Ministero dell'Economia e delle Finanze
UFFICIO LEGISLATIVO ECONOMIA

Prot. n. 559

Roma, 20 GEN 2021

Alla Presidenza del Consiglio dei Ministri
Dipartimento politiche europee

E, p.c. Al Ministero degli affari esteri e della cooperazione internazionale
Nucleo di valutazione degli atti UE

All'Ufficio del coordinamento legislativo

Al Dipartimento della tesoro

Al Dipartimento della Ragioneria generale dello Stato

LORO SEDI

Oggetto: Richiesta di relazione (art. 6 legge n. 234/2012) - proposta di regolamento del Parlamento europeo e del Consiglio relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) 600/2014 e (UE) n. 909/2014- Cod. Consiglio 11051/20- Cod. interistituzionale 2020/0266 (COD)- Cod. Commissione COM (2020) 595.

In riferimento alla richiesta in oggetto, si trasmette la relazione di cui all'art. 6, commi 4 e 5, della legge 24 dicembre 2012, n. 234, unitamente alla tabella di corrispondenza, elaborata da questo dicastero con l'allegata nota del Dipartimento del tesoro prot.1928 del 13 gennaio 2021.

IL CAPO DELL'UFFICIO
Olivia Rinaldi

Ministero dell'Economia e delle Finanze

DIPARTIMENTO DEL TESORO
DIREZIONE V

ALL'UFFICIO LEGISLATIVO- ECONOMIA
SEDE

OGGETTO: Richiesta di Relazione (art. 6 legge n. 234/2012) - Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO 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- Cod. Consiglio 11051/20 – Cod. interistituzionale 2020/0266 (COD) – Cod. Commissione COM(2020) 595.

Si trasmette, come da richiesta di cui alla lettera prot. 2021/304 del 23 dicembre 2020 ricevuta dalla Presidenza del Consiglio dei Ministri, Dipartimento Politiche Europee, Servizio Informative parlamentari e Corte di Giustizia UE, la relazione ai sensi dell'art. 6, commi 4 e 5, della legge 24 dicembre 2012, n. 234, unitamente alla tabella di corrispondenza, elaborata dal Ministero dell'Economia e delle Finanze in merito al progetto di atto legislativo dell'Unione europea di cui all'oggetto.

IL DIRIGENTE GENERALE
Firmato digitalmente da:

Ministero
dell' Economia e delle Finanze
DIPARTIMENTO DEL TESORO
DIREZIONE V

Relazione
ai sensi dell'art. 6, comma 4, della legge n. 234/2012

Oggetto dell'atto: Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO 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
– **Codice della proposta:** COM(2020) 595 del 24/09/2020 – **Codice interistituzionale:**2020/0266 (COD) – **Amministrazione con competenza prevalente:** Ministero dell'Economia e delle Finanze

***

Premessa: finalità e contesto

La proposta di regolamento relativa ad un quadro normativo rafforzato *di Digital Operational Resilience Act* (DORA) fa parte del pacchetto sulla finanza digitale (*Digital Finance Package*) presentato dalla Commissione europea il 24 settembre 2020 al fine di favorire lo sviluppo nell'Unione Europea di un settore finanziario competitivo. L'iniziativa legislativa è parte della più ampia strategia *di Digital Finance* per l'UE, basata su tre pilastri: resilienza delle singole infrastrutture di mercato; resilienza dell'ecosistema finanziario europeo; dialogo strategico tra tutte le parti interessate pubbliche e private. Essa fa seguito al piano d'azione *Fintech* della Commissione (marzo 2018), che ha definito le fasi necessarie per lo sviluppo di un approccio specifico alla *cybersecurity* nell'ambito della resilienza operativa del settore finanziario europeo. Il pacchetto sulla finanza digitale comprende una nuova strategia in materia di finanza digitale per il settore finanziario dell'UE[1] avente lo scopo di garantire che l'Unione abbracci la rivoluzione digitale e ne assuma la guida con le imprese europee innovative in prima linea, offrendo alle imprese e ai consumatori i benefici della finanza digitale. Oltre alla proposta di regolamento per la resilienza operativa digitale, il pacchetto comprende anche una proposta di regolamento UE in materia di mercati delle cripto- attività[2] (MiCA), una proposta di regolamento relativa a un regime pilota sulle

[1] Comunicazione della Commissione al Parlamento europeo, al Consiglio, alla Banca centrale europea, al Comitato economico e sociale europeo e al Comitato delle regioni relativa a una strategia in materia di finanza digitale per l'UE [COM (2020) 591], 24 settembre 2020.

[2] Proposta di Regolamento del Parlamento europeo e del Consiglio relativo ai mercati delle cripto-attività e che modifica la direttiva (UE) 2019/1937 [COM (2020) 593].

infrastrutture di mercato della tecnologia di registro distribuito (DLT)[3] e una proposta di direttiva finalizzata ad apportare i necessari chiarimenti o modifiche agli atti legislativi impattati dalla nuova normativa UE in materia di servizi finanziari[4].

Le tecnologie digitali, o Tecnologie dell'Informazione e della Comunicazione (TIC), offrono molte opportunità, ma presentano al contempo rischi, che rappresentano una sfida per la resilienza operativa, per le prestazioni e per la stabilità del sistema finanziario dell'UE. La riforma che è seguita alla crisi finanziaria del 2008 ha rafforzato in primo luogo la resilienza finanziaria del settore finanziario dell'UE, affrontando solo indirettamente i rischi relativi alle TIC in alcuni ambiti, nel quadro di misure volte a contrastare in generale i rischi operativi. Le modifiche alla legislazione dell'UE in materia di servizi finanziari introdotte dopo la crisi hanno creato un codice unico che disciplina gran parte dei rischi finanziari associati ai servizi di questo tipo, ma non hanno affrontato in maniera esaustiva il problema della resilienza operativa digitale. Spesso, infatti, si è trattato di misure concepite come direttive di armonizzazione minima o regolamenti basati su principi, che lasciano ampio spazio ad approcci divergenti nell'ambito del mercato unico. L'intervento a livello di Unione Europea non è allo stato attuale, pertanto, in grado di garantire pienamente alle entità finanziarie una gestione dei rischi operativi che consenta di resistere e reagire all'impatto degli incidenti connessi alle TIC e di riprendersi dai relativi effetti.

L'assenza di norme dettagliate e complete sulla resilienza operativa digitale a livello di UE ha portato alla proliferazione di iniziative di regolamentazione e di approcci di vigilanza a livello nazionale. L'azione a livello di Stati membri ha tuttavia un effetto limitato, a causa della natura transfrontaliera dei rischi relativi alle TIC. Inoltre, la mancanza di coordinamento delle iniziative nazionali ha dato luogo a sovrapposizioni, incoerenze, duplicazione di requisiti, elevati costi amministrativi e di conformità (soprattutto per le entità finanziarie transfrontaliere) oppure ha impedito di individuare e quindi affrontare i rischi relativi alle TIC. Questa situazione determina la frammentazione del mercato unico, compromettendo la stabilità e l'integrità del settore finanziario dell'UE, nonché la protezione dei consumatori e degli investitori.

