III

(Atti preparatori)

BANCA CENTRALE EUROPEA

PARERE DELLA BANCA CENTRALE EUROPEA

del 4 giugno 2021

su una proposta di regolamento del Parlamento europeo e del Consiglio relativo alla resilienza operativa digitale per il settore finanziario

(CON/2021/20)

(2021/C 343/01)

Introduzione e base giuridica

In data 22, 23 e 29 dicembre 2020 la Banca centrale europea (BCE) ha ricevuto, rispettivamente, dal Consiglio dell'Unione europea e dal Parlamento europeo richieste di parere in merito a una 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 ([1]) (di seguito, la «proposta di regolamento») e a una proposta di direttiva che modifica le direttive 2006/43/CE, 2009/65/CE, 2009/138/UE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 e UE/2016/2341 ([2]) (di seguito la «proposta di direttiva modificativa», insieme alla «proposta di regolamento», gli «atti proposti»).

La BCE è competente a formulare un parere in virtù dell'articolo 127, paragrafo 4, e dell'articolo 282, paragrafo 5, del trattato sul funzionamento dell'Unione europea, in quanto gli atti proposti contengono disposizioni che rientrano negli ambiti di competenza della BCE, in particolare la definizione e l'attuazione della politica monetaria, la promozione del regolare funzionamento dei sistemi di pagamento, il contributo alla buona conduzione delle politiche perseguite dalle autorità competenti in materia di stabilità del sistema finanziario e i compiti della BCE in materia di vigilanza prudenziale degli enti creditizi ai sensi dell'articolo 127, paragrafo 2, primo e quarto trattino, dell'articolo 127, paragrafo 5, e dell'articolo 127, paragrafo 6, del trattato. In conformità al primo periodo dell'articolo 17.5 del regolamento interno della Banca centrale europea, il Consiglio direttivo ha adottato il presente parere.

1. Osservazioni di carattere generale

1.1 La BCE accoglie con favore la proposta di regolamento, che mira a rafforzare la cibersicurezza e la resilienza operativa del settore finanziario. In particolare, la BCE accoglie con favore l'obiettivo della proposta di regolamento di eliminare gli ostacoli che si frappongono all'istituzione del mercato interno dei servizi finanziari e migliorarne il funzionamento, armonizzando le norme applicabili nel settore della gestione, della segnalazione e della verifica dei rischi relativi alle tecnologie dell'informazione e della comunicazione (TIC), nonché dei rischi relativi alle TIC derivanti da terzi. Inoltre, la BCE accoglie con favore l'obiettivo della proposta di regolamento di razionalizzare e armonizzare eventuali prescrizioni normative o aspettative di vigilanza che si sovrappongono e a cui le entità finanziare sono attualmente soggette ai sensi del diritto dell'Unione.

1.2 La BCE evince che, per quanto riguarda le entità finanziarie identificate come operatori di servizi essenziali ([3]), la proposta di regolamento rappresenta un atto giuridico settoriale dell'Unione ai sensi dell'articolo 1, paragrafo 7, della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio ([4]) (di seguito la «direttiva NIS»); ciò implica che i requisiti previsti dalla proposta di regolamento prevarrebbero, in linea di principio, sulla direttiva NIS. In pratica, le entità finanziare identificate come operatori di servizi essenziali ([5])

([1]) COM(2020) 595 final.
([2]) COM (2020) 596 final.
([3]) Cfr. l'articolo 1, paragrafo 2, della proposta di regolamento.
([4]) 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).
([5]) Cfr. l'articolo 5 della direttiva NIS.

segnalerebbero, tra l'altro, gli incidenti conformemente alla proposta di regolamento anziché alla direttiva NIS. Se da un lato la BCE accoglie con favore la riduzione delle potenziali sovrapposizioni di prescrizioni per le entità finanziarie nel settore della segnalazione degli incidenti, dall'altro si dovrebbe prestare maggiore attenzione all'interazione tra la proposta di regolamento e la direttiva NIS. Ad esempio, ai sensi della proposta di regolamento un fornitore terzo di servizi di TIC ([6]) potrebbe essere destinatario di raccomandazioni formulate dall"autorità di sorveglianza capofila ([7]). Allo stesso tempo, lo stesso fornitore terzo di servizi di TIC può essere classificato come operatore di servizi essenziali ai sensi della direttiva NIS ed essere soggetto a istruzioni vincolanti emesse dall'autorità competente ([8]). In tal caso, il fornitore terzo di servizi di TIC potrebbe essere soggetto a raccomandazioni contrastanti formulate ai sensi della proposta di regolamento e a istruzioni vincolanti emanate ai sensi della direttiva NIS. La BCE suggerisce che gli organi legislativi dell'Unione riflettano ulteriormente sulle potenziali incongruenze tra la proposta di regolamento e la direttiva NIS che possono ostacolare l'armonizzazione e la riduzione degli obblighi che si sovrappongono e contrastano per le entità finanziarie.

1.3 La BCE evince inoltre che, ai sensi della proposta di direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 ([9]) (di seguito la «proposta di direttiva NIS2»), i «quasi incidenti» ([10]) saranno soggetti a obblighi di segnalazione ([11]). Mentre il considerando n. 39 della proposta di direttiva NIS2 fa riferimento al significato del termine «quasi incidenti», non è chiaro se l'intenzione sia quella di esigere che i quasi incidenti siano segnalati dalle entità finanziarie elencate all'articolo 2 della proposta di regolamento. A tale riguardo, e tenendo conto anche del fatto che i quasi incidenti possono essere identificati come tali solo dopo che si sono verificati, la BCE gradirebbe ricevere tempestivamente la notifica dei