regolamento eIDAS](#), per sostenere l'adempimento delle prescrizioni di autenticazione forte del cliente a norma della PSD2 per l'accesso al conto e la disposizione di operazioni di pagamento. Nel 2022 la Commissione intende realizzare uno studio sul livello di accettazione dei pagamenti digitali nell'UE, in particolare da parte delle PMI e delle pubbliche amministrazioni. Al fine di sostenere l'emissione di una **valuta digitale della banca centrale** per le operazioni al dettaglio in euro, la Commissione intende lavorare a stretto contatto con la BCE sugli obiettivi e sulle opzioni politiche nonché sulle misure per garantire un elevato livello di complementarità tra le soluzioni di pagamento sviluppate dal settore privato e il necessario intervento delle autorità pubbliche;

2. **mercati innovativi e competitivi dei pagamenti al dettaglio**: in stretto coordinamento con l'ABE, la Commissione intende monitorare attentamente l'**attuazione delle prescrizioni in materia di autenticazione forte del cliente**. Nel contesto del riesame della PSD2, la Commissione farà il punto sull'impatto dell'autenticazione forte del cliente sul **livello di frode nei pagamenti** nell'UE ed esaminerà se si debbano prendere in considerazione misure supplementari per affrontare nuovi tipi di frode, in particolare per quanto riguarda i pagamenti istantanei. Nel riesaminare la PSD2, la Commissione, in stretto coordinamento con l'ABE, intende considerare i limiti legali esistenti per i **pagamenti senza contatto**, al fine di trovare un **equilibrio tra la loro praticità e i rischi di frode**. Al fine di affrontare adeguatamente i rischi potenziali, garantire una maggiore coerenza nei vari atti legislativi sui pagamenti al dettaglio e promuovere una vigilanza e una sorveglianza solide, la Commissione intende valutare i nuovi rischi derivanti dai servizi non regolamentati, in particolare i **servizi tecnici accessori alla prestazione di servizi di pagamento o di moneta elettronica regolamentati**, e valutare se e come tali rischi possano essere mitigati, anche sottoponendo a una vigilanza

diretta i prestatori di servizi accessori o le entità cui sono esternalizzate tali attività, facendole eventualmente rientrare nell'ambito di applicazione della PSD2. La Commissione intende valutare altresì **l'adeguatezza dei requisiti prudenziali, operativi e in materia di tutela dei consumatori** applicabili a istituti di pagamento, istituti di moneta elettronica ed emittenti di *token* di moneta elettronica, considerando l'opportunità di allinearne il contenuto e di garantire collegamenti adeguati tra la vigilanza dei servizi di pagamento e la sorveglianza di sistemi, schemi e strumenti di pagamento;

3. **sistemi di pagamento al dettaglio efficienti e interoperabili e altre infrastrutture di sostegno:** nel quadro del riesame della **direttiva sul carattere definitivo del regolamento (direttiva 98/26/CE)**, volta a garantire che gli ordini di trasferimento e pagamento di prodotti finanziari possano essere finalizzati, principalmente limitando i problemi dovuti all'insolvenza di un partecipante, la Commissione intende valutare se **includere nell'ambito di applicazione gli istituti di pagamento e di moneta elettronica**, da sottoporre a vigilanza e attenuazione dei rischi adeguate. Parallelamente all'applicazione attuale e futura delle norme sulla concorrenza, la Commissione valuterà inoltre l'opportunità di proporre una legislazione volta a garantire un diritto di accesso a condizioni eque, ragionevoli e non discriminatorie alle infrastrutture tecniche ritenute necessarie per supportare la prestazione di servizi di pagamento;
4. **pagamenti internazionali efficienti, anche per le rimesse:** ove possibile, la Commissione si aspetta che i gestori dei sistemi di pagamento, in particolare laddove anche la giurisdizione del destinatario abbia adottato sistemi di pagamento istantaneo, **facilitino i collegamenti tra sistemi europei** quali il TARGET *Instant Payment settlement* (TIPS) o il *Real Time 1* (RT1) e **i sistemi di pagamento istantaneo di Paesi terzi**, purché questi ultimi garantiscano un livello adeguato di tutela dei consumatori, misure di prevenzione del riciclaggio e del finanziamento del terrorismo e misure di attenuazione dei rischi derivanti da interdipendenze. L'accesso diretto dei prestatori di servizi di pagamento non bancari ai sistemi di pagamento potrebbe aumentare i potenziali vantaggi di tali collegamenti. La Commissione intende adoperarsi affinché le norme internazionali facilitino **l'inclusione di dati più approfonditi nei messaggi di pagamento**. Al fine di aumentare ulteriormente la trasparenza delle operazioni transfrontaliere, la Commissione incoraggia i prestatori di servizi di pagamento a utilizzare l'iniziativa globale per i pagamenti (*Global Payment Initiative* - GPI) della Società per le telecomunicazioni finanziarie interbancarie mondiali (SWIFT), che facilita il tracciamento in tempo reale dei pagamenti transfrontalieri da parte degli istituti partecipanti. L'ampio utilizzo della funzione di tracciamento (*tracker*) consentirebbe ai prestatori di servizi di pagamento da cui ha origine l'operazione di stimare meglio e comunicare al pagatore il tempo massimo di esecuzione di un pagamento transfrontaliero. La Commissione intende valutare, nel quadro del riesame della PSD2, se sia necessario migliorare ulteriormente la trasparenza delle operazioni internazionali transfrontaliere. Dato che i pagamenti istantanei stanno diventando la norma anche a livello internazionale, la Commissione valuterà l'opportunità di prescrivere che il tempo massimo di esecuzione delle operazioni tra prestatori di servizi di pagamento che hanno entrambi sede nell'UE (le cosiddette operazioni "*two-leg*") si applichi anche alle operazioni "*one-leg*" (operazioni in cui il prestatore di servizi di pagamento o del beneficiario o del pagatore si trova al di fuori dell'Unione). La Commissione segue con interesse i lavori in corso svolti nel quadro del Consiglio europeo dei pagamenti sull'eventuale **ulteriore armonizzazione delle regole commerciali e degli standard di messaggistica per le operazioni "one-leg"** e intende valutare se sia necessario renderli obbligatori. Tutte le azioni strategiche di cui sopra possono, secondo la Commissione, facilitare i flussi transfrontalieri e quindi apportare benefici anche alle rimesse.

3. Finanza digitale

La **strategia in materia di finanza digitale** prevede 4 ambiti di obiettivi e strumenti:

1. **rimuovere la frammentazione del mercato unico digitale**: la Commissione ritiene opportuno che entro il 2024 l'UE attui un solido quadro normativo che permetta **l'utilizzo di soluzioni interoperabili per l'identità digitale**, così da consentire ai nuovi clienti di **accedere ai servizi finanziari in modo rapido e semplice ("onboarding")**. Tale quadro dovrebbe essere basato su **norme in materia di antiriciclaggio e di contrasto del finanziamento del terrorismo più armonizzate**, nonché sulla **revisione del quadro in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche** (regolamento eIDAS). Il riutilizzo dei dati del cliente dovrebbe essere subordinato al consenso informato del cliente stesso, consenso basato sulla piena trasparenza in merito alle conseguenze e alle implicazioni di tale riutilizzo. La Commissione, inoltre, ritiene che entro il 2024 il **sistema del "passaporto"** e lo **sportello unico per il rilascio delle autorizzazioni** dovrebbero essere applicati in **tutti i settori con un forte potenziale per la finanza digitale**. Le imprese dovrebbero poter contare sulla stretta collaborazione tra i facilitatori dell'innovazione in materia di vigilanza nazionali del [forum europeo dei facilitatori in materia di innovazione](#) (*European Forum for Innovation Facilitators* - EFIF) e su una **nuova piattaforma dell'UE per la finanza digitale**. Nel 2021, la Commissione intende proporre l'armonizzazione delle norme sull'accesso dei clienti e avviare il riesame del regolamento eIDAS per attuare un **quadro transfrontaliero interoperabile per le identità digitali**. La Commissione intende valutare la necessità di introdurre ulteriori regimi armonizzati in materia di rilascio di autorizzazioni e di "passaporto", collaborare con le autorità europee di vigilanza (AEV) al fine di rafforzare l'EFIF e istituire una piattaforma dell'UE per la finanza digitale allo scopo di incoraggiare la cooperazione tra portatori di interessi pubblici e privati;
2. **adeguare il quadro normativo dell'UE per favorire l'innovazione digitale**: in tale ambito la Commissione [propone un nuovo quadro normativo dell'UE per le crypto-attività](#), che comprende *token* correlati ad attività (conosciuti anche come "*stablecoin*") "*token* di moneta elettronica" e "*utility token*" (COM(2020) 593 final - Proposta di Regolamento relativo ai mercati delle crypto-attività e che modifica la direttiva (UE) 2019/1937, **cosiddetta proposta "MICA" - Markets in Crypto-assets**). Tramite un ciclo stabile di valutazione, la Commissione intende **rimuovere i potenziali ostacoli normativi sostanziali all'innovazione derivanti dalla legislazione in materia di servizi finanziari**. Fornirà su base regolare orientamenti interpretativi sulle modalità di applicazione della normativa vigente in materia di servizi finanziari alle nuove tecnologie, con il fine di contribuire a conseguire una maggiore efficienza mediante un **utilizzo più ampio della tecnologia di registro distribuito** (*Distributed Ledger Technology* - DLT) nell'ambito dei mercati dei capitali, pur continuando a rispettare le norme di sicurezza e mantenendo un alto livello di protezione dell'utente. Al riguardo, la Commissione [propone un nuovo quadro normativo per infrastrutture di mercato basate sulla DLT](#) (COM(2020) 594 final - Proposta di Regolamento relativo ad un regime pilota per le infrastrutture di mercato basate sulla tecnologia di registro distribuito);
3. **promuovere l'innovazione guidata dai dati nella finanza, istituendo uno spazio comune di dati finanziari**: la Commissione intende modificare la normativa dell'UE, al fine di **garantire che le informazioni finanziarie siano rese disponibili al pubblico in formati standardizzati e leggibili meccanicamente** e metterà a punto **un'infrastruttura per l'informativa al pubblico finanziata dall'UE**. Nel 2021 la Commissione intende presentare una **strategia sui dati di vigilanza**. Entro la metà del 2022, inoltre, dovrebbe essere elaborata

una proposta legislativa su un **nuovo quadro in materia di finanza aperta**, che intende allineare la normativa europea ai contesti di migliore **accesso ai dati** da parte degli investitori;

4. **far fronte alle sfide e ai rischi connessi alla trasformazione digitale**: la Commissione intende realizzare, entro la metà del 2022, i necessari adattamenti dell'attuale quadro normativo in materia di servizi finanziari per quanto riguarda la tutela del consumatore e le norme prudenziali, al fine di proteggere gli utenti finali della finanza digitale, salvaguardare la stabilità finanziaria, proteggere l'integrità del settore finanziario dell'UE e garantire la parità di condizioni. Al riguardo, la Commissione **propone un nuovo quadro** dell'UE per il **rafforzamento della resilienza operativa digitale per i settori della finanza in tutta l'Unione**, al fine di migliorare la gestione del rischio relativo alle tecnologie dell'informazione e della comunicazione (TIC) di vari istituti finanziari, compresi i prestatori di servizi di pagamento (COM(2020) 595 final - Proposta di Regolamento relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014, **cosiddetta proposta "DORA" - *Digital Operational Resilience Act***). Tale iniziativa è coerente con la direttiva sulle infrastrutture critiche europee. La Commissione lavorerà in stretto coordinamento con l'ABE per avvalersi degli insegnamenti tratti dall'attuazione degli orientamenti dell'ABE sulle TIC e la gestione dei rischi per la sicurezza, che sono applicabili dal giugno 2020.

4. Gli sviluppi del negoziato nel Consiglio ECOFIN

L'iniziativa della Commissione europea è stata oggetto di uno scambio di opinioni nel primo **Consiglio ECOFIN** successivo alla sua presentazione (6 ottobre 2020). I **ministri hanno espresso il loro sostegno alle proposte della Commissione**. La presidenza ha messo in evidenza la sua intenzione di **lavorare intensamente alle proposte legislative**, cogliendo anche gli spunti contenuti nel **report sull'euro digitale pubblicato** dalla BCE il 2 ottobre 2020.