La proposta di regolamento si inserisce in un lavoro più ampio per rafforzare la *cybersecurity* nei servizi finanziari e affrontare in generale i rischi operativi[5]. La strategia europea per i dati[6] stabilisce quattro pilastri, ovvero protezione dei dati, diritti fondamentali, sicurezza e cibersicurezza, come prerequisiti essenziali per una società che, grazie all'uso dei dati, disponga di maggiori strumenti. Più di recente il Parlamento europeo ha avviato i lavori su una relazione in materia di finanza digitale, che esorta tra l'altro ad adottare un approccio comune sulla *cyber resilience* del settore finanziario[7]. La proposta, pertanto, oltre ad essere coerente con questi obiettivi,

---

[3] Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un regime pilota per le infrastrutture di mercato basate sulla tecnologia di registro distribuito (COM (2020) 594).

[4] Proposta di direttiva del Parlamento europeo e del Consiglio 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 [COM (2020) 596].

[5] Comitato di Basilea per la vigilanza bancaria, *Cyber-resilience: Range of practices*, dicembre 2018 e *Principles for sound management of operational risk* (PSMOR), ottobre 2014.

[6] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Una strategia europea per i dati (COM (2020) 66 final).

[7] Relazione recante raccomandazioni alla Commissione sulla finanza digitale: rischi emergenti legati alle cripto-attività -

sosterrebbe le politiche volte a favorire la ripresa dopo la pandemia dovuta al COVID-19, in quanto garantirebbe che all'accresciuta dipendenza dalla finanza digitale corrisponda un'adeguata, efficace ed efficiente resilienza operativa.

Accanto alla legislazione sui servizi finanziari, la direttiva (UE) 2016/1148 (*NIS- Network and Information Security*) del Parlamento europeo e del Consiglio[8] rappresenta l'attuale quadro generale per la cibersicurezza a livello di Unione. Fra i sette settori critici cui si applica, questa direttiva individua anche tre tipi di entità finanziarie, vale a dire enti creditizi, sedi di negoziazione e controparti centrali. Dal momento, però, che la direttiva NIS introduce un meccanismo di identificazione a livello nazionale per gli Operatori di Servizi Essenziali (OSE)[9], ciò comporta che solo alcune di tali entità finanziarie, identificate quali operatori essenziali dagli Stati membri, rientrano nel suo ambito di applicazione e sono quindi tenute a rispettare le prescrizioni in materia di notifica degli incidenti e sicurezza connessi alle TIC contenute nella direttiva stessa.

L'iniziativa normativa, pertanto, avrebbe lo scopo di conservare i benefici connessi al quadro orizzontale sulla cibersicurezza (quali la direttiva NIS) mantenendo il settore finanziario nel proprio ambito di applicazione. La proposta è infine pienamente in linea con la strategia per l'Unione della sicurezza[10] che auspica un'iniziativa per la resilienza operativa digitale nel settore finanziario, considerata l'elevata dipendenza di quest'ultimo dai servizi di TIC e la sua elevata vulnerabilità agli attacchi informatici.

La proposta di direttiva che accompagna quella di regolamento non prevede modifiche alla direttiva NIS, in quanto a partire da settembre 2020 sono iniziati i lavori del Gruppo di Cooperazione NIS, incentrati sulla predisposizione di una nuova strategia *cyber* e sulla revisione della predetta direttiva. In base alla proposta presentata dalla Commissione, il regolamento DORA costituirà *lex specialis* rispetto alla direttiva NIS, mentre Autorità competenti per il settore saranno le Autorità di vigilanza. Il regolamento si applicherà, garantendo la proporzionalità, pressoché a tutto il settore finanziario (esclusi i sistemi di pagamento), nonché ai soggetti terzi fornitori di servizi critici relativi alle TIC, al fine di armonizzare all'interno dell'Unione Europea le disposizioni normative su tali sistemi e sulla sicurezza informatica nell'ambito dei servizi finanziari, in maniera tale da alleviare il settore da eccessivi oneri sia per gli operatori del mercato sia per le autorità competenti.

---

sfide a livello della regolamentazione e della vigilanza nel settore dei servizi, degli istituti e dei mercati finanziari (2020/2034(INL)).

[8] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1).

[9] La direttiva NIS è stata recepita dal D. Lgs. 18 maggio 2018, n.65, il quale all'art. 7, comma 1, lett. c, per il settore bancario e per il settore delle infrastrutture dei mercati finanziari ha individuato il MEF, in collaborazione con Banca d'Italia e Consob, quale Autorità NIS. La direttiva prevede la designazione di uno o più gruppi nazionali di risposta agli incidenti in materia di sicurezza informatica (CSIRT), nonché un'Autorità Nazionale Competente NIS e un Punto di Contatto Unico; la cooperazione tra Stati membri per mezzo del Gruppo di Cooperazione e la rete CSIRT; l'individuazione di Operatori di Servizi Essenziali (OSE) in tutti i settori vitali per l'economia e la società, tenuti ad adottare adeguate misure di sicurezza per la prevenzione e la gestione dei rischi informatici, nonché a notificare gli incidenti informatici che possono interrompere la continuità dei servizi.

[10] Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sulla strategia dell'UE per l'Unione della sicurezza (COM (2020) 605 final).

La proposta di regolamento si concentra su cinque blocchi normativi, vale a dire:

- prescrizioni relative alla *governance* e alla gestione dei rischi TIC, basate su principi chiave e requisiti comuni individuati dalle Autorità Europee di Vigilanza finanziaria (AEV), applicabili, tenendo conto del principio di proporzionalità, a tutte le istituzioni finanziarie;
- obblighi di segnalazione di incidenti rilevanti connessi alle TIC secondo criteri, modelli e meccanismi uniformi e semplificati, da estendere anche ai sotto settori attualmente non coperti da tali norme;
- test di resilienza operativa digitale (test di base per tutte le entità finanziarie, test avanzati solo per entità più significative), al fine di aggiornare e rivedere regolarmente i sistemi e gli strumenti di risposta agli attacchi informatici o alle interruzioni TIC e garantire in tal modo la resilienza operativa;
- gestione dei rischi derivanti da terze parti fornitrici di servizi TIC critici alle entità finanziarie, tramite la previsione di un quadro di sorveglianza indiretta e un controllo diretto dei servizi critici TIC di terze parti;
- condivisione delle informazioni sulle minacce informatiche tra le entità finanziarie.

A. Rispetto dei principi dell'ordinamento europeo

1. Rispetto del principio di attribuzione, con particolare riguardo alla correttezza della base giuridica

La proposta rispetta il principio di attribuzione, in base al quale l'Unione europea può agire esclusivamente nei limiti delle competenze che le sono attribuite dagli Stati membri nei Trattati per realizzare gli obiettivi da questi determinati (art. 5, par. 1 e 2, TUE).

La base giuridica è correttamente individuata nell'art. 114, TFUE, che conferisce alle istituzioni europee la competenza di stabilire le disposizioni appropriate per il ravvicinamento delle legislazioni degli Stati membri aventi per oggetto l'instaurazione e il funzionamento del mercato interno. Le disparità che si riscontrano attualmente nel settore della gestione e della segnalazione dei rischi relativi alle TIC, dei relativi test e dei rischi relativi alle TIC derivanti da terzi ostacolano il mercato unico dei servizi finanziari, poiché le entità finanziarie impegnate in attività transfrontaliere si trovano a dover soddisfare prescrizioni normative o aspettative di vigilanza differenti o potenzialmente sovrapposte, tali da intralciare la libertà di stabilimento e la libera prestazione di servizi. La differenza di norme falsa anche la concorrenza tra entità finanziarie dello stesso tipo attive in Stati membri diversi. Inoltre, in settori in cui l'armonizzazione è assente, parziale o limitata, la definizione di norme o approcci nazionali divergenti, già in vigore oppure in via di adozione e attuazione a livello nazionale, può costituire un deterrente per le libertà del mercato unico dei servizi finanziari.

Con riferimento alla scelta del tipo di atto giuridico, il ricorso a un regolamento serve a ridurre la complessità normativa, favorisce la convergenza della vigilanza, incrementa la certezza del diritto e contribuisce nel contempo a limitare i costi di conformità, specialmente per le entità finanziarie che operano a livello transfrontaliero, riducendo altresì le distorsioni della concorrenza. Le misure necessarie per disciplinare la gestione dei rischi relativi alle TIC, la segnalazione dei rischi

connessi alle TIC nonché i test e la sorveglianza dei fornitori terzi di servizi di TIC critici devono essere inserite in un regolamento, allo scopo di garantire che le prescrizioni dettagliate siano efficacemente e direttamente applicabili in maniera uniforme, fatte salve la proporzionalità e le norme specifiche previste del presente regolamento.

Dato che la proposta incide su varie direttive del Parlamento europeo e del Consiglio adottate sulla base dell'articolo 53, paragrafo 1, TFUE, contestualmente viene adottata una proposta di direttiva per introdurre le necessarie modifiche a dette direttive.

2. Rispetto del principio di sussidiarietà

La proposta rispetta il principio di sussidiarietà, in quanto l'azione dell'Unione Europea si esplica nel conseguimento del corretto funzionamento del mercato interno. Tale obiettivo non può essere sufficientemente realizzato dagli Stati membri, potendo invece essere meglio conseguito a livello dell'Unione, in considerazione dell'alto grado di interconnessione tra i servizi finanziari, della cospicua attività transfrontaliera delle entità finanziarie e dell'estesa dipendenza dell'intero settore finanziario da fornitori terzi di servizi di TIC, che richiedono una forte resilienza operativa digitale per mantenere la solidità dei mercati finanziari dell'UE. Le disparità derivanti da regimi non uniformi o parziali, da sovrapposizioni o da molteplicità di prescrizioni applicabili alle medesime entità finanziarie operanti a livello transfrontaliero o che detengono numerose autorizzazioni[11] nell'ambito del mercato unico si possono affrontare in maniera efficace solo a livello di Unione europea. La proposta, infatti, armonizza la componente operativa digitale di un settore profondamente integrato e interconnesso, che già dispone, in quasi tutti gli altri ambiti principali, di un sistema unico di regolamentazione e vigilanza.

3. Rispetto del principio di proporzionalità

La proposta rispetta il principio di proporzionalità, in quanto le norme proposte non vanno al di là di quanto necessario per conseguire gli obiettivi della proposta e riguardano soltanto gli aspetti che gli Stati membri non possono disciplinare da soli, in cui gli oneri e i costi amministrativi sono commisurati agli obiettivi generali e specifici da conseguire.

Per quanto riguarda l'ambito di applicazione e l'intensità, la proporzionalità è concepita mediante il ricorso a criteri di valutazione qualitativi e quantitativi, che mirano a garantire che le nuove norme si estendano a tutte le entità finanziarie in maniera adeguata rispetto ai rischi e alle esigenze delle loro specifiche caratteristiche in termini di dimensioni e profilo commerciale. La proporzionalità si esplica anche nelle norme in materia di gestione dei rischi relativi alle TIC, test di resilienza digitale, segnalazione di incidenti gravi connessi alle TIC e sorveglianza dei fornitori terzi di servizi di TIC critici.

[11] La stessa entità finanziaria può detenere autorizzazioni a operare quale banca, impresa di investimento e istituto di pagamento, ciascuna delle quali rilasciata da una diversa autorità di vigilanza in uno o più Stati membri.

B. Valutazione complessiva del progetto e delle sue prospettive negoziali

1. Valutazione del progetto e urgenza

La valutazione delle finalità generali del progetto è complessivamente positiva in quanto tali finalità rispondono alla necessità di definire un quadro normativo europeo armonizzato, perseguendo obiettivi di carattere generale quali la certezza del diritto, il sostegno all'innovazione, la tutela dei consumatori, degli investitori e dell'integrità del mercato, nonché infine la stabilità finanziaria. Il regolamento, infatti, mira a cancellare le disparità legislative e la disomogeneità degli approcci normativi o di vigilanza ai rischi relativi alle TIC, rimuovendo in tal modo gli ostacoli al mercato unico dei servizi finanziari, in particolare per quanto riguarda il regolare esercizio della libertà di stabilimento e della libera prestazione di servizi per le entità finanziarie con una presenza transfrontaliera.

Il regolamento mira a consolidare e aggiornare le prescrizioni in materia di rischi relativi alle TIC trattati finora separatamente nei diversi regolamenti e direttive. L'obiettivo generale, infatti, consiste nel rafforzamento della resilienza operativa digitale delle entità del settore finanziario dell'UE, razionalizzando e aggiornando le norme vigenti e introducendo nuove prescrizioni in caso di lacune, in maniera tale da: 1) ridurre il rischio di instabilità e perturbazioni finanziarie; 2) ridurre gli oneri amministrativi e accrescere l'efficacia della vigilanza; 3) rafforzare la protezione dei consumatori e degli investitori.

Obiettivi specifici della proposta sono i seguenti:

- affrontare i rischi relativi alle Tecnologie dell'Informazione e della Comunicazione (TIC) in maniera più esaustiva e potenziare il livello complessivo di resilienza digitale del settore finanziario;
- razionalizzare le segnalazioni di incidenti connessi alle TIC e affrontare il problema delle sovrapposizioni fra prescrizioni in materia di segnalazioni;
- consentire alle autorità di vigilanza finanziaria di accedere alle informazioni relative agli incidenti connessi alle TIC;
- garantire alle entità finanziarie interessate dalla proposta di valutare l'efficacia delle proprie misure di prevenzione e resilienza, identificando le vulnerabilità connesse alle TIC;
- ridurre la frammentazione del mercato unico e far sì che i risultati dei test siano accettati su scala transfrontaliera;
- potenziare le salvaguardie contrattuali a favore delle entità finanziarie che fruiscono di servizi di TIC, anche per quanto riguarda le norme sull'esternalizzazione (disciplinando il monitoraggio di fornitori terzi di servizi di TIC);
- attivare una cornice europea per la sorveglianza delle attività dei fornitori terzi di servizi di TIC critici;
- incoraggiare lo scambio di dati sulle minacce nel settore finanziario.