Nel corso dell'ECOFIN del **4 novembre 2020** la presidenza ha informato i ministri dell'avvio dei lavori relativi alle proposte legislative per il **rafforzamento della resilienza operativa digitale per i settori della finanza in tutta l'Unione** ("DORA" - *Digital Operational Resilience Act for financial services*) e per un **nuovo quadro normativo dell'UE per le crypto-attività** ("MICA" - *Markets in Crypto-assets*). Nei **successivi tre mesi** è stata impressa una progressiva accelerazione ai lavori, aprendo il dibattito fra gli Stati membri sui principali aspetti di *policy* connessi al pacchetto di proposte della Commissione.

Nell'**ECOFIN del 16 marzo 2021** la presidenza ha informato i ministri che, in seguito a un accordo raggiunto a livello tecnico, il Consiglio avrebbe adottato, senza dibattito, le **conclusioni sulla strategia in materia di pagamenti al dettaglio** nella sessione del Consiglio "Agricoltura e pesca" del 22 e 23 marzo. Nel progetto di conclusioni il Consiglio conferisce alla Commissione un **forte mandato politico per portare avanti iniziative nel settore**, anche con l'obiettivo di **promuovere l'uso di soluzioni di pagamento istantaneo in tutta l'UE e di accompagnare lo sviluppo di un euro digitale**, sottolineando allo stesso tempo le molte sfide di cui tenere conto, quali l'inclusione finanziaria, la sicurezza e la tutela dei consumatori, la protezione dei dati e l'antiriciclaggio.

La Presidenza ha sostenuto la **necessità di revisione della Direttiva sui servizi di pagamento (PSD2)** e l'importanza di preservare la tutela consumatori e di garantire elevati *standard* di sicurezza nelle transazioni. Le conclusioni del Consiglio richiamano esplicitamente l'importanza della **resilienza delle infrastrutture**, della tutela consumatori, della prevenzione delle frodi e del contrasto al riciclaggio. La Commissione ha sottolineato come in un'economia sempre più digitalizzata l'applicazione della strategia sui pagamenti al dettaglio sia molto importante per il conseguimento

dell'autonomia strategica dell'UE e ha messo in evidenza i benefici potenziali dei pagamenti istantanei, compiendo alcune valutazioni circa i fattori che possono favorirne la diffusione. Circa il progetto di emissione di un **euro digitale**, la **Commissione e la BCE collaboreranno per eseguire un vaglio tecnico, politico e giuridico** tenendo conto dei rispettivi mandati come sanciti dai Trattati. È stata inoltre sottolineata l'importanza di **accrescere l'inclusione finanziaria** e di **ridurre gli elevati costi derivanti dalla insufficiente alfabetizzazione finanziaria dei risparmiatori**.

Per quanto riguarda le **proposte legislative contenute nel pacchetto finanza digitale**, è stato rappresentato che sono in corso presso il Consiglio i negoziati sulle proposte **MICA** (Mercati delle cripto-attività), su cui si sta lavorando per trovare un punto di equilibrio tra sicurezza e innovazione nella disciplina sugli *stablecoin* e **DORA** (Resilienza operativa digitale), dove permangono divergenze di opinioni con riferimento alla vigilanza dei fornitori di servizi ICT. **La Commissione sia nel meeting di marzo che in quello successivo del 16 aprile ha manifestato l'auspicio che entrambi i negoziati possano concludersi sotto la Presidenza portoghese**.

5. Le Conclusioni del Consiglio sulla strategia in materia di pagamenti al dettaglio

Nelle sue conclusioni il Consiglio parte dal presupposto che l'emergere di nuove soluzioni di pagamento comporti una serie di sfide strategiche per l'UE in termini di regolamentazione e vigilanza, in particolare per quanto riguarda obiettivi essenziali quali la sicurezza, la tutela dei consumatori, la concorrenza, la protezione dei dati, l'antiriciclaggio e il contrasto del finanziamento del terrorismo.

Il Consiglio **concorda con i "pilastri" individuati per le azioni strategiche**, che esaminano 1) le **soluzioni di pagamento sempre più digitali e istantanee di portata paneuropea**, 2) le questioni in materia di **innovazione e competitività**, 3) gli aspetti relativi **all'accesso, all'efficienza e all'interoperabilità dei sistemi** di pagamento al dettaglio e di altre infrastrutture di sostegno, e 4) la **dimensione internazionale**. Il Consiglio evidenzia, in particolare, gli **obiettivi di promuovere un utilizzo diffuso dei pagamenti istantanei**, unitamente ad altre soluzioni di pagamento, di disporre di un insieme di strumenti legislativi idoneo a rispondere alle sfide poste dal passaggio alla digitalizzazione, e di promuovere un ecosistema dei pagamenti innovativo, aperto, resiliente, sicuro e inclusivo.

Il Consiglio **invita la Commissione europea ad agire**, se necessario a seguito di una valutazione d'impatto, **in modo graduale e proporzionato, verso un'azione legislativa che promuova l'adesione allo schema di bonifico istantaneo SEPA (SCT Inst) e alle sue funzionalità aggiuntive** (ad esempio "*Request-To-Pay*", i codici QR e i servizi "*Proxy Lookup*") e che possano essere valutati altri modi per favorire la sua adozione, anche sfruttando le infrastrutture già disponibili, in particolare il sistema di pagamento istantaneo TARGET (TIPS). Sostiene gli sforzi compiuti dalla Commissione per favorire lo sviluppo di soluzioni paneuropee e il miglioramento del quadro interoperabile dell'UE in materia di identificazione elettronica, sottolineando l'importanza di monitorare costantemente gli sviluppi e le nuove tecnologie in tale settore.

Prima dell'elaborazione di qualsiasi eventuale proposta legislativa volta a **incrementare i pagamenti digitali**, incoraggia la realizzazione di uno **studio sul livello di accettazione** degli stessi, sottolineando che a tale riguardo **esistono differenze significative in tutta l'UE**. **Il contante continua a svolgere un ruolo essenziale nei pagamenti al dettaglio**, anche per coloro che sono esclusi dal sistema finanziario o digitale, e talvolta come garanzia in caso di malfunzionamento dei sistemi e delle infrastrutture di pagamento. Quindi sia il contante sia i pagamenti digitali dovrebbero essere ampiamente disponibili e accettati, in risposta alla domanda e alle preferenze degli utenti. Il Consiglio **incoraggia la promozione dell'alfabetizzazione digitale e finanziaria** per far fronte al

rischio di esclusione finanziaria e concorda sulla necessità di garantire che gli approcci improntati all'applicazione dell'autenticazione forte del cliente non comportino l'esclusione di talune categorie di utenti di servizi di pagamento (USP).

Le conclusioni sottolineano i **potenziali benefici delle valute digitali della banca centrale (CBCD)**, anche per quanto riguarda la digitalizzazione dell'economia e la sovranità dell'UE, pur riconoscendo la **complessità di tale questione** e l'importanza di realizzare un'analisi attenta e approfondita dei potenziali effetti negativi, in particolare **per i modelli di business degli intermediari finanziari** e dei fornitori di altri servizi, per la stabilità finanziaria, la politica monetaria, la protezione dei dati e la vita privata. In tale contesto, il Consiglio sostiene i lavori svolti dall'Eurosistema relativi a una valuta digitale della banca centrale per le operazioni al dettaglio in euro (o "euro digitale") e riconosce l'importante ruolo svolto dalla Commissione e dall'Eurogruppo per lo sviluppo di tale strumento, tenendo conto dei rispettivi ruoli e mandati previsti dai trattati e garantendo piena trasparenza nei confronti degli Stati membri non appartenenti alla zona euro.

Con riferimento alle future iniziative della Commissione europea, il Consiglio:

- **accoglie con favore un riesame globale dell'attuazione della seconda direttiva sui servizi di pagamento (PSD2)**, in seguito alla sua piena realizzazione e tenuto conto delle sfide incontrate nella sua messa in atto, ponendo l'accento in particolare sulla valutazione dei seguenti elementi: *i)* l'adeguatezza dell'**ambito di applicazione** (anche per quanto riguarda i prestatori di servizi tecnici) e l'esigenza di chiarire ulteriormente i concetti e le norme esistenti; *ii)* l'**interazione con altre normative** del settore, segnatamente la direttiva sulla moneta elettronica, la direttiva antiriciclaggio, il *General Data Protection Regulation* (GDPR) e altri sviluppi legislativi in corso; *iii)* l'**evoluzione verso i servizi bancari aperti**, la gestione dei rischi connessi alla vita privata e l'interazione con le linee guida del Comitato Europeo per la Protezione dei Dati (EDPB) in materia; *iv)* l'impatto sulla **concorrenza**, compreso il ruolo crescente delle grandi imprese tecnologiche e delle imprese FinTech; *v)* l'efficacia per limitare le frodi e accrescere la protezione dei consumatori, compresa l'autenticazione forte del cliente;
- **sostiene gli ulteriori sforzi intesi a conseguire l'interoperabilità delle interfacce di programmazione di applicazioni (API)** e a valutare se un'ulteriore **standardizzazione** possa liberare il pieno potenziale dei servizi bancari aperti, sottolineando nel contempo l'importanza di consentire agli utenti di controllare facilmente l'utilizzo dei propri dati;
- **è favorevole a una valutazione dei limiti legali esistenti per i pagamenti senza contatto** e di campagne di sensibilizzazione dei consumatori, alla luce della recente esperienza maturata durante la pandemia;
- **sostiene l'ampliamento dell'ambito di applicazione della direttiva sul carattere definitivo del regolamento dei pagamenti** per includervi gli istituti di pagamento e di moneta elettronica, a condizione che i rischi potenziali siano attentamente soppesati e opportunamente mitigati;
- **è a favore di un intervento legislativo per assicurare il diritto di accesso**, a condizioni eque, ragionevoli e non discriminatorie, **alle infrastrutture tecniche considerate necessarie** per sostenere la fornitura di servizi di pagamento come le comunicazioni in prossimità (*Near Field Communication*, NFC);
- **ritiene necessarie ulteriori iniziative per facilitare i collegamenti tra i sistemi di pagamento istantaneo e altri sistemi di pagamento digitale a livello mondiale**, compresi quelli che tengono conto delle raccomandazioni e delle norme sviluppate in consessi internazionali, per ridurre i costi e accrescere la velocità e la praticità dei trasferimenti transfrontalieri di denaro, in ottemperanza dei quadri antiriciclaggio (*Anti-Money Laundering*

- AML) e di contrasto al finanziamento del terrorismo (*Counter Terrorist Financing* - CFT), pur prendendo atto dei numerosi ostacoli da superare in questo settore (diverse pratiche normative applicate dalle giurisdizioni, scarsa trasparenza in materia di costi e l'assenza di interoperabilità tra le infrastrutture informatiche e di pagamento);

- **sostiene la facilitazione di collegamenti qualora le giurisdizioni di Paesi terzi garantiscano un livello adeguato di protezione dei consumatori**, prevenzione delle frodi nonché rispetto delle disposizioni in materia di AML CFT e degli obblighi previsti dal GDPR;
- **incoraggia l'adozione della norma globale ISO 20022** per facilitare l'inclusione di dati più ricchi nei messaggi di pagamento, pur riconoscendo che, per i pagamenti internazionali, rispettare il termine fissato a fine 2022 è un compito impegnativo;
- **conviene che la possibilità di applicare alle operazioni "one-leg" il tempo massimo di esecuzione attualmente previsto per le operazioni** tra prestatori di servizi di pagamento che hanno entrambi sede nell'UE (le cosiddette operazioni "two-leg") potrebbe essere **valutata con attenzione**, unitamente alle relative sfide, nel contesto del riesame della PSD2, tenendo conto delle conseguenze, in particolare in termini di responsabilità, per i prestatori di servizi di pagamento con sede nell'UE che inviano denaro a paesi terzi;
- **sostiene le iniziative pubbliche e private in numerosi Stati membri a favore di rimesse più rapide**, economiche e pratiche, nel rispetto delle norme in materia di protezione dei consumatori, prevenzione delle frodi, AML/CFT e GDPR;
- **invita la Commissione a promuovere nei Paesi a reddito medio e basso, nel quadro della politica di sviluppo dell'UE, l'accesso ai conti di pagamento e lo sviluppo di soluzioni di pagamento interoperabili a livello mondiale.**

6. Illustrazione delle proposte di atti normativi incluse nel Pacchetto sulla finanza digitale

COM(2020) 593 final

Proposta di REGOLAMENTO relativo ai mercati delle cripto-attività e che modifica la direttiva (UE) 2019/1937

Secondo la Commissione il mercato delle cripto-attività è ancora di dimensioni modeste e ad oggi non costituisce una minaccia per la stabilità finanziaria. È tuttavia probabile che i consumatori adottino in larga misura un sottoinsieme di cripto-attività che mirano a stabilizzare il loro prezzo ancorandone il valore a una specifica attività o a un paniere di attività. **Tale sviluppo potrebbe comportare ulteriori sfide per la stabilità finanziaria, la trasmissione della politica monetaria o la sovranità monetaria.** La Commissione ha pertanto ritenuto necessario proporre un quadro specifico e armonizzato a livello dell'Unione, allo scopo di definire norme specifiche per le cripto-attività e le attività e i servizi correlati e per chiarire il quadro giuridico applicabile.