Nell'affrontare i rischi relativi alle TIC è opportuno che le entità finanziarie seguano lo stesso approccio e le stesse norme basate su principi. La coerenza contribuisce ad accrescere la fiducia nel sistema finanziario e a preservarne la stabilità, soprattutto in tempi in cui l'intensissimo uso di

infrastrutture, piattaforme e sistemi di TIC comporta maggiori rischi digitali. Il rispetto di un'igiene informatica di base dovrebbe anche evitare l'imposizione di costi elevati per l'economia, riducendo al minimo l'impatto e i costi delle perturbazioni a livello di TIC.

Il progetto riveste carattere di moderata urgenza, alla luce della necessità di contemperare da un lato l'esigenza di un'attenta e complessa analisi della definizione degli effetti delle disposizioni del regolamento nei confronti delle imprese finanziarie e dei fornitori terzi di TIC presenti sul mercato, nonché delle interrelazioni con le discipline settoriali già vigenti; dall'altro, le esigenze di tutela dei consumatori e degli investitori e di salvaguardia della stabilità finanziaria, che rendono necessaria l'adozione di un quadro normativo europeo armonizzato.

2. Conformità del progetto all'interesse nazionale

Le disposizioni contenute nel progetto possono ritenersi conformi all'interesse nazionale, in quanto risulta condivisibile l'obiettivo, delineato nella Strategia in materia di finanza digitale per il settore finanziario dell'UE, di definire un quadro dettagliato e completo sulla resilienza operativa digitale per le entità finanziarie dell'UE.

3. Prospettive negoziali ed eventuali modifiche ritenute necessarie od opportune

La proposta è oggetto di procedura legislativa ordinaria e assumerà la forma di regolamento del Parlamento europeo e del Consiglio. L'applicazione del regolamento è prevista decorsi 12 mesi dalla data di entrata in vigore dello stesso, salvo che per le disposizioni degli articoli 23 e 24 (rispettivamente relativi ai test avanzati di strumenti, sistemi e processi di TIC fondati su test di penetrazione basati su minacce e ai requisiti per i tester), che si applicheranno decorsi 36 mesi dall'entrata in vigore del regolamento.

La proposta di regolamento è stata oggetto di una presentazione, a cura della Commissione europea, durante il primo *virtual meeting* del *Working Party on Financial Services (Digital Operational Resilience)* tenutosi il 30 settembre 2020, al quale partecipano in qualità di membri rappresentanti del Ministero dell'Economia e delle Finanze e della Rappresentanza Permanente per l'Italia presso l'Unione Europea. I successivi incontri del *Working Party* si sono svolti come segue:

- 22 ottobre 2020, Capo I, II e V (Disposizioni generali, ambito di applicazione, definizioni, quadro per la gestione dei rischi relativi alle TIC, gestione dei rischi relativi alle TIC derivanti da terzi);
- 28 ottobre 2020, Capo III, IV e VI (segnalazione di incidenti connessi alle TIC e rapporto con la direttiva NIS, condivisione di informazioni e test di resilienza operativa digitale);
- 09 novembre 2020, Capo V e IX (principi per un efficace *management* del rischio TIC derivante da terze parti ed entrata in vigore del regolamento);
- 27 novembre 2020, (principio di proporzionalità, *management* dei rischi relativi alle TIC, segnalazione di incidenti connessi alle TIC ai sensi del regolamento DORA e rapporti con direttiva PSD2);
- 08 dicembre 2020, Capo V (principi per un efficace *management* del rischio TIC derivante da

terze parti, quadro di sorveglianza sui fornitori terzi di servizi critici connessi alle TIC, presentazione mandato e compiti dell'ENISA).

In occasione delle sedute del *Working Party* la delegazione italiana ha rappresentato la posizione nazionale, fornendo risposta ai quesiti formulati in relazione alle singole disposizioni del regolamento. A seguito del primo *virtual meeting*, in data 09 ottobre è stato trasmesso un primo insieme di commenti riferiti all'intero articolato della proposta di regolamento. I riscontri forniti dalla delegazione italiana ai quesiti oggetto dei singoli *Working Party* sono stati successivamente trasmessi in forma scritta, di volta in volta, alla Presidenza dell'UE.

Le attività di analisi e revisione delle singole disposizioni della proposta di regolamento, di definizione della posizione italiana e di redazione delle risposte ai quesiti presentati in occasione dei *Working Party* sono state condotte dal Ministero dell'Economia e delle Finanze 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. A seguito delle attività di analisi e di confronto svolta in collaborazione tra Ministero dell'Economia e delle Finanze, Banca d'Italia e Consob, la delegazione italiana ha espresso la necessità di apportare le seguenti modifiche e/o integrazioni alla proposta di regolamento, nonché ha sollevato alcune criticità, in relazione ai punti individuati come segue:

I. con riferimento al Capo I (Disposizioni generali), per quanto riguarda l'ambito di applicazione soggettivo si è concordato 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, 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;

II. in riferimento al Capo II (Gestione dei rischi relativi alle TIC), è in primo luogo 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.

III. In merito al Capo III (Incidenti connessi alle TIC), per quanto riguarda la segnalazione di incidenti connessi alle TIC, è necessario 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.

IV. 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 maggiore 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.

V. In relazione al Capo V (Gestione dei rischi relativi alle TIC derivanti da terzi), nell'ambito della vigilanza sui fornitori terzi di servizi TIC, emerge 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 Autorità Europee di Vigilanza finanziaria (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 maggiore 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.

VI. In merito al Capo VII (Autorità competenti) si rimanda a quanto già evidenziato rispetto al Capo III rispetto ai rapporti tra il regolamento e la direttiva NIS.

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 maggiore chiarezza nei criteri per la designazione dei fornitori terzi.

Da ultimo, si evidenzia la necessità di un confronto con altri Stati membri finalizzato a porre maggiore attenzione al rapporto tra la nuova normativa prevista nel regolamento e le legislazioni

nazionali in materia di sicurezza nazionale e perimetro *cyber* (Legge 18 novembre 2019, n. 133).

Le attività negoziali proseguiranno sotto la nuova Presidenza, al fine di consentire agli Stati membri di continuare a confrontarsi, soprattutto con riferimento alle questioni oggetto di maggiore attenzione e criticità. In tal senso, gli Stati membri sono stati invitati a illustrare ulteriormente le proprie posizioni rispetto ad una bozza di regolamento revisionato, in cui si è tenuto conto di quanto già espresso finora dagli Stati membri.

C. Valutazione d'impatto

1. Impatto finanziario

In termini di incidenza sul bilancio UE, la proposta comporterebbe l'impiego di maggiori risorse, dal momento che il regolamento rafforza il ruolo delle AEV, conferendo loro i poteri per sorvegliare adeguatamente i fornitori terzi di servizi di TIC critici, in particolare per lo svolgimento delle missioni di vigilanza e il ricorso a personale che possieda specifiche competenze in materia di sicurezza delle TIC. L'entità e la ripartizione di tali costi dipenderanno dall'ampiezza dei nuovi poteri di sorveglianza e dai compiti che le AEV dovranno svolgere. Il numero delle risorse effettive necessarie alla sorveglianza diretta dipenderà, nel corso del tempo, dall'evoluzione del numero e delle dimensioni dei fornitori terzi di servizi di TIC critici da sorvegliare, ma la spesa corrispondente sarà interamente finanziata dalle commissioni pagate da questi partecipanti al mercato.

Secondo l'analisi della Commissione europea, pertanto, non si prevede alcun impatto sugli stanziamenti di bilancio dell'UE (ad eccezione del personale aggiuntivo), poiché tali costi saranno interamente finanziati dalle commissioni in questione. Inoltre, le funzioni regolamentari supplementari concernenti la resilienza operativa digitale attribuite alle AEV saranno assolte per mezzo di una ridistribuzione interna del personale attuale, che si tradurrà in una proposta di aumento del personale autorizzato dell'agenzia nel corso della procedura annuale di bilancio. L'agenzia continuerà ad adoperarsi per massimizzare le sinergie e gli incrementi di efficienza (anche attraverso sistemi informatici) e a monitorare attentamente il carico di lavoro supplementare associato alla presente proposta, che si rifletterà nel livello di personale autorizzato richiesto dall'agenzia nella procedura annuale di bilancio.

La proposta di regolamento comporta implicazioni in termini di costi, di oneri amministrativi e di impiego delle risorse anche per le autorità di vigilanza nazionali competenti, a causa dei compiti ulteriori che sarebbero chiamate a svolgere. In ogni caso, si ritiene opportuno evidenziare che per poter procedere ad una compiuta analisi dei costi gravanti sul bilancio nazionale, appare necessario attendere i futuri sviluppi negoziali relativi al progetto di norma di cui trattasi.

2. Effetti sull'ordinamento nazionale

La proposta può generare effetti positivi sull'ordinamento nazionale, soprattutto in termini di armonizzazione. Un atto sulla resilienza operativa digitale per il settore finanziario offrirebbe un quadro generale per tutti gli aspetti della resilienza operativa digitale e costituirebbe uno strumento efficace per migliorare la resilienza operativa complessiva del settore finanziario.

Renderebbe, inoltre, più chiara e coerente l'interazione con la direttiva NIS e il riesame di quest'ultima. L'armonizzazione, infatti, renderebbe più chiare alle entità finanziarie le diverse norme che esse devono rispettare in materia di resilienza operativa digitale, in particolare per quelle entità finanziarie che detengono più autorizzazioni e operano in diversi mercati dell'UE.

Il regolamento mira a cancellare le disparità legislative e la disomogeneità degli approcci normativi o di vigilanza ai rischi relativi alle TIC, rimuovendo in tal modo gli ostacoli al mercato unico dei servizi finanziari, in particolare per quanto riguarda il regolare esercizio della libertà di stabilimento e della libera prestazione di servizi per le entità finanziarie con una presenza transfrontaliera.

Gli adeguamenti resi necessari dalla proposta per l'adattamento dell'ordinamento nazionale riguarderanno, principalmente, l'attività di vigilanza e sanzionatoria delle autorità nazionali competenti, con l'attribuzione alle stesse di specifici ulteriori poteri e funzioni, secondo quanto previsto dal regolamento stesso.

3. Effetti sulle competenze regionali e delle autonomie locali

La norma non incide sulle competenze regionali e delle autonomie locali ai sensi di quanto previsto dalla Costituzione; pertanto la relazione non dovrà essere inviata alle Regioni, per il tramite delle loro Conferenze (art. 24, comma 2, legge n. 234/2012).

4. Effetti sull'organizzazione della pubblica amministrazione

La proposta di regolamento prevede l'attribuzione alle autorità nazionali competenti di ulteriori funzioni e poteri di vigilanza. L'attribuzione dei predetti poteri e funzioni e potrà comportare dei costi di adeguamento per le predette autorità, in relazione alla predisposizione di strutture, sistemi e procedure, nonché all'individuazione delle risorse umane dedicate.

In termini di semplificazione normativa, le misure qualitative previste nella proposta razionalizzerebbero e aggiornerebbero la normativa finanziaria dell'UE, introducendo nuovi requisiti in caso di lacune, ma allo stesso tempo mantenendo collegamenti con la direttiva NIS a carattere orizzontale. Il mercato unico dei servizi finanziari dell'UE è disciplinato da un ampio insieme di norme stabilite a livello dell'UE, che consentono alle imprese finanziarie autorizzate in uno Stato membro di prestare servizi in tutto il mercato unico grazie a un passaporto dell'UE. Di conseguenza, le norme stabilite a livello nazionale non costituirebbero un metodo efficace per rafforzare la resilienza operativa delle imprese finanziarie che utilizzano il passaporto. Inoltre il codice unico dell'UE contiene, a seguito della crisi finanziaria, norme estremamente dettagliate e prescrittive che affrontano rischi più "tradizionali" quali i rischi di credito, di mercato, di controparte e di liquidità. Il rafforzamento della resilienza operativa digitale richiede adeguamenti delle disposizioni sui rischi operativi già definite a livello dell'UE; pertanto miglioramenti e integrazioni sono possibili solo a livello dell'Unione.

5. Effetti sulle attività dei cittadini e delle imprese

La proposta di regolamento avrebbe un impatto positivo sui cittadini e sulle imprese, in quanto affronta i rischi relativi alle TIC in tutto il settore finanziario, rafforzando la capacità degli enti finanziari di resistere agli incidenti connessi alle TIC, di conseguenza diminuendo il rischio che un incidente informatico si propaghi rapidamente sui mercati finanziari. La proposta normativa ridurrebbe i costi diretti e gli eventuali impatti più ampi che gli incidenti informatici gravi potrebbero avere sulla stabilità finanziaria. Eliminando le sovrapposizioni di obblighi di segnalazione si ridurrebbero, inoltre, gli oneri amministrativi. L'armonizzazione delle pratiche in materia di test renderebbe più facile individuare vulnerabilità e rischi sconosciuti, diminuendo anche i costi, in particolare per le imprese transfrontaliere. L'introduzione di un insieme coerente di norme sulla gestione dei rischi legati ai fornitori terzi di servizi di TIC darebbe alle imprese finanziarie un maggior controllo sul modo in cui i fornitori terzi si conformano al quadro normativo. Vi sarebbero inoltre benefici prudenziali derivanti dalla vigilanza sui fornitori terzi di TIC da parte delle autorità preposte.