La proposta sui mercati delle cripto-attività (*markets in crypto assets* - MICA) **mira a stabilire regole per alcune tipologie di "attività" non disciplinate dalla vigente legislazione dell'UE in materia di servizi finanziari e a stabilire norme uniformi per gli emittenti e i fornitori di servizi per le cripto-attività a livello dell'UE.**

Le cripto-attività sono **rappresentazioni digitali di valore e di diritti**, la cui diffusione è andata di pari passo con una nuova tecnologia cosiddetta di "**registro distribuito**" di informazioni digitali ("*Distributed Ledgers Technology*"), la cui principale applicazione è rappresentata dalla **blockchain**. Il registro è "distribuito" in quanto è composto da unità indipendenti ("nodi") invece che essere centralizzato in una unità da cui dipende l'accesso delle altre. La **blockchain** ne rappresenta una specifica tipologia, che prevede l'archiviazione delle informazioni in "blocchi" che ad intervalli regolari vengono condivisi dai nodi del sistema e resi immutabili.

Questi registri possono ospitare una grande varietà di informazioni. In ambito finanziario la loro utilità dipende dal fatto che possono contenere **informazioni sui diritti che spettano al possessore** (*token* di attività), al quale è garantito **l'accesso esclusivo** per mezzo della **crittografia**, per cui un solo soggetto è in possesso della chiave di accesso all'informazione da cui dipende l'esercizio di uno o più diritti. Il **token** è il gettone (virtuale) che consente questo esercizio e per questo è dotato di un **valore**, che non è intrinseco ma **dipende dal bene o dalla prestazione alla quale consente di accedere**. Più tale bene o prestazione è diffusa e standardizzata e più aumentano le potenzialità di un *token* come mezzo di scambio, unità di conto e riserva di valore. In altri termini, il valore del *token* dipende dal "contesto" in cui viene accettato come strumento rappresentativo, come una *fiches*, un buono pasto o un titolo azionario.

Poiché un *token* è un sistema di informazioni gestite attraverso un registro distribuito (DLT), esso può assumere una varietà enorme di forme virtuali. Questo rende estremamente complesso il suo inquadramento dal punto di vista normativo. Il Pacchetto per la finanza digitale della Commissione prevede tre tipologie di *token*:

a. "**utility token**": cripto-attività destinate a fornire l'accesso digitale a un bene o a un servizio, disponibile mediante DLT, e che è accettato solo dall'emittente di tale *token*;

b. **"token collegati ad attività"**: mirano a mantenere un valore stabile ancorandosi a diverse monete aventi corso legale, a una o più merci, a una o più cripto-attività o a un paniere di tali attività. Spesso la stabilizzazione del valore dei *token* collegati ad attività è finalizzata a far sì che i loro possessori li utilizzino come mezzo di pagamento per acquistare beni e servizi e come riserva di valore;

c. **"token di moneta elettronica"**: cripto-attività destinate a essere utilizzate principalmente come mezzo di pagamento e che mirano alla stabilizzazione del valore ancorandosi a un'unica moneta fiduciaria. La funzione di tali cripto-attività è molto simile a quella della moneta elettronica.

Alcuni token infine sono assimilabili a "strumenti finanziari" come definiti dalla MiFID (azioni, obbligazioni, fondi di investimento, strumenti derivati). Con le modifiche apportate dal Pacchetto per la finanza digitale alla MiFID (vedi *infra*) tali cripto-attività gestite attraverso una DLT rientreranno nell'ambito di applicazione della legislazione dell'Unione in materia di servizi finanziari.

Il regolamento in esame ne costituisce il complemento ad uno, e sostituirà le regole nazionali esistenti applicabili alle cripto-attività prevedendo norme specifiche per i cosiddetti *stablecoin*, anche laddove questi siano considerati una moneta elettronica. La proposta di regolamento è suddivisa in nove titoli.

Disposizioni generali

Il **titolo I** contiene l'**oggetto**, l'**ambito di applicazione** e le **definizioni**. L'**articolo 1** stabilisce che il regolamento si applica agli emittenti e ai fornitori di servizi per le cripto-attività e presenta l'**elenco indicativo degli obblighi** uniformi in materia di trasparenza e di informativa in relazione all'emissione, al funzionamento, all'organizzazione e alla *governance* dei fornitori di servizi per le cripto-attività, nonché prevede l'applicazione di norme e misure per garantire l'integrità dei mercati. L'**articolo 2** **limita l'ambito di applicazione** del regolamento alle **cripto-attività non assimilabili a strumenti finanziari, depositi o depositi strutturati** ai sensi della legislazione dell'UE in materia di servizi finanziari (MiFID). Sono escluse anche le cripto-attività assimilabili a moneta elettronica, tranne quando rientrano nella definizione di *token* di moneta elettronica, e a cartolarizzazioni. L'**articolo 3** stabilisce i termini e le **definizioni** utilizzati nel regolamento, tra cui "cripto-attività", "emittente di cripto-attività", "*token* collegati ad attività" (spesso descritti come *stablecoin*), "*token* di moneta elettronica" (spesso descritti come *stablecoin*), "fornitore di servizi per le cripto-attività", "*utility token*" e altri. La "tecnologia di registro distribuito (DLT)" viene definita come un tipo di tecnologia che supporta la registrazione distribuita di dati cifrati. L'**articolo 3** definisce anche i vari **servizi per le cripto-attività**. La lista dei servizi appare analoga a quella definita dalla MiFID per i servizi relativi a strumenti finanziari, con l'aggiunta di specifiche previsioni per lo "**scambio di cripto-attività con moneta fiduciaria**" (la conclusione di contratti con terzi per l'acquisto o la vendita di cripto-attività a fronte di moneta fiduciaria avente corso legale utilizzando capitale proprio) e per lo "**scambio di cripto-attività con altre cripto-attività**" (la conclusione di contratti con terzi per l'acquisto o la vendita di cripto-attività a fronte di altre cripto-attività utilizzando capitale proprio). Questi due servizi disciplinano dunque un "micro" attività di mercato, che inquadra il singolo contratto di scambio, mentre la "**gestione di una piattaforma di negoziazione di cripto-attività**" è configurata come la gestione di una o più piattaforme di negoziazione delle cripto-attività, all'interno delle quali possono interagire molteplici interessi di terzi per l'acquisto e la vendita di cripto-attività, in modo tale da portare alla conclusione di contratti relativi allo scambio di una cripto-attività con un'altra o di una cripto-attività con una moneta fiduciaria a corso legale. È importante sottolineare che la Commissione può adottare **atti delegati per precisare alcuni elementi tecnici delle definizioni, al fine di adeguarli agli sviluppi tecnologici e di mercato.**

Le regole per gli emittenti di utility token

Il **titolo II** disciplina l'**offerta al pubblico** e l'**ammissione a negoziazione** di *utility token* (cripto-attività diverse dai *token* collegati ad attività e dai *token* di moneta elettronica). L'**articolo 4** prevede una serie di **requisiti che un emittente deve soddisfare** per avere il diritto di **offrire** tali cripto-attività al pubblico nell'Unione o di chiederne l'**ammissione alla negoziazione** su una piattaforma di negoziazione: lo **stabilimento** sotto forma di persona giuridica, la **redazione** un *White Paper* (documento informativo) sulle cripto-attività a norma dell'**articolo 5** (con l'allegato I), la relativa **notifica alle autorità competenti (articolo 7)** e la **pubblicazione (articolo 8)**. Una volta pubblicato il documento informativo, l'emittente può offrire le sue cripto-attività nell'UE o chiederne l'ammissione alla negoziazione su una piattaforma di negoziazione (**articolo 10**). L'articolo 4 prevede inoltre alcune **esenzioni** dalla pubblicazione di un *White Paper*, ad esempio per le offerte di cripto-attività di importo limitato (inferiori a un milione di euro in un periodo di 12 mesi) e per le offerte rivolte a investitori qualificati ai sensi del regolamento (UE) 2017/1129 (Regolamento prospetto). L'**articolo 5** della proposta stabilisce gli elementi previsti per il documento informativo (descrizione dettagliata dell'emittente, del progetto, delle caratteristiche e dei rischi dell'operazione e altri elementi indicati nell'allegato I), mentre l'**articolo 6** introduce alcuni **obblighi relativi al materiale di marketing** (chiarezza, correttezza e coerenza con il documento informativo). Il *White Paper* per gli *utility token* **non sarà soggetto a una procedura di approvazione preliminare da parte delle autorità nazionali competenti (articolo 7)**. Il documento e le eventuali informazioni di *marketing* dovranno essere notificati alle autorità nazionali competenti almeno 20 giorni prima dell'inizio dell'offerta. La notifica ha l'obbligo di **illustrare i motivi per cui le cripto-attività che si intende offrire non sono: uno strumento finanziario "MiFID", moneta elettronica, un deposito o un deposito strutturato**. Viene dunque richiesto all'emittente (presumibilmente con l'ausilio di un parere legale, almeno in una prima fase) di effettuare l'**inquadramento giuridico dell'attività**. Dopo la notifica del *White Paper*, le autorità competenti avranno la **facoltà di sospendere o vietare l'offerta, di esigere l'inserimento di informazioni aggiuntive** all'interno del documento o di rendere di dominio pubblico il fatto che l'emittente non rispetta il regolamento (**articolo 7**). Il titolo II contiene inoltre disposizioni specifiche sulle offerte di cripto-attività che prevedono un **termine** (articolo 9), sulle **modifiche di un *White Paper* iniziale (articolo 11)**, sul **diritto di recesso riconosciuto agli acquirenti di cripto-attività** entro 14 giorni dall'acquisto, il quale tuttavia **non si applica se le cripto-attività sono ammesse alla negoziazione** su una piattaforma di negoziazione (articolo 12), sugli **obblighi generali di correttezza, professionalità, onestà, trasparenza e gestione dei conflitti di interessi** imposti a tutti gli emittenti di cripto-attività (articolo 13) e sulla responsabilità per gli emittenti derivante dal *White Paper* sulle cripto-attività (articolo 14), per cui qualora un emittente abbia fornito nel suo *White Paper* (di seguito "*WP*") informazioni incomplete, non corrette o poco chiare, oppure fuorvianti, il possessore delle cripto-attività può chiedere (con l'onere della prova a suo carico) un **risarcimento per i danni** che gli sono stati arrecati a causa di detta violazione.

Le regole per gli emittenti di token collegati ad attività

Il **titolo III, capo 1**, stabilisce un **obbligo generale di autorizzazione per l'offerta al pubblico e l'ammissione a negoziazione di token collegati ad attività (TCA)** e descrive la procedura per l'**autorizzazione degli emittenti** e per l'**approvazione del loro *White Paper*** da parte delle **autorità nazionali competenti (articoli da 15 a 19 e allegati I e II)**. Per essere autorizzati a operare nell'Unione, gli emittenti di *token* collegati ad attività sono costituiti sotto forma di soggetto giuridico stabilito nell'UE. L'articolo 15 prevede inoltre **esenzioni** per i soggetti che emettono un **ammontare minimo** (importo medio in circolazione inferiore a 5 milioni calcolato giornalmente su un periodo di

12 mesi) nonché per i TCA che sono **offerti esclusivamente a investitori qualificati** senza possibilità di rivendita al pubblico. La **procedura di autorizzazione si svolge nell'arco temporale di circa 6 mesi**: dopo 3 mesi l'autorità nazionale competente invia una bozza di decisione alle autorità europee che emettono un parere non vincolante entro 2 mesi. Entro un mese dal ricevimento del parere le autorità competenti adottano una **decisione pienamente motivata che concede o rifiuta l'autorizzazione** (e approva il *WP*) all'emittente richiedente. La revoca di un'autorizzazione è descritta in dettaglio all'**articolo 20**, mentre l'**articolo 21** stabilisce la procedura per la **modifica del documento informativo** connessa a una modifica prevista del modello di *business* dell'emittente che possa avere un'influenza significativa sulla decisione di acquisto di qualsiasi possessore effettivo o potenziale di TCA.

Il **titolo III, capo 2**, stabilisce gli **obblighi ai quali deve conformarsi l'attività gli emittenti di TCA**, stabilendo che essi **sono tenuti ad agire in modo onesto, corretto, professionale e trasparente (articolo 23)**. In particolare, sono **tenuti alla pubblicazione del documento informativo sulle cripto-attività** sul proprio sito *web* e delle eventuali **comunicazioni di marketing (articolo 24)**, per le quali sono previsti **specifici requisiti (articolo 25)**. Inoltre, gli emittenti sono soggetti a obblighi di **informativa continua** sugli eventi che possono avere un impatto significativo sul valore dei TCA (**articolo 26**) e, con cadenza almeno mensile sono tenuti a pubblicare sul proprio sito *web* **l'importo dei token collegati ad attività in circolazione e il valore e la composizione delle attività di riserva**. Essi sono inoltre tenuti a istituire una **procedura di trattamento dei reclami (articolo 27)** a prevenire, individuare, gestire e comunicare i **conflitti di interesse (articolo 28)**, notificare **modifiche dell'organo di amministrazione** alla rispettiva autorità competente (**articolo 29**), dotarsi di **dispositivi di governance** trasparenti e coerenti, **procedure** efficaci per l'individuazione, la gestione, il monitoraggio e la segnalazione dei rischi ai quali sono o potrebbero essere esposti e adeguati **meccanismi di controllo interno**, tra cui valide procedure amministrative e contabili (**articolo 30**). L'**articolo 31** stabilisce che gli emittenti di TCA dispongono in qualsiasi momento di **fondi propri pari almeno a 350.000 euro ovvero, se superiore, al 2 % dell'importo medio delle attività di riserva** disciplinate dal successivo **articolo 32**. In particolare, viene sancito **l'obbligo per gli emittenti di TCA di mantenere una riserva di attività e di definire una politica chiara e dettagliata che descrive il meccanismo di stabilizzazione di tali token** (elenco attività, valutazione rischi, procedura di creazione e distruzione di TCA, politica di investimento delle riserve, procedura per il rimborso di TCA con attività di riserva). L'**articolo 33 stabilisce norme per la custodia delle attività di riserva**, prevedendo che esse **siano separate** dalle attività proprie dell'emittente, mentre l'**articolo 34** dispone che l'emittente **investa le attività di riserva solo in attività a basso rischio** (in particolare per quanto riguarda la loro liquidabilità). L'articolo 35 regola i diritti riconosciuti ai possessori di TCA, in particolare i **diritti di rimborso o credito diretto nei confronti dell'emittente o sulle attività di riserva, imponendo all'emittente di stabilire, mantenere e attuare politiche e procedure chiare e dettagliate su tali diritti**. L'articolo 36 vieta agli emittenti di *token* collegati ad attività e ai fornitori di servizi per le cripto-attività di **concedere qualsiasi interesse ai possessori dei token**.

Il **titolo III, capo 4**, stabilisce le **norme applicabili all'acquisizione di partecipazioni societarie in emittenti di TCA**: l'articolo 37 prevede degli **obblighi di comunicazione delle partecipazioni rilevanti** e descrive la **valutazione di un progetto di acquisizione da parte dell'autorità competente ai fini dell'eventuale esercizio del potere di opposizione**. Gli specifici elementi di **valutazione** (reputazione, solidità finanziaria, conformità normativa, in particolare connessa ai

fenomeni del riciclaggio e finanziamento del terrorismo) contenuto di tale valutazione sono dettagliati dall'articolo 38.

Il **titolo III, capo 5**, articolo 39, stabilisce i **criteri** che l'**Autorità bancaria europea (ABE)** utilizza per determinare se un **TCA sia significativo**. Tali criteri sono: le **dimensioni della clientela** dei promotori dei *token*, il **valore** dei TCA o la loro capitalizzazione di mercato, il **numero** e il **valore delle operazioni**, l'**entità della riserva** di attività, la rilevanza delle **attività transfrontaliere** degli emittenti e l'interconnessione con il sistema finanziario. L'**articolo 39** prevede alcune soglie minime (2 milioni di clienti, valore del TCA superiore a 1 miliardo, 500.000 operazioni per un controvalore minimo giornaliero di 100 milioni di euro, riserva minima pari a un miliardo di euro, diffusione dei TCA in minimo 7 Stati membri) e conferisce alla Commissione del **potere di adottare un atto delegato** al fine di specificare ulteriormente le soglie al di là delle quali un emittente di TCA sarà considerato significativo nonché le relative circostanze. L'articolo 40 precisa la possibilità per l'emittente di un TCA di classificarsi di propria iniziativa come significativo al momento della presentazione della domanda di autorizzazione. L'articolo 41 elenca gli **obblighi aggiuntivi applicabili agli emittenti di TCA significativi**, quali **requisiti di fondi propri aggiuntivi, politica retributiva e di gestione della liquidità**.

Il **titolo III, capo 6**, articolo 42 impone all'emittente di disporre di un **piano per la liquidazione ordinata delle sue attività**.

Le regole per gli emittenti di token di moneta elettronica

Il **titolo IV, capo 1**, stabilisce un **obbligo generale di autorizzazione per l'offerta al pubblico e l'ammissione a negoziazione di token di moneta elettronica (TME)**. Rispetto ai TCA viene ristretto il campo dei possibili emittenti, prevedendo che fra questi rientrino esclusivamente i soggetti autorizzati come **enti creditizi o istituti di moneta elettronica** ai sensi dell'articolo 2, paragrafo 1, della direttiva 2009/110/CE. L'**articolo 43** stabilisce inoltre che i "**token di moneta elettronica**" sono **considerati moneta elettronica** ai fini della direttiva 2009/110/CE.

L'**articolo 44** prevede gli obblighi applicabili agli emittenti di TME, in deroga alla relativa disciplina: **i TME sono emessi al valore nominale e al ricevimento dei fondi e, su richiesta del possessore di token di moneta elettronica, gli emittenti devono rimborsarli in qualsiasi momento e al valore nominale**. L'**articolo 45** vieta agli emittenti di TME e ai relativi fornitori di servizi di **concedere qualsiasi interesse ai possessori di tali token**. L'**articolo 46** e l'**allegato III** stabiliscono i **requisiti per il documento informativo** che accompagna l'emissione di TME (descrizione dell'emittente, descrizione dettagliata del progetto dell'emittente e delle caratteristiche dell'operazione, nonché informazioni sui rischi connessi all'emittente di moneta elettronica, ai TME e all'attuazione di eventuali progetti). L'**articolo 47** contiene le disposizioni sulla **responsabilità derivante dal White Paper (WP)** sulle crypto-attività in relazione ai TME. L'**articolo 48** definisce i **requisiti per le potenziali comunicazioni di marketing** prodotte in relazione a un'offerta di TME e l'**articolo 49** stabilisce che **i fondi ricevuti da un emittente in cambio di TME sono investiti in attività "sicure e a basso rischio" conformemente all'articolo 7, paragrafo 2, della direttiva 2009/110/CE denominate nella valuta di riferimento del TME**.

Il **titolo IV, capo 2, articolo 50**, stabilisce che l'ABE classifica i **TME come significativi** sulla base dei **criteri** elencati all'articolo 39 **per i token connessi ad attività** (vedi *supra*). Anche per gli emittenti di TME è prevista la possibilità di classificarsi di propria iniziativa come "significativo" al momento della presentazione della domanda di autorizzazione. L'**articolo 52** contiene gli **obblighi**

aggiuntivi applicabili agli emittenti di TME significativi. Gli emittenti di TME significativi devono applicare l'articolo 33 sulla custodia delle attività di riserva e l'articolo 34 sull'investimento di tali attività anziché l'articolo 7 della direttiva 2009/110/CE; l'articolo 41, paragrafi 1, 2 e 3, sulla remunerazione e la gestione della liquidità; l'articolo 41, paragrafo 4, anziché l'articolo 5 della direttiva 2009/110/CE e l'articolo 42 sulla liquidazione ordinata delle loro attività.

Le regole per i fornitori di servizi per le cripto-attività

Il **titolo V** prevede un **obbligo di autorizzazione e disciplina le condizioni operative dei fornitori di servizi per le cripto-attività.** Il capo 1 definisce le disposizioni in materia di autorizzazione (articolo 53), precisando il contenuto della **domanda** (articolo 54), la **valutazione** della domanda (articolo 55) e i **diritti di revoca di un'autorizzazione riconosciuti alle autorità competenti** (articolo 56). Il capo conferisce inoltre **all'ESMA** il compito di istituire un **registro di tutti i fornitori di servizi per le cripto-attività** (articolo 57) nel quale saranno conservate anche **informazioni sui WP** notificati alle autorità competenti. Per la **prestazione transfrontaliera di servizi** per le cripto-attività, l'articolo 58 stabilisce i dettagli e le modalità con cui le **informazioni sulle attività transfrontaliere** delle cripto-attività dovrebbero essere comunicate dall'autorità competente dello Stato membro d'origine a quella dello Stato membro ospitante.

Il capo 2 stabilisce **requisiti applicabili a tutti i fornitori di servizi** per le cripto-attività, applicando un modello normativo analogo a quello previsto dalla MiFID per fornitori di servizi relativi a strumenti finanziari, pur con previsioni caratterizzate da un minore dettaglio. Vengono definiti degli obblighi generali di comportamento quali l'obbligo di **agire in modo onesto, corretto, trasparente e professionale secondo il migliore interesse dei loro clienti effettivi e potenziali** (articolo 59), requisiti **prudenziali** (articolo 60 e allegato IV), requisiti **organizzativi** (articolo 61), norme sulla **custodia** delle cripto-attività e dei fondi dei clienti (articolo 63), l'obbligo di istituire una procedura di **trattamento dei reclami** (articolo 64), norme sul **conflitto di interesse** (articolo 65) e norme sull'**esternalizzazione di funzioni operative** (66). Il titolo V, capo 3, stabilisce i **requisiti per servizi specifici: custodia** delle cripto-attività (articolo 67), **piattaforme di negoziazione** delle cripto-attività (articolo 68), **scambio** di cripto-attività con una moneta fiduciaria o altre cripto-attività (articolo 69), **esecuzione di ordini** (articolo 70), **collocamento** di cripto-attività (articolo 71), **ricezione e trasmissione di ordini** per conto di terzi (articolo 72) e **consulenza** sulle cripto-attività (articolo 73). Il capo 4 stabilisce le **norme applicabili all'acquisizione di partecipazioni societarie in fornitori di servizi per le cripto-attività** ricalcando la disciplina già dettata per gli emittenti (articoli 37-38): l'articolo 74 prevede degli **obblighi di comunicazione delle partecipazioni rilevanti** e descrive la **valutazione di un progetto di acquisizione da parte dell'autorità competente ai fini dell'eventuale esercizio del potere di opposizione.** Gli specifici **elementi di valutazione** (reputazione, solidità finanziaria, conformità normativa, in particolare connessa ai fenomeni del riciclaggio e finanziamento del terrorismo) contenuto di tale valutazione sono dettagliati dall'articolo 75.

Integrità dei mercati

Il **titolo VI** introduce **divieti e obblighi** che si applicano agli **atti compiuti da qualsiasi persona e riguardanti le cripto-attività ammesse alla negoziazione** su una piattaforma di negoziazione di cripto-attività gestita da un fornitore di servizi autorizzato o per le quali è stata presentata una domanda di ammissione alla negoziazione (articolo 76). L'**articolo 77** definisce la nozione di **informazione privilegiata** e introduce l'**obbligo** per l'emittente le cui cripto-attività sono ammesse alla negoziazione su una piattaforma di negoziazione di cripto-attività **di divulgazione delle**

informazioni privilegiate in modo da consentire al pubblico di accedervi agevolmente e di valutarle in modo completo, corretto e tempestivo. L'utilizzo diretto e indiretto di tali informazioni prima della divulgazione ai fini della negoziazione è vietato (articolo 78), come la divulgazione illecita di informazioni privilegiate (articolo 79) e la **manipolazione informativa e operativa del mercato** attraverso condotte esemplificate nell'elenco non esaustivo recato dall'articolo 80.