Nel complesso, la proposta comporterebbe benefici sociali più ampi, derivanti da un contesto operativo più resiliente per tutti i partecipanti ai mercati finanziari e da una maggiore tutela dei consumatori e degli investitori. Una maggiore resilienza operativa digitale del sistema finanziario dell'UE diminuirebbe il numero e i costi medi degli incidenti, permettendo un accrescimento della fiducia nel settore dei servizi finanziari da parte della società nel suo complesso. In termini di impatto ambientale, inoltre, il regolamento incoraggerebbe un uso maggiore delle infrastrutture e dei servizi di TIC di ultima generazione, prevedibilmente destinati a diventare più sostenibili dal punto di vista ambientale.

Il regolamento riguarderebbe tutte le imprese finanziarie, al fine di aumentare la resilienza operativa dell'intero settore. Tale vasto ambito di applicazione è importante alla luce della natura interconnessa del settore finanziario e della corrispondente necessità di dotarsi di un solido livello di resilienza operativa complessiva. Nel definire i requisiti fondamentali nei principali settori di intervento, il principio di proporzionalità, da declinarsi in maniera efficace, si applicherebbe sia all'insieme dei sotto settori che in seno a ciascun sotto settore, tenendo conto, tra l'altro, delle differenze a livello di modelli d'impresa, dimensioni, profili di rischio, importanza sistemica.

Il regolamento comporterebbe per le imprese costi sia una tantum sia ricorrenti. I primi dipendono dagli investimenti in sistemi informatici e sono difficili da quantificare, data la diversa situazione dei sistemi preesistenti delle imprese. Per le grandi imprese finanziarie il costo delle misure contenute nella proposta sarà probabilmente modesto. Anche per le imprese più piccole i costi dovrebbero essere inferiori, in quanto sarebbero soggette a misure meno rigorose, proporzionate al loro minor rischio. Per quanto riguarda i test, le Autorità Europee di Vigilanza (AEV) hanno stimato che i costi relativi ai test di penetrazione basati su minacce variano tra lo 0,1% e lo 0,3% del bilancio totale destinato dalle imprese interessate alle TIC. I costi relativi alla segnalazione degli incidenti sarebbero drasticamente ridotti, in quanto non vi sarebbero sovrapposizioni con la segnalazione ai sensi della direttiva NIS.

Altro

La proposta di regolamento vede il necessario coinvolgimento di Banca d'Italia e Consob, in qualità di autorità di vigilanza e in relazione all'incidenza della proposta su profili di competenza delle stesse. In particolare, l'applicazione del regolamento comporterà l'attribuzione a Banca d'Italia e Consob, nell'ambito delle rispettive competenze, di ulteriori funzioni e poteri di vigilanza diretta sui soggetti destinatari delle disposizioni del regolamento, nonché di coordinamento e di collaborazione con le autorità europee e le autorità nazionali competenti di altri Stati membri. L'analisi e la discussione della proposta di regolamento, anche per quanto riguarda la definizione della posizione italiana in sede negoziale, pertanto, sono coordinate dal Ministero dell'Economia e delle Finanze in collaborazione con Banca d'Italia e Consob.

Si evidenzia che la versione originale della proposta di regolamento è suscettibile di modifica nel corso del negoziato nell'ambito delle competenti sedi istituzionali comunitarie all'esito dei continui confronti e contributi dei vari Stati Membri, così come la posizione della delegazione italiana è suscettibile di modifica ed evoluzione, anche all'esito di consultazioni con le amministrazioni e le parti interessate, con particolare riferimento ai profili illustrati nella sezione 3 della presente relazione (Prospettive negoziali ed eventuali modifiche ritenute necessarie od opportune).

Ministero
dell'Economia e delle Finanze

DIPARTIMENTO DEL TESORO
DIREZIONE V

Tabella di corrispondenza ai sensi dell'art. 6, comma 5, della legge n. 234/2012

(D.P.C.M. 17marzo 2015)

Oggetto dell'atto: Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO 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
– **Codice della proposta:** COM(2020) 595 del 24/09/2020 – **Codice interistituzionale:**2020/0266 (COD) – **Amministrazione con competenza prevalente:** Ministero dell'Economia e delle Finanze

Premessa

Stante la scelta di disciplinare la materia mediante un regolamento UE, le relative disposizioni saranno direttamente applicabili nei singoli Stati membri. L'articolato della proposta di regolamento è attualmente in fase di revisione, in quanto la Commissione ha recepito le prime indicazioni fornite dagli Stati membri, chiedendo contestualmente loro un riscontro sulle possibili modifiche prospettate alla formulazione degli articoli. Un'analisi completa e approfondita circa la corrispondenza e l'incidenza sulle norme nazionali vigenti sarà possibile soltanto una volta stabiliti i concetti sostanziali circa le disposizioni contenute nel regolamento. La presente redazione, pertanto, costituisce una prima disamina degli articoli che potrebbero avere impatto sull'ordinamento nazionale, sia in termini di normativa vigente, sia in termini di necessità di intervento normativo, in quanto una valutazione definitiva della proposta potrà essere compiuta soltanto una volta finalizzati i contenuti del regolamento, anche all'esito dei futuri sviluppi negoziali.

Disposizione del progetto di atto legislativo dell'Unione europea (articolo e paragrafo)	**Norma nazionale vigente** (norma primaria e secondaria)	**Commento** (natura primaria o secondaria della norma, competenza ai sensi dell'art. 117 della Costituzione, eventuali oneri finanziari, impatto sull'ordinamento nazionale, oneri amministrativi aggiuntivi, amministrazioni coinvolte, eventuale necessità di intervento normativo di natura primaria o secondaria)
Articolo 1	**Decreto Legislativo 18 maggio 2018, n. 65** Attuazione della direttiva (UE) 2016/1148 del	Rispetto alle entità finanziarie identificate come operatori di servizi essenziali (OSE) ai sensi del D. Lgs. 18 maggio 2018, n. 65 che

	Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione	recepisce l'articolo 5 della direttiva (UE) 2016/1148, il regolamento è considerato un atto giuridico settoriale dell'Unione ai sensi dell'articolo 1, paragrafo 7, della stessa direttiva, pertanto per gli obblighi imposti agli operatori di servizi essenziali o ai fornitori di servizi digitali in materia di sicurezza delle reti e dei sistemi informativi o relativi alla notifica di incidenti, non si applicheranno più le norme settoriali nazionali (come accade ora in virtù del principio *lex specialis*), ma si applicheranno le disposizioni del regolamento quale atto giuridico settoriale dell'Unione.
Articoli da 4 a 9	**Decreto Legislativo 18 maggio 2018, n. 65** Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione	L'interazione tra il regolamento sui servizi finanziari e la direttiva NIS sarà disciplinata dalla clausola *lex specialis*, esentando in tal modo le entità finanziarie da prescrizioni sostanziali contenute nella direttiva NIS (che in Italia attualmente trova attuazione in virtù del predetto principio di *lex specialis* tramite la normativa settoriale nazionale) ed evitando sovrapposizioni tra i due strumenti. Si rimanda a quanto osservato in relazione all'articolo 1 del regolamento.
Articolo 10 paragrafi 8 e 9		8. Si prevede che alcune entità finanziarie debbano trasmettere alle autorità competenti copie dei risultati dei test di continuità operativa delle TIC o di esercizi analoghi. 9. Si prevede che le entità finanziarie diverse dalle microimprese debbano segnalare alle autorità competenti tutti i costi e le perdite causati dalle perturbazioni a livello di TIC e dagli incidenti connessi alle TIC.