Autorità nazionali competenti

Il **titolo VII** fornisce informazioni dettagliate sui **poteri delle autorità nazionali competenti, dell'ABE e dell'ESMA**. Il titolo VII, capo 1, impone agli Stati membri l'obbligo di **designare** una o più autorità competenti e, in tale secondo caso, un'autorità designata come punto di contatto unico (articolo 81). L'articolo 82 contiene un **elenco dei poteri minimi** (informativi, ispettivi e di intervento) che devono essere riconosciuti autorità nazionali competenti per vigilare sulla piena attuazione del regolamento, regole sulla **cooperazione tra le autorità designate** (articolo 83), con l'ABE e l'ESMA (articolo 84) o con **altre autorità** non designate (articolo 85). Vengono precisati gli obblighi di **notifica degli Stati membri** rispetto alle istituzioni europee (articolo 86) e le norme in materia di segreto d'ufficio (articolo 87), protezione dei dati (articolo 88) e **misure precauzionali** che possono essere adottate dalle autorità nazionali competenti degli Stati membri ospitanti (articolo 89). L'articolo 90 stabilisce le norme sulla cooperazione con i Paesi terzi, in particolare attraverso la stipula di appositi accordi, e l'articolo 91 specifica il **trattamento delle segnalazioni di presunte violazioni inviate da clienti e altre parti interessate alle autorità competenti**.

Il **titolo VII**, capo 2, indica agli Stati membri l'ambito delle condotte violative per le quali, conformemente al diritto nazionale, è necessario provvedere ad istituire **sanzioni e misure amministrative** che possono essere adottate dalle autorità competenti, con esplicitazione della forbice edittale (articolo 92) e vengono inoltre dettati i **parametri di cui tenere conto per stabilire il tipo e il livello delle sanzioni e delle altre misure amministrative** (articolo 93). L'articolo 94 impone agli Stati membri di provvedere affinché qualsiasi **decisione** adottata in applicazione del presente regolamento sia adeguatamente **motivata e soggetta al diritto di impugnazione giurisdizionale**. In generale, viene prevista la **pubblicazione delle decisioni**, ad eccezione dei casi espressamente citati dall'articolo 95, la **segnalazione delle sanzioni all'ABE e all'ESMA** (articolo 96), nonché la **segnalazione di violazioni (whistleblowing)** e la protezione delle persone che segnalano tali violazioni (articolo 97).

Responsabilità dell'ABE

Il **titolo VII**, capo 3, assegna all'ABE la **vigilanza sugli emittenti di TCA significativi ed affianca l'autorità europea a quelle nazionali per i TME significativi** (articolo 98) e detta le norme per la definizione di **collegi delle autorità di vigilanza per gli emittenti di TCA significativi** (articolo 99). Il collegio è composto, tra l'altro, dall'autorità competente dello Stato membro d'origine in cui l'emittente dei TCA ha ricevuto l'autorizzazione, dall'ABE, dall'ESMA e dalle **autorità competenti** che esercitano la vigilanza sulle **piattaforme di negoziazione delle cripto-attività più rilevanti**, sui **depositari** e sugli **enti creditizi** che forniscono servizi connessi ai TCA significativi, nonché dalla **BCE**. Se l'emittente di TCA significativi è stabilito in uno Stato membro la cui moneta non è l'euro, o nel caso in cui nelle attività di riserva figura una valuta diversa dall'euro, la banca centrale nazionale di tale Stato membro fa parte del collegio. Le autorità competenti che non fanno parte del collegio possono chiedere a quest'ultimo tutte le informazioni pertinenti per l'esercizio delle loro funzioni di vigilanza. L'articolo 99 descrive inoltre il modo in cui l'ABE, in cooperazione con l'ESMA e il

Sistema europeo di banche centrali, deve elaborare **progetti di norme tecniche di regolamentazione per determinare le piattaforme di negoziazione e i depositari più rilevanti** e i dettagli delle modalità pratiche di funzionamento del collegio. L'articolo 100 conferisce al **collegio** il potere di formulare **pareri non vincolanti**. Tali pareri possono riguardare, tra l'altro, l'obbligo per un emittente di detenere un importo più elevato di fondi propri, la modifica di un *WP* sulle cripto-attività, la revoca prevista dell'autorizzazione, l'accordo per lo scambio di informazioni previsto con un'autorità di vigilanza di un Paese terzo. Le autorità competenti o l'ABE tengono debitamente conto dei pareri del collegio e, qualora non concordino con il parere, ivi comprese le eventuali raccomandazioni, la loro decisione definitiva contiene spiegazioni su qualsiasi scostamento significativo dal parere o dalle raccomandazioni.

Il modello di vigilanza differenziato per cui l'ABE è responsabile della vigilanza dei TCA significativi mentre per quanto riguarda i TME è responsabile esclusivamente per il rispetto dei parametri da cui dipende l'inquadramento del soggetto fra quelli di maggiori dimensioni è stato **oggetto dei rilievi della BCE** nell'ambito del parere rilasciato sulla proposta. La BCE ha sottolineato come nel caso in cui l'emittente di TME sia anche un ente creditizio i soggetti responsabili della vigilanza sarebbero tre (BCE, ABE, autorità nazionale).

L'**articolo 101** stabilisce le norme in materia di **collegi delle autorità di vigilanza per gli emittenti di TME significativi** (tra i partecipanti aggiuntivi figurano le **autorità competenti per gli istituti di pagamento** più rilevanti che forniscono **servizi di pagamento** in relazione ai TME significativi), e l'articolo 102 conferisce a tale collegio il potere di emettere pareri non vincolanti.

Il capo 4 specifica i **poteri e le competenze di vigilanza dell'ABE**, che devono essere esercitati nel rispetto del segreto professionale degli operatori del diritto (articolo 103): richiesta di **informazioni** (articolo 104), poteri di **indagine** generali (articolo 105), **ispezioni in loco** (articolo 106), **scambio di informazioni** (articolo 107), accordo sullo scambio di informazioni con Paesi terzi (articolo 108), comunicazione di informazioni da Paesi terzi (articolo 109) e cooperazione con altre autorità (articolo 110). All'articolo 111 applica all'ABE l'obbligo del segreto d'ufficio, mentre all'articolo 112 sono menzionate le **misure di vigilanza che l'ABE può intraprendere in caso di violazione delle disposizioni del regolamento**. Le **sanzioni amministrative e altre misure**, in particolare le sanzioni amministrative pecuniarie, sono **specificate all'articolo 113**, e gli articoli conseguenti disciplinano le sanzioni per la **reiterazione** dell'inadempimento (articolo 114), la **comunicazione al pubblico**, la **natura e l'applicazione** delle sanzioni amministrative pecuniarie (articolo 115) e le corrispondenti norme procedurali per l'adozione di misure di vigilanza e l'imposizione di sanzioni amministrative pecuniarie (articolo 116). L'articolo 117 e l'articolo 118 stabiliscono rispettivamente i requisiti per **l'audizione delle persone interessate e la competenza giurisdizionale anche di merito della Corte di giustizia sulle decisioni dell'ABE**. Conformemente all'articolo 119, l'ABE dovrebbe poter imporre agli emittenti significativi il pagamento di **contributi di vigilanza** sulla base di un atto delegato adottato a norma del regolamento. L'articolo 120 conferisce all'ABE il potere di **delegare specifiche funzioni di vigilanza alle autorità competenti**, ove necessario per la vigilanza adeguata di un emittente significativo.

L'**esercizio della delega da parte Commissione** è disciplinato dal titolo VIII. La proposta di regolamento conferisce alla Commissione il potere di adottare atti delegati per specificare alcuni elementi, requisiti e disposizioni secondo quanto stabilito dal regolamento (articolo 121).

Il **titolo IX** contiene le **disposizioni transitorie e finali**, compreso l'obbligo per la Commissione di redigere una **relazione di valutazione dell'impatto del regolamento** (articolo 122). Le misure

transitorie, che comprendono una clausola di salvaguardia per gli *utility token* emessi prima dell'entrata in vigore del regolamento. L'articolo 124 modifica la direttiva riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione (direttiva sul "*whistleblowing*") aggiungendovi il regolamento e l'articolo 125 specifica che tale modifica deve essere recepita nel diritto nazionale 12 mesi dopo l'entrata in vigore del regolamento. L'articolo 126 stabilisce che il regolamento **diviene applicabile 18 mesi dopo la sua entrata in vigore**, ad eccezione delle **disposizioni relative ai TME e ai TCA, che divengono applicabili alla data di entrata in vigore del regolamento**.

Relazione del Governo

Nella Relazione predisposta ai sensi dell'articolo 6 della legge n. 234 del 2012 il Governo valuta che la **proposta rispetti il principio di attribuzione, il principio di sussidiarietà e di proporzionalità**. La valutazione delle finalità generali del progetto è complessivamente positiva e le disposizioni contenute nel progetto possono ritenersi conformi all'interesse nazionale. Rispetto ai tempi necessari per l'adozione viene segnalata da una parte l'opportunità di un'attenta valutazione degli elementi da regolare e, dall'altra, l'esigenza di tutela dei consumatori e degli investitori e di salvaguardia della stabilità finanziaria, da cui dipende una "moderata urgenza" di adozione del progetto.

Con riferimento alle prospettive negoziali, il Governo rappresenta che la proposta di regolamento è stata oggetto di una presentazione, a cura della Commissione europea, il 29 settembre 2020, in occasione della quale si è svolto anche il primo *meeting* del *Working Party on Financial Services (Crypto Assets)* al quale partecipano, in qualità di membri, esponenti del Ministero dell'Economia e delle Finanze (MEF) e della Rappresentanza Permanente d'Italia presso l'Unione Europea. Successivamente sono stati svolti altri **tre incontri del Working Party** (29 ottobre, 11 e 24 novembre 2020) in occasione dei quali la delegazione italiana ha presentato la **posizione nazionale**, fornendo risposta ai quesiti formulati in relazione alle singole disposizioni del regolamento. I riscontri forniti dalla delegazione italiana ai quesiti oggetto dei singoli Working Party sono successivamente stati trasmessi, in forma scritta, alla Presidenza dell'UE.

Le attività di definizione della posizione italiana sono state condotte dal **MEF nell'ambito di un costante coordinamento e collaborazione con Banca d'Italia e Consob**, nella loro qualità di autorità di settore e in relazione all'incidenza della proposta su profili di competenza delle stesse. In merito al Titolo I (Oggetto, ambito di applicazione e definizioni), è stata sottolineata la **necessità di una più puntuale definizione dell'ambito di applicazione del regolamento** al fine di distinguere tra le cripto-attività ricomprese nello stesso e strumenti finanziari oggetto di disciplina della direttiva MiFID, da realizzarsi tramite la previsione di misure normative di secondo livello (atti delegati). È stato suggerito di adottare un approccio fondato sulla funzione economica degli *asset*, al fine di chiarire le definizioni di *token* collegato ad attività (TCA), *token* di moneta elettronica (TME) e *utility token* e le relative discipline applicabili. Con specifico riferimento alla categoria dei TCA, è stata manifestata la necessità di **chiarire la possibile funzione di pagamento associata agli stessi** (anche alla luce dei profili di interrelazione con la funzione di investimento) e l'individuazione delle disposizioni applicabili.

Per quanto riguarda il Titolo II (Cripto-attività diverse dai *token* collegati ad attività o dai *token* di moneta elettronica), è stata rappresentata la necessità di **definire il trattamento giuridico degli emittenti** di cripto-attività diversi dalle persone giuridiche.

In merito al Titolo III (*Token* collegati ad attività), è stata sottolineata la **necessità di potenziare i presidi di tutela della stabilità finanziaria e degli utenti**, mediante il **rafforzamento degli obblighi inerenti alla riserva di attività** sottostanti e della **definizione dei diritti dei possessori dei *token***.

In relazione al Titolo VII (Autorità competenti, ABE ed ESMA), è stato richiesto di **definire specificamente la ripartizione di ruoli e responsabilità tra autorità europee e nazionali**, in particolare nel caso dei TCA significativi. Per quanto riguarda le disposizioni transitorie e finali, inoltre, sono state segnalate le potenziali criticità, alla luce dell'obiettivo di garantire una tutela completa di consumatori e investitori, riferite alla misura transitoria di cui all'articolo 123, paragrafo 1, della proposta, il quale prevede la non applicazione dei Titoli I e II alle cripto-attività diverse dai *token* collegati ad attività e dai *token* di moneta elettronica, offerte al pubblico nell'Unione o ammesse alla negoziazione su una piattaforma di negoziazione di cripto-attività prima della data di applicazione del regolamento. Al riguardo, la delegazione italiana ha pertanto segnalato un **rischio connesso alla scelta di non applicare, in tali casi, i presidi di cui ai Titoli I e II del regolamento**.

Con riferimento ai predetti ambiti, il Governo segnala che nel corso dei negoziati anche **numeroso altre delegazioni nazionali hanno sostenuto la necessità di definire più chiaramente l'ambito di applicazione della proposta di regolamento** in relazione alla nozione di cripto-attività e al trattamento giuridico degli emittenti di cripto-attività diversi dalle persone giuridiche, oltre a formulare osservazioni e proposte in ordine alla **disciplina dei TCA** e alla **ripartizione delle funzioni di vigilanza tra autorità europee e nazionali**.