Articolo 17	**Decreto Legislativo 18 maggio 2018, n. 65** Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione	Si dispone che la segnalazione degli incidenti gravi connessi alle TIC sia effettuata nei confronti delle autorità competenti ai sensi dell'art. 41 del regolamento, vale a dire a livello nazionale nei confronti delle Autorità di vigilanza Banca d'Italia e Consob. Il Decreto Legislativo 18 maggio 2018, n. 65 di attuazione della Direttiva NIS, invece, richiede che la segnalazione da parte dell'Operatore di Servizi Essenziali sia effettuata nei confronti del CSIRT italiano con contestuale comunicazione all'Autorità competente NIS, vale a dire il MEF in collaborazione con Banca d'Italia e Consob. Come indicato nell'articolo 1, il regolamento costituirà *lex specialis* rispetto alla direttiva NIS (attualmente in fase di revisione). Sono, però, in fase di valutazione possibili modifiche o integrazioni a tale articolo del regolamento, pertanto soltanto all'esito delle consultazioni tra Stati membri sarà possibile verificare la necessità di un intervento normativo in tal senso.
Articolo 18		Si stabilisce che ENISA, BCE e AEV entro un anno dall'entrata in vigore del regolamento elaboreranno progetti di norme tecniche di regolamentazione comuni per precisare ulteriormente le condizioni alle quali le entità finanziarie possono delegare a un fornitore terzo di servizi, previa approvazione dell'autorità competente, gli obblighi di segnalazione di incidenti connessi alle TIC.
Articolo 19		Si prevede che le AEV, tramite il comitato congiunto, in consultazione con la BCE e l'ENISA, entro tre anni dall'entrata

		in vigore del regolamento redigeranno una relazione congiunta al fine di valutare la fattibilità dell'istituzione di un polo UE unico per l'ulteriore centralizzazione della segnalazione degli incidenti gravi connessi alle TIC da parte delle entità finanziarie.
Articolo 20		Si stabilisce che l'autorità competente ai sensi del regolamento, dopo aver ricevuto la relazione di cui all'articolo 17, paragrafo 1, accusa ricevuta della notifica e invia il prima possibile all'entità finanziaria tutti i riscontri o gli orientamenti necessari, in particolare allo scopo di discutere rimedi a livello di entità o metodi per ridurre al minimo gli effetti avversi nei diversi settori.
Articolo 21		L'articolo stabilisce che le entità finanziarie dovranno sottoporre a test tutte le applicazioni e i sistemi di TIC critici con cadenza almeno annuale.
Articolo 23		L'articolo prevede che le entità finanziarie più rilevanti devono effettuare test avanzati sotto forma di test di penetrazione basati su minacce con cadenza almeno triennale. Alla fine dei test l'entità finanziaria e i tester esterni trasmettono all'autorità competente la documentazione attestante che i test di penetrazione basati su minacce sono stati svolti conformemente alle prescrizioni. La documentazione viene poi convalidata dalle autorità competenti, le quali rilasciano un attestato. Le autorità competenti identificano le entità finanziarie tenute a svolgere test di

		penetrazione basati su minacce secondo modalità proporzionate alle dimensioni, all'attività e al profilo di rischio complessivo dell'entità finanziaria, sulla base della valutazione degli elementi indicati nel regolamento. L'ABE, l'ESMA e l'EIOPA elaborano progetti di norme tecniche di regolamentazione almeno due mesi prima dell'entrata in vigore del regolamento.
Articolo 25		Si stabilisce che le entità finanziarie devono comunicare almeno una volta all'anno alle autorità competenti informazioni sui nuovi accordi per l'utilizzo di servizi di TIC, nonché, su richiesta delle predette autorità, devono mettere a disposizione il registro delle informazioni completo, necessario per consentire l'efficace vigilanza sull'entità finanziaria. Le entità finanziarie, inoltre, devono informare tempestivamente l'autorità competente sui contratti previsti per funzioni critiche o importanti, nonché del momento in cui una funzione diventa critica o importante. Le AEV, tramite il comitato congiunto, elaborano progetti di norme tecniche di attuazione per definire modelli standard ai fini del registro delle informazioni. Le AEV presenteranno progetti di norme tecniche di attuazione alla Commissione entro un anno dall'entrata in vigore del regolamento. Le AEV, inoltre, presenteranno progetti di norme tecniche di regolamentazione alla Commissione entro un anno dall'entrata in vigore del

		regolamento.
Articolo 28		Le AEV, tramite il comitato congiunto e su raccomandazione del forum di sorveglianza (a) designano i fornitori terzi di servizi di TIC che sono critici per le entità finanziarie; (b) nominano l'ABE, l'ESMA o l'EIOPA quale autorità di sorveglianza capofila di ciascun fornitore terzo di servizi di TIC critico.
Articolo 29 Paragrafi 1 e 4		L'articolo stabilisce che il comitato congiunto istituisce il forum di sorveglianza come sottocomitato incaricato di coadiuvare il lavoro del comitato congiunto e dell'autorità di sorveglianza capofila, per quanto concerne i rischi relativi alle TIC derivanti da terzi in tutti i settori finanziari. Si prevede che un rappresentante di alto livello del personale in servizio dell'autorità competente interessata di ciascuno Stato membro faccia parte del forum di sorveglianza dei fornitori terzi di servizi di TIC critici.
Articolo 31 Paragrafi 4 e 7		Il paragrafo 4 stabilisce che l'autorità di sorveglianza capofila può imporre una penalità di mora, al fine di costringere il fornitore terzo di servizi di TIC critico rispetto a quanto previsto in riferimento ai poteri di richiedere informazioni e documentazione, condurre indagini e ispezioni, richiedere relazioni da parte dell'autorità di sorveglianza capofila. Ai sensi del paragrafo 4, le penalità sono di natura amministrativa ed esecutive. L'applicazione delle penalità è regolata dalle norme di procedura civile vigenti nello Stato membro sul cui territorio si svolgono le ispezioni e l'accesso. I giudici dello