COM(2020) 594 final

Proposta di REGOLAMENTO relativo ad un regime pilota per le infrastrutture di mercato basate sulla tecnologia di registro distribuito

La Comunicazione della Commissione europea su una strategia per la finanza digitale sostiene l'adozione di proposte legislative che innovino il diritto dell'Unione in materia di servizi finanziari per consentire di **cogliere i vantaggi tecnologici dell'era digitale dell'economia, affrontando i relativi rischi**. L'Unione ha manifestato un deciso interesse politico a sviluppare e a **promuovere la diffusione di tecnologie trasformative nel settore finanziario**, quali la *blockchain* e più in generale la tecnologia di registro distribuito ("DLT"), ovvero la "classe di tecnologie che supportano la registrazione distribuita di dati cifrati". Le **cripto-attività costituiscono una delle principali applicazioni della DLT al settore finanziario e pertanto la proposta è strettamente collegata a quella che modifica la MiFID per includervi gli strumenti finanziari gestiti mediante DLT nonché, come complemento logico, alla proposta che regola i mercati delle altre cripto-attività**.

La proposta mira a stabilire un "regime pilota" caratterizzato da **requisiti uniformi** per gli operatori di mercato che desiderano gestire un'infrastruttura di mercato DLT. Le autorizzazioni concesse a norma di tale regolamento consentirebbero agli operatori di mercato di gestire un'infrastruttura di mercato DLT e di prestare i loro servizi in tutti gli Stati membri.

L'**articolo 1** definisce l'oggetto e l'ambito di applicazione. In particolare, tale regolamento stabilisce le **condizioni operative per le infrastrutture di mercato basate sulla DLT**, le **autorizzazioni** ad avvalersene nonché la vigilanza e la collaborazione delle autorità competenti e dell'ESMA. Il

regolamento si applica agli **operatori** di mercato: **imprese di investimento, gestori del mercato e depositari centrali di titoli** (CSD) autorizzati a norma dell'articolo 7 o 8. L'articolo 2 stabilisce i termini e le **definizioni**. La "**infrastruttura di mercato DLT**" è composta da "**sistemi multilaterali di negoziazione DLT**" ("MTF DLT"), gestiti da un'impresa di investimento o da un gestore del mercato, che ammettono alla negoziazione solo valori mobiliari DLT, e che sono autorizzati, sulla base di regole e procedure trasparenti, non discrezionali e uniformi, ad assicurare la registrazione iniziale dei valori; regolarne le operazioni contro pagamento e prestare servizi di custodia, o da un "**sistema di regolamento titoli DLT**" gestito da un depositario centrale di titoli che regola le operazioni in valori mobiliari DLT contro pagamento. I "**valori mobiliari DLT**" sono azioni, obbligazioni e strumenti derivati standardizzati e normalmente negoziati come definiti dalla MIFID emessi, registrati, trasferiti e stoccati mediante DLT.

L'articolo 3 descrive le **limitazioni imposte ai valori mobiliari DLT** che possono essere ammessi alla negoziazione sulle infrastrutture di mercato DLT o registrati da queste ultime. Per quanto riguarda le **azioni**, la capitalizzazione di mercato, anche provvisoria, dell'emittente di valori mobiliari DLT dovrebbe essere **inferiore a 200 milioni di euro**; per le **obbligazioni** pubbliche diverse da quelle sovrane, le obbligazioni garantite e le obbligazioni societarie, il limite è di **500 milioni di euro**. Le infrastrutture di mercato DLT **non ammettono alla negoziazione né registrano obbligazioni sovrane ma possono trattare altre obbligazioni pubbliche**, emesse, ad esempio, da una società veicolo per diversi Stati membri, dalla Banca europea per gli investimenti (BEI) o dal Meccanismo di stabilità europea (MES). Il **valore totale** di mercato dei valori mobiliari DLT registrati da un'infrastruttura di mercato DLT autorizzata a operare nel "regime pilota" istituito dalla proposta in esame **non dovrà superare i 2,5 miliardi di euro**.

L'**articolo 4** stabilisce i **requisiti di un MTF che opera con la tecnologia del registro distribuito DLT**. Si tratta degli stessi requisiti previsti per un MTF ai sensi della direttiva MiFID, anche se il regime ordinario viene affiancato da un regime che rende possibile operare in **esenzione** nel rispetto comunque di specifici obblighi di conformità dettati dal regolamento e dall'autorità competente, in modo da garantire comunque la tutela degli investitori, l'integrità del mercato e la stabilità finanziaria. L'articolo 5 stabilisce i **requisiti di un CSD che gestisce un sistema di regolamento titoli DLT**, che sono gli stessi applicabili ai CSD ai sensi del regolamento (UE) n. 909/2014. Anche in questo caso viene previsto uno specifico regime di operatività in esenzione.

L'**articolo 6** stabilisce i **requisiti aggiuntivi applicabili alle infrastrutture di mercato DLT per far fronte alle nuove forme di rischio derivanti dall'uso della tecnologia di registro distribuito**. Le infrastrutture di mercato DLT devono fornire a tutti i membri, gli operatori, i clienti e gli investitori informazioni chiare sulle modalità di svolgimento delle loro funzioni, di prestazione dei loro servizi e di esercizio delle loro attività e su come esse si differenziano da un MTF o un CSD tradizionale. Le infrastrutture di mercato DLT devono inoltre garantire che tutti i dispositivi informatici e cibernetici relativi all'uso della DLT siano adeguati. Qualora il modello di *business* di un'infrastruttura di mercato DLT preveda la custodia di fondi dei clienti o di valori mobiliari DLT, o i mezzi per accedervi, essi devono disporre di dispositivi adeguati per salvaguardare tali attività.

Gli **articoli 7 e 8** stabiliscono la **procedura di autorizzazione** specifica a gestire rispettivamente un MTF DLT e un sistema di regolamento titoli DLT ed elencano dettagliatamente le informazioni che devono essere trasmesse all'autorità competente.

L'**articolo 9** definisce le **modalità di collaborazione tra l'infrastruttura di mercato DLT, le autorità competenti e l'ESMA**. Ad esempio, le infrastrutture di mercato DLT devono informare le

autorità competenti e l'ESMA sulle proposte di modifiche sostanziali al piano aziendale, tra cui personale critico, prove di pirateria informatica, frodi o altri gravi abusi, su modifiche sostanziali alle informazioni contenute nella domanda iniziale, sulle difficoltà operative o tecniche intervenute durante lo svolgimento di attività o di servizi contemplati dall'autorizzazione e su eventuali rischi per la tutela degli investitori, l'integrità del mercato o la stabilità finanziaria che potrebbero essere emersi e che non erano previsti al momento di concedere l'autorizzazione. In caso di notifica di tali informazioni, l'autorità competente può chiedere all'infrastruttura di mercato DLT di presentare domanda per ottenere un'altra autorizzazione, un'altra esenzione o adottare qualsiasi misura correttiva che ritenga opportuna. L'infrastruttura di mercato DLT è tenuta a fornire le informazioni richieste all'ESMA e all'autorità competente che ha concesso l'autorizzazione. L'autorità competente, previa consultazione dell'ESMA, può raccomandare all'infrastruttura di mercato DLT misure correttive volte a garantire la tutela degli investitori, l'integrità del mercato o la stabilità finanziaria. L'infrastruttura di mercato DLT deve specificare in che modo si conformerà a tali misure. Inoltre l'infrastruttura di mercato DLT dovrà redigere e presentare all'autorità competente e all'ESMA una relazione contenente tutte le informazioni suddette, comprese le potenziali difficoltà nell'applicare la legislazione dell'UE in materia di servizi finanziari. L'ESMA dovrà informare regolarmente tutte le autorità competenti in merito alle suddette relazioni redatte dalle infrastrutture di mercato DLT e alle esenzioni concesse a norma degli articoli 7 e 8, monitorare l'applicazione di tali esenzioni e presentare alla Commissione una relazione annuale sulle modalità di applicazione pratica.

L'articolo 10 specifica che, **dopo un periodo massimo di cinque anni, l'ESMA presenterà alla Commissione una relazione dettagliata sul "regime pilota"**. Sulla base della valutazione dell'ESMA, la Commissione redigerà una relazione comprendente un'analisi costi-benefici per stabilire se il regime pilota debba essere mantenuto o modificato, se debba essere esteso in termini qualitativi e quantitativi, se si debbano prendere in considerazione modifiche mirate da apportare alla legislazione dell'UE per consentire un utilizzo diffuso della DLT e se il regime pilota debba essere soppresso.

L'articolo 11 stabilisce che il regolamento si applicherà 12 mesi dopo la sua entrata in vigore.

Relazione del Governo

Nella Relazione predisposta ai sensi dell'articolo 6 della legge n. 234 del 2012 il Governo valuta che **la proposta rispetti il principio di attribuzione, il principio di sussidiarietà e di proporzionalità**. La valutazione delle finalità generali del progetto è complessivamente positiva e le disposizioni vengono ritenute conformi all'interesse nazionale. Con riferimento alle prospettive negoziali, nell'accogliere con favore l'iniziativa della Commissione il Governo fa presente che occorrerebbe **maggiore chiarezza rispetto ai modelli di business che possono essere oggetto di sperimentazione** nell'ambito del regime pilota, valutando l'apertura a ulteriori entità rispetto agli MTF e ai CSD. Ulteriori chiarimenti vengono ritenuti necessari con riferimento alle **soglie per l'individuazione dei valori mobiliari ammessi**. Per quanto riguarda le **esternalizzazioni** di funzioni viene sottolineata l'opportunità di estendere le regole previste per gli MTF anche alla fase di *post-trading*. Il Governo ritiene inoltre necessaria la definizione di **ulteriori presidi in relazione all'accesso alle infrastrutture di mercato da parte delle persone fisiche**, nonché regole riguardanti le verifiche che i soggetti vigilati sono tenuti a effettuare. In generale, viene sottolineata la necessità di **regole più dettagliate con riferimento alle esenzioni** e di un **maggiore coordinamento con la proposta MICA**.

COM(2020) 595 final

Proposta di REGOLAMENTO relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014

La Commissione parte dal presupposto che nell'era digitale le **tecnologie dell'informazione e della comunicazione (TIC) sostengono sistemi complessi impiegati nelle quotidiane attività sociali**. Mantengono in funzione i principali settori delle nostre economie, tra cui la finanza, e migliorano il funzionamento del mercato unico. Il crescente grado di digitalizzazione e interconnessione amplifica d'altra parte l'impatto potenziale di circostanze negative relative alle TIC, rendendo l'intera società, e in particolare il sistema finanziario, più **vulnerabile alle minacce informatiche o ai rischi legati a disfunzioni delle TIC**. A fronte di tale assunto, la Commissione ritiene che **la resilienza digitale non sia ancora sufficientemente integrata nei loro quadri operativi**. Con particolare riferimento alla finanza, la digitalizzazione è divenuta un fattore cruciale per i pagamenti, la compensazione e il regolamento dei titoli, la negoziazione elettronica e algoritmica, le operazioni di prestito e finanziamento, il *crowdfunding* e il *peer-to-peer lending*, i *rating* del credito, la sottoscrizione di assicurazioni, la gestione dei crediti e le operazioni di *back-office* degli operatori, anche di coloro che continuano ad avere tecniche di interazione tradizionale con la clientela. Non solo l'intero settore finanziario è diventato in larga misura digitale, ma la digitalizzazione ha anche approfondito le interconnessioni e le dipendenze all'interno del settore e nei confronti di infrastrutture di terzi e fornitori terzi di servizi.

La proposta della Commissione si articola in vari settori d'intervento principali, che costituiscono pilastri ritenuti essenziali per **promuovere la resilienza informatica e operativa del settore finanziario**.

Ambito di applicazione del regolamento e applicazione proporzionale delle misure richieste

L'oggetto fondamentale della proposta sono gli **obblighi applicabili alle entità finanziarie in materia di gestione dei rischi delle TIC, segnalazione alle autorità competenti degli incidenti gravi connessi alle TIC, test di resilienza operativa digitale, condivisione di dati e di informazioni in relazione alle vulnerabilità** e alle minacce informatiche, misure relative a una **solida gestione** da parte delle entità finanziarie dei **rischi relativi alle TIC derivanti da terzi**. Con riferimento ai fornitori di servizi, sono inoltre oggetto di regolazione gli **obblighi relativi agli accordi contrattuali** stipulati tra fornitori terzi di servizi di TIC ed entità finanziarie e il **quadro di sorveglianza per i fornitori terzi** di servizi di TIC critici, allorché forniscono i loro servizi a entità finanziarie (**articolo 1**).

Per quanto riguarda l'**ambito soggettivo (articolo 2)**, il regolamento include un **insieme estremamente ampio di entità finanziarie regolamentate a livello di Unione**: enti creditizi, istituti di pagamento, istituti di moneta elettronica, imprese di investimento, fornitori di servizi per le crypto-attività, depositari centrali di titoli, controparti centrali, sedi di negoziazione, repertori di dati sulle negoziazioni, gestori di fondi di investimento, fornitori di servizi di comunicazione dati, imprese di assicurazione e di riassicurazione, intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio, enti pensionistici aziendali o professionali, agenzie di *rating* del credito, revisori legali e società di revisione, amministratori di indici di riferimento critici e fornitori di servizi di *crowdfunding*.

L'ampiezza dell'ambito soggettivo ha l'obiettivo di **favorire l'applicazione omogenea e coerente** di tutte le componenti della gestione del rischio nei settori connessi alle TIC, salvaguardando contemporaneamente la parità di condizioni tra le entità finanziarie per quanto riguarda gli obblighi normativi in materia di rischi relativi alle TIC. Allo stesso tempo il regolamento riconosce l'esistenza di differenze significative tra le entità finanziarie in termini di dimensioni, profilo commerciale o esposizione al rischio digitale. Per introdurre un **principio di proporzionalità** degli obblighi imposti, le microimprese vengono esentate, ad esempio, dall'introduzione di complesse disposizioni di *governance* e funzioni di gestione dedicate, dall'effettuazione di valutazioni approfondite dopo modifiche di rilievo delle infrastrutture di reti e dei sistemi informativi e da altri obblighi che potrebbero risultare non pertinenti con riferimento a strutture organizzative di ridotte dimensioni. Inoltre solo le entità finanziarie identificate come significative ai fini dei **test avanzati di resilienza digitale dovranno svolgere test di penetrazione basati su minacce** (tale tipologia di test è definita dalla proposta come "un quadro che imita le tattiche, le tecniche e le procedure messe in atto nella vita reale dagli autori delle minacce e percepite come minaccia informatica autentica, che consente di eseguire un *test* controllato, mirato e fondato su dati dei reali sistemi di produzione critici dell'entità"). Nonostante l'ampio ambito di applicazione soggettivo, restano esclusi gli operatori dei sistemi di pagamento e di regolamento titoli (direttiva sul carattere definitivo del regolamento), a meno che non si tratti di entità finanziarie regolamentate a livello di Unione, nonché gli operatori del mercato delle quote di emissioni. Tali esclusioni non sono tuttavia definitive ma la Commissione ritiene che sia necessario un maggiore approfondimento sulle implicazioni che riguardano anche le banche centrali. **L'articolo 3 definisce i principali elementi normativi.**

Responsabilità e coinvolgimento degli organi di governo societario

La proposta (**articolo 4**) intende favorire una maggiore omogeneità nelle strategie commerciali delle entità finanziarie e della gestione dei rischi relativi alle TIC. A tale scopo, il regolamento prevede che l'organo di gestione sia tenuto a mantenere un ruolo attivo e cruciale nel dirigere il quadro di gestione dei rischi relativi alle TIC e debba garantire il rispetto di una scrupolosa "igiene informatica". La piena responsabilità dell'organo di gestione nella gestione dei rischi relativi alle TIC dell'entità finanziaria costituisce un principio generale da cui derivano prescrizioni specifiche, come l'attribuzione di **responsabilità e ruoli precisi per tutte le funzioni relative alle TIC**, l'impegno costante nel **controllo del monitoraggio** della gestione dei rischi relativi alle TIC nonché l'intera gamma di processi di approvazione e controllo e l'adeguata allocazione di investimenti e formazione relativi alle TIC.

Prescrizioni relative alla gestione dei rischi relativi alle TIC

La **resilienza operativa digitale si fonda su una serie di prescrizioni e principi chiave concernenti il quadro di gestione dei rischi relativi alle TIC**, conformemente al parere tecnico congiunto delle autorità europee di vigilanza (AEV). Tali prescrizioni (articoli da 5 a 14), che la Commissione ha definito sulla base delle pertinenti norme, linee guida e raccomandazioni fissate a livello internazionale, nazionale e settoriale, vertono su **funzioni specifiche nella gestione dei rischi relativi alle TIC** (identificazione, protezione e prevenzione, individuazione, risposta e ripristino, apprendimento, evoluzione e comunicazione). Per tenere il passo con il rapido sviluppo del contesto delle minacce informatiche, le entità finanziarie devono: **istituire e mantenere strumenti e sistemi di TIC resilienti**, tali da ridurre al minimo l'impatto dei rischi relativi alle TIC; **identificare costantemente tutte le fonti di rischi relativi alle TIC**; **introdurre misure di protezione e prevenzione**; **individuare tempestivamente le attività anomale**; mettere in atto **strategie di**

continuità operativa e piani di ripristino in caso di incidenti come parte integrante della strategia di continuità operativa, in particolare in caso di attacchi informatici, limitando i danni e privilegiando una ripresa sicura delle attività. Il regolamento **non impone una standardizzazione specifica**, ma si fonda su **norme tecniche riconosciute a livello europeo e internazionale** e sulle **migliori pratiche del settore**, nella misura in cui queste siano pienamente conformi alle istruzioni delle autorità di vigilanza sull'utilizzo e l'integrazione di tali norme internazionali. L'articolo 14 prevede che le AEV elaborino progetti di norme tecniche di regolamentazione per specificare ulteriori elementi da inserire nelle politiche, nelle procedure, nei protocolli e negli strumenti in materia di sicurezza, prescrivere le modalità, specificare ulteriormente le tecniche, i metodi e i protocolli adeguati di prevenzione ed elaborare ulteriormente gli elementi relativi a individuazione delle attività anomale, strategie di continuità operativa e piani di ripristino. Il regolamento si occupa altresì dell'integrità, la sicurezza e la resilienza delle **infrastrutture e attrezzature fisiche che supportano l'uso della tecnologia** nonché del **personale e dei processi collegati alle TIC**, nell'ambito dell'impronta digitale delle operazioni delle entità finanziarie.

Segnalazione di incidenti connessi alle TIC (articoli da 15 a 20)

L'**articolo 15** prevede una **prescrizione generale che impone alle entità finanziarie di stabilire e attuare un processo di gestione per monitorare e registrare gli incidenti connessi alle TIC**, seguita dall'obbligo di **classificare gli incidenti** sulla base di criteri precisati nel regolamento e ulteriormente definiti dalle AEV per **specificare le soglie di rilevanza**. L'obbligo di segnalazione alle autorità competenti riguarda esclusivamente gli incidenti connessi alle TIC ritenuti gravi. Per il trattamento della segnalazione dovrebbe essere utilizzato un modello comune, seguendo una procedura armonizzata messa a punto dalle AEV. Le entità finanziarie dovrebbero inviare segnalazioni iniziali, intermedie e finali, informando utenti e clienti qualora l'incidente abbia o possa avere un impatto sui loro interessi finanziari. Le autorità competenti devono fornire dettagli pertinenti sugli incidenti ad altre istituzioni o autorità: le AEV, la BCE e i punti di contatto unici designati ai sensi della direttiva (UE) 2016/1148 (direttiva NIS - *Network and Information Security*). Per avviare tra entità finanziarie e autorità competenti un dialogo che contribuisca a ridurre al minimo l'impatto e a individuare i rimedi opportuni, la segnalazione degli incidenti gravi connessi alle TIC dovrebbe essere integrata da riscontri e orientamenti delle autorità di vigilanza. Nella relazione illustrativa dell'atto, la Commissione fa presente inoltre che **occorre esplorare ulteriormente la possibilità di centralizzare a livello di Unione le segnalazioni di incidenti connessi alle TIC**, mediante una relazione congiunta delle AEV, della BCE e dell'ENISA che valuti la fattibilità dell'istituzione di un polo unico dell'UE per la segnalazione degli incidenti gravi connessi alle TIC da parte delle entità finanziarie.

Test di resilienza operativa digitale

Le **capacità e le funzioni incluse nel quadro di gestione dei rischi** relativi alle TIC devono essere **sottoposte periodicamente a test** per accertarne il grado di preparazione, identificarne punti deboli, carenze o lacune, verificarne la capacità di attuare tempestivamente misure correttive (**articoli da 21 a 24**). Il regolamento prevede un'applicazione orientata dal principio di **proporzionalità delle prescrizioni in materia di test di resilienza operativa digitale**, in funzione delle dimensioni e del profilo industriale e di rischio delle entità finanziarie: tutte le entità dovrebbero svolgere test sui sistemi e gli strumenti di TIC, ma solo quelle identificate dalle autorità competenti (in base ai criteri del regolamento, ulteriormente definiti dalle AEV) come significative e mature sotto il profilo informatico dovrebbero avere l'obbligo di svolgere prove avanzate mediante test di penetrazione

basati su minacce. Il regolamento fissa anche **prescrizioni per i tester** esterni (articolo 24) e impone il riconoscimento in tutta l'Unione dei risultati dei test di penetrazione basati su minacce per le entità finanziarie operanti in vari Stati membri.

Rischi relativi alle TIC derivanti da terzi

Il regolamento prevede il **monitoraggio dei rischi relativi alle TIC derivanti da terzi (articoli da 25 a 39)**. Inoltre, **armonizza gli elementi essenziali del servizio e dei rapporti con i fornitori terzi** di TIC. Questi elementi coprono gli aspetti minimi considerati cruciali per consentire il monitoraggio completo, da parte dell'entità finanziaria, del rischio derivante da fornitori terzi di TIC in tutte le fasi del rapporto con tali fornitori: stipula, esecuzione, estinzione e fase post-contrattuale. In particolare, i contratti che disciplinano il rapporto dovranno contenere una descrizione completa dei servizi, l'indicazione delle località in cui i dati devono essere trattati, descrizioni complete del livello dei servizi accompagnate da obiettivi di prestazione quantitativi e qualitativi, disposizioni pertinenti in materia di accessibilità, disponibilità, integrità, sicurezza e protezione dei dati personali, nonché garanzie per l'accesso, il ripristino e la restituzione in caso di inadempienze dei fornitori terzi di servizi di TIC, termini di preavviso e obblighi di segnalazione dei fornitori terzi di servizi di TIC, diritti di accesso, ispezione e audit da parte dell'entità finanziaria o di un terzo designato a tale scopo, chiari diritti di estinzione e strategie di uscita dedicate. Dato che alcuni di questi elementi contrattuali possono essere standardizzati, il regolamento incoraggia il ricorso volontario a clausole contrattuali standard per l'utilizzo del servizio di *cloud computing* che dovranno essere definite dalla Commissione.

Il regolamento intende infine promuovere la **convergenza per quanto riguarda gli approcci di vigilanza ai rischi relativi alle TIC derivanti da terzi nel settore finanziario**, sottoponendo i fornitori terzi di servizi di TIC critici a un quadro di sorveglianza dell'Unione. Tramite un nuovo quadro legislativo armonizzato, all'AEV designata come autorità di sorveglianza capofila per ciascun fornitore terzo di servizi di TIC critico sono conferiti poteri idonei a garantire l'adeguato monitoraggio su scala paneuropea dei fornitori di servizi tecnologici che assolvono una funzione critica per il funzionamento del settore finanziario. Il quadro di sorveglianza previsto dalla proposta di regolamento **si fonda sull'architettura istituzionale esistente nel settore dei servizi finanziari, per cui il comitato congiunto delle AEV garantisce il coordinamento intersettoriale** in tutte le questioni concernenti i rischi relativi alle TIC, conformemente ai propri compiti in materia di cibersicurezza, coadiuvato dal sottocomitato pertinente (forum di sorveglianza) che svolge il lavoro preparatorio per le singole decisioni e per le raccomandazioni collettive rivolte ai fornitori terzi di servizi di TIC critici.

Condivisione delle informazioni

Per sensibilizzare in merito ai rischi relativi alle TIC, ridurre al minimo la propagazione, sostenere le capacità di difesa e le tecniche di individuazione delle minacce delle entità finanziarie, l'articolo 40 consente a queste ultime di stipulare accordi per scambiarsi informazioni e dati sulle minacce informatiche.

Relazione del Governo

Nella Relazione predisposta ai sensi dell'articolo 6 della legge n. 234 del 2012 il Governo valuta che la **proposta rispetti il principio di attribuzione, il principio di sussidiarietà e di proporzionalità**.