		Stato membro interessato esercitano la giurisdizione sui reclami concernenti l'irregolarità dell'applicazione delle penalità. Gli importi delle penalità sono assegnati al bilancio generale dell'Unione europea.
Articolo 35		L'articolo prevede che nello svolgimento dei compiti di sorveglianza costante le autorità di sorveglianza capofila sono coadiuvate da un gruppo di esaminatori istituito per ciascun fornitore terzo di servizi di TIC critico. Tale gruppo di esaminatori congiunto è composto da membri del personale dell'autorità di sorveglianza capofila e delle autorità competenti che vigilano sulle entità finanziarie cui il fornitore terzo di servizi di TIC critico presta servizi, che parteciperanno alla preparazione e allo svolgimento delle attività di sorveglianza. Le AEV, tramite il comitato congiunto, elaboreranno un progetto di norme tecniche di regolamentazione comuni da presentare alla Commissione entro un anno dall'entrata in vigore del regolamento.
Articolo 37		Si stabilisce che le autorità competenti verificano se le entità finanziarie tengono conto dei rischi individuati nelle raccomandazioni inviate ai fornitori terzi di servizi di TIC critici da parte dell'autorità di sorveglianza capofila. Inoltre, le autorità competenti possono chiedere alle entità finanziarie di sospendere temporaneamente, in tutto o in parte, l'utilizzo o l'introduzione di un servizio prestato dal fornitore

		terzo di servizi di TIC critico, fino a quando non siano stati affrontati i rischi identificati nelle raccomandazioni trasmesse al fornitore terzo di servizi di TIC critico. Laddove si renda necessario, le autorità competenti possono chiedere alle entità finanziarie di risolvere, in tutto o in parte, gli accordi contrattuali pertinenti stipulati con i fornitori terzi di servizi di TIC critici. Le autorità competenti informano l'autorità di sorveglianza capofila in merito alle misure e agli approcci adottati nell'ambito dei propri compiti di vigilanza in relazione alle entità finanziarie, nonché in merito alle misure contrattuali adottate da queste ultime qualora i fornitori terzi di servizi di TIC critici non abbiano accolto, in tutto o in parte, le raccomandazioni formulate dall'autorità di sorveglianza capofila.
Articolo 38		L'articolo prevede che le AEV addebitano ai fornitori terzi di servizi di TIC critici commissioni che coprono completamente le spese necessarie sostenute dalle AEV in relazione allo svolgimento dei compiti di sorveglianza ai sensi del regolamento, compreso il rimborso dei costi eventualmente sostenuti in seguito al lavoro svolto dalle autorità competenti che hanno partecipato alle attività di sorveglianza. L'importo della commissione addebitata al fornitore di servizi di TIC critico copre tutti i costi amministrativi ed è proporzionato al fatturato del fornitore.
Articolo 39		L'articolo prevede che l'ABE, l'ESMA e l'EIOPA possono concludere accordi amministrativi

		con le autorità di vigilanza e di regolamentazione di paesi terzi per promuovere la cooperazione internazionale in materia di rischi relativi alle TIC derivanti da terzi tra i diversi settori finanziari, in particolare definendo migliori prassi per il riesame delle pratiche e dei controlli per la gestione dei rischi relativi alle TIC nonché per le misure di attenuazione e risposta agli incidenti.
Articolo 40		Si stabilisce che le entità finanziarie devono notificare alle autorità competenti la propria partecipazione ai meccanismi di condivisione delle informazioni, al momento della convalida della propria adesione o, se del caso, della cessazione dell'adesione, quando quest'ultima abbia effetto.
Articolo 41	**Decreto Legislativo 18 maggio 2018, n. 65** Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione	L'articolo dispone che il rispetto degli obblighi sanciti dal regolamento è assicurato dalle autorità competenti conformemente ai poteri conferiti dagli atti giuridici settoriali, fatte salve le disposizioni sul quadro di sorveglianza per i fornitori terzi di servizi di TIC critici. Si rimanda al precedente commento di cui all'art. 17
Articolo 42		Si stabilisce che le AEV e le autorità competenti possono chiedere di essere invitate ai lavori del gruppo di cooperazione istituito dalla direttiva (UE) 2016/1148 (direttiva NIS). Le autorità competenti, inoltre, possono consultare il punto di contatto unico e i gruppi di intervento per la sicurezza informatica in caso di incidente istituiti rispettivamente ai sensi degli articoli 8 e 9 della predetta direttiva.

Articolo 43		Si prevedono obblighi di cooperazione e scambio di informazioni tra autorità competenti, AEV e BCE nello svolgimento dei compiti di cui agli articoli da 42 a 48, nonché uno stretto coordinamento dell'attività di vigilanza per rilevare e correggere le violazioni del regolamento, sviluppare e promuovere migliori pratiche, agevolare la collaborazione, promuovere la coerenza dell'interpretazione.
Art. 44		Si conferiscono alle autorità competenti tutti i poteri di vigilanza, di indagine e sanzionatori necessari per adempiere i propri compiti ai sensi del regolamento. Si richiede agli Stati membri di provvedere affinché le autorità competenti abbiano il potere di applicare almeno le sanzioni amministrative o misure di riparazione per le violazioni del regolamento elencate al paragrafo 4 dell'articolo. Si richiede, inoltre, che gli Stati membri garantiscano che qualsiasi decisione di imporre sanzioni amministrative o misure di riparazione adottata ai sensi del paragrafo 2, lettera c) di tale articoli sia adeguatamente motivata e preveda il diritto di ricorso.
Art. 46		È concessa agli Stati membri la facoltà di decidere di non emanare norme relative a sanzioni amministrative o misure di riparazione per violazioni che, ai sensi del rispettivo diritto nazionale, siano passibili di sanzioni penali. Qualora abbiano deciso di imporre sanzioni penali per

		violazioni del regolamento, gli Stati membri devono provvedere affinché siano messe in atto misure adeguate per far sì che le autorità competenti dispongano di tutti i poteri necessari per stabilire contatti con le autorità giudiziarie, le autorità inquirenti o le autorità di giustizia penale della loro giurisdizione, al fine di ricevere informazioni specifiche sulle indagini o i procedimenti penali avviati per violazioni del presente regolamento, e di trasmetterle alle altre autorità competenti, nonché all'ABE, all'ESMA o all'EIOPA in modo tale che possano adempiere l'obbligo di cooperazione ai fini del regolamento. Si segnala che, qualora in relazione all'ordinamento nazionale si decida di stabilire sanzioni penali per le violazioni del regolamento, si renderanno pertanto necessari interventi normativi per la definizione delle predette misure.
Art. 47		Si prevede che gli Stati membri notifichino alla Commissione, all'ABE, all'ESMA e all'EIOPA le disposizioni legislative, regolamentari ed amministrative adottate in attuazione del Capo del regolamento relativo alle autorità competenti, incluse le eventuali norme di diritto penale applicabili, entro un anno dalla data di entrata in vigore del regolamento. Gli Stati membri devono, altresì, notificare senza indebito ritardo alla Commissione, all'ESMA, all'ABE e all'EIOPA tutte le successive modifiche.
Art. 48		Le disposizioni recano la disciplina della pubblicazione, da parte delle

		autorità competenti, delle decisioni con cui si impongono sanzioni o altre misure amministrative per la violazione del regolamento.