La valutazione delle finalità generali del progetto è complessivamente positiva e le disposizioni contenute nel progetto possono ritenersi conformi all'interesse nazionale.

Rispetto alle prospettive negoziali, il Governo fa presente che la proposta di regolamento è stata oggetto di una presentazione, a cura della Commissione europea, durante il primo incontro virtuale del *Working Party on Financial Services (Digital Operational Resilience)* tenutosi il 30 settembre 2020, al quale partecipano in qualità di membri rappresentanti del MEF e della Rappresentanza Permanente per l'Italia presso l'UE. Successivamente sono stati svolti altri **quattro incontri del Working Party** (22 e 28 ottobre, 9 e 27 novembre 2020) in occasione dei quali la delegazione italiana ha presentato la **posizione nazionale**, fornendo risposta ai quesiti formulati in relazione alle singole disposizioni del regolamento.

Le attività di definizione della posizione italiana e di redazione delle risposte ai quesiti presentati in occasione dei Working Party sono state condotte dal **MEF in costante coordinamento e collaborazione con Banca d'Italia e Consob**, nella loro qualità di autorità di settore ed in relazione all'incidenza della proposta su profili di competenza delle stesse.

Con riferimento al Capo I (Disposizioni generali), la posizione italiana è concorde con la proposta della Commissione, in particolare rispetto **all'esclusione dei sistemi di pagamento** da tale ambito, ritenendo che la scelta sia coerente con l'attuale quadro giuridico e di controllo, malgrado alcuni Stati membri abbiano espresso la volontà che essi vengano inclusi. L'inclusione di tali entità, però, secondo il Governo potrebbe portare in particolare a incertezza giuridica, poiché la definizione di sistema esistente, all'interno della direttiva concernente il carattere definitivo del regolamento nei sistemi di pagamento e nei sistemi di regolamento titoli, è molto ampia ed i sistemi di pagamento comprendono un insieme variegato di soggetti, sottoposti a discipline e regimi diversi all'interno dei vari Stati membri.

In riferimento al Capo II (Gestione dei rischi relativi alle TIC), viene ritenuto essenziale trovare un **giusto equilibrio tra il rafforzamento della sicurezza delle TIC e la riduzione dei costi e degli oneri amministrativi per gli enti finanziari**, attraverso l'efficace applicazione del criterio di proporzionalità e l'ulteriore specificazione dei criteri di applicazione, prendendo in considerazione non soltanto fattori legati alla "dimensione" delle entità finanziarie, ma anche fattori legati al relativo rischio.

In merito al Capo III (Incidenti connessi alle TIC), per quanto riguarda la **segnalazione di incidenti connessi alle TIC**, nella relazione viene sottolineata la necessità di un **maggior coordinamento tra il regolamento e la direttiva (UE) 2016/1148 (NIS - Network and Information Security)**, nonché una **migliore cooperazione tra autorità competenti secondo DORA e gli organismi esistenti nell'ecosistema NIS** (CSIRT, Punto di Contatto Unico ed Autorità Nazionali competenti NIS quali il MEF in collaborazione con Banca d'Italia e Consob per il settore finanziario). La proposta dovrebbe tenere conto del fatto che in alcuni Stati membri l'Operatore di Servizi Essenziali (OSE) segnala gli incidenti al CSIRT nazionale, comunicandolo allo stesso tempo all'Autorità Nazionale Competente NIS (che potrebbe non coincidere con l'autorità di vigilanza finanziaria). Considerando quanto sopra, la delegazione italiana ha suggerito di prevedere, in aggiunta alla segnalazione alle autorità competenti ai sensi di DORA, una **comunicazione da parte delle entità finanziarie alle altre autorità pertinenti (quali le autorità nazionali NIS)** in caso di grave incidente correlato alle TIC, in maniera tale da coprire tutte le attuali autorità competenti in materia. In alternativa, è stato proposto di includere nell'articolo 17 paragrafo 5 (c) del regolamento la disposizione secondo cui l'autorità competente ai sensi del regolamento debba fornire tempestivamente una comunicazione con i dettagli

dell'incidente non soltanto al Punto di Contatto Unico ma anche alle altre autorità nazionali competenti ai sensi della direttiva NIS.

In riferimento al Capo IV (Test di resilienza operativa digitale), la delegazione italiana ha sostenuto **l'applicazione del principio di proporzionalità** al fine di evitare oneri eccessivi per le entità più piccole, suggerendo al contempo **maggior chiarezza nella distinzione tra test avanzati e altri**. In particolare, per i test avanzati, la delegazione si è dimostrata favorevole alla menzione esplicita del **framework TIBER-EU come esempio e riferimento pertinente**, in quanto già operativo in diversi Paesi europei e rappresentante un modello di riferimento adatto per entità finanziarie di diversi settori in virtù della sua neutralità.

In relazione al Capo V (Gestione dei rischi relativi alle TIC derivanti da terzi), nell'ambito della vigilanza sui fornitori terzi di servizi TIC, viene segnalata la necessità di **precisare i criteri per la designazione dei fornitori**, specie situati in un Paese terzo, nonché di chiarezza in merito al ruolo e ai poteri delle AEV e ai poteri delle Autorità di vigilanza nazionali, già sanciti dalla normativa settoriale. Dal punto di vista della vigilanza bancaria e finanziaria, si è ritenuto che le disposizioni relative alla gestione del rischio TIC di terzi prevista dal regolamento dovrebbe evitare oneri eccessivi per gli enti finanziari e le Autorità di vigilanza competenti, nonché dovrebbero rimanere coerenti con le regole generali esistenti sull'esternalizzazione. Si è, inoltre, suggerito di condurre un'analisi di impatto *ad hoc* volta ad identificare, sulla base dei parametri e dei criteri previsti, i **fornitori terze parti di TIC che sarebbero considerati "critici"** e l'Autorità di sorveglianza capofila di riferimento per valutare se gli attuali parametri e criteri debbano essere rivisti. Infine, è stata rappresentata l'esigenza di **maggior chiarezza sulla relazione e il coordinamento tra il previsto quadro di controllo dell'UE e le attività e i poteri delle Autorità nazionali competenti**, particolarmente importante per i fornitori terze parti che servono settori anche non finanziari o diversi sotto settori finanziari.

Nel corso dei negoziati **anche diverse altre delegazioni nazionali hanno sostenuto la necessità di definire più chiaramente l'ambito di applicazione del principio di proporzionalità**, nonché una **maggior chiarezza nei criteri per la designazione dei fornitori terzi**.

COM(2020) 596 final

Proposta di DIRETTIVA che modifica le direttive 2006/43/CE, 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 e UE 2016/2341

L'ultima proposta del Pacchetto per la finanza digitale consiste in una direttiva volta a **integrare nell'ordinamento vigente la proposta di regolamento sulla resilienza operativa** e ad **includere nell'elenco degli strumenti finanziari previsto dalla MiFID il riferimento agli strumenti gestiti attraverso una DLT**.

In particolare, vengono modificati i vari **requisiti in materia di rischio operativo o di gestione del rischio** previsti dalle direttive 2006/43/CE, 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341, introducendo riferimenti incrociati precisi in tali disposizioni alla proposta di regolamento DORA. Più specificatamente:

– gli articoli da 2 a 4, 6 e 8 modificano la direttiva 2009/65/CE concernente il coordinamento delle disposizioni legislative, regolamentari e amministrative in materia di **organismi d'investimento collettivo in valori mobiliari (OICVM)**, la direttiva 2009/138/CE in materia di accesso ed esercizio delle attività di **assicurazione e di riassicurazione (Solvency II)**, la direttiva 2011/61/UE sui **gestori di fondi di investimento alternativi (AIFMD)**, la direttiva 2014/56/UE relativa alle **revisioni legali dei conti annuali e dei conti consolidati** e la direttiva (UE) 2016/2341 relativa alle attività e alla **vigilanza degli enti pensionistici aziendali o professionali (EPAP)**, al fine di introdurre, in ciascuna di tali direttive, specifici riferimenti incrociati al regolamento DORA **in relazione alla gestione, da parte di questi soggetti finanziari, di strumenti e sistemi TIC che dovrebbe realizzarsi ai sensi delle disposizioni di tale regolamento;**

– l'articolo 5 modifica i requisiti della direttiva 2013/36/UE (**direttiva sui requisiti patrimoniali, CRD**) in materia di **piani di emergenza e di continuità operativa** al fine di includere i piani di continuità operativa in materia di TIC e di ripristino in caso di disastro istituiti conformemente alle disposizioni del regolamento DORA;

– l'articolo 6 modifica la **direttiva 2014/65/UE (MiFID)** relativa ai mercati degli strumenti finanziari **aggiungendo riferimenti incrociati al regolamento DORA anche con riferimento alla definizione di strumenti finanziari e modificando le disposizioni relative alla continuità e alla regolarità nella prestazione di servizi e nell'esercizio di attività di investimento, alla resilienza e alla capacità sufficiente dei sistemi di negoziazione e infine a efficaci dispositivi in materia di continuità operativa e gestione del rischio.** In particolare, il primo paragrafo dell'articolo 6 contribuisce inoltre a **chiarire il trattamento giuridico delle cripto-attività ammissibili come strumenti finanziari.** A tal fine modifica la definizione di "strumento finanziario" di cui alla direttiva MiFID relativa ai mercati degli strumenti finanziari per chiarire, al di là di ogni dubbio giuridico, che tali strumenti possono essere emessi e gestiti utilizzando una tecnologia di registro distribuito;

– l'articolo 7 modifica la direttiva (UE) 2015/2366 relativa ai **servizi di pagamento** nel mercato interno (PSD2) e più precisamente le norme di autorizzazione, introducendo un riferimento incrociato al regolamento DORA. Inoltre, le norme in materia di notifica degli incidenti contenute in tale direttiva dovrebbero escludere la notifica di incidenti connessi alle TIC che il regolamento DORA armonizza pienamente;

L'articolo 6, paragrafo 4, integra la proposta di regolamento relativo a un **regime pilota** per le **infrastrutture di mercato** basate sulle tecnologie di registro distribuito **esentando temporaneamente gli MTF DLT e i CSD DLT da alcuni requisiti previsti dalla MiFID**, al fine di consentire loro di sviluppare soluzioni per la negoziazione e il regolamento delle operazioni in cripto-attività ammissibili come strumenti finanziari.

Relazione del Governo

Nella Relazione predisposta ai sensi dell'articolo 6 della legge n. 234 del 2012 il Governo valuta che la **proposta rispetti il principio di attribuzione, il principio di sussidiarietà e di proporzionalità.** La valutazione delle finalità generali del progetto è complessivamente positiva e le disposizioni contenute nel progetto possono ritenersi conformi all'interesse nazionale.

Con riferimento alle prospettive negoziali, per ciò che concerne in particolare il testo della proposta di direttiva, la delegazione Italiana ha trasmesso alcuni commenti concernenti i seguenti elementi di attenzione:

- la necessità di valutare **l'adeguatezza del regime di esenzione previsto dall'articolo 6 della proposta di direttiva**, con riferimento all'accesso ai sistemi multilaterali di negoziazione DLT, per i quali nel testo proposto si prevede una deroga limitata alle sole persone fisiche per facilitare l'accesso alle suddette sedi di negoziazione, senza considerare l'eventuale deroga potenziale anche per altre tipologie di soggetti (ad esempio aziende o altri investitori istituzionali) diversi dai soggetti abilitati ai sensi della direttiva MiFID;
- con riferimento alle **modifiche previste alla direttiva MiFID** oggetto dell'articolo 6 della proposta di direttiva, è stata rappresentata l'esigenza di **ulteriori approfondimenti in relazione alla definizione di strumenti finanziari** per garantire la neutralità tecnologica delle proposte normative, poiché l'attuale testo menziona esclusivamente gli strumenti finanziari **"originati da una DLT"**. In particolare, viene suggerito di valutare più approfonditamente la scelta di menzionare una specifica tecnologia (DLT) in uno scenario di sviluppo tecnologico rapido che potrebbe modificarsi in seguito;

25 maggio 2021

A cura di Davide Zaottini

La documentazione dei Servizi e degli Uffici del Senato della Repubblica è destinata alle esigenze di documentazione interna per l'attività degli organi parlamentari e dei parlamentari. Si declina ogni responsabilità per la loro eventuale utilizzazione o riproduzione per fini non consentiti dalla legge. I contenuti originali possono essere riprodotti, nel rispetto della legge, a condizione che sia citata la fonte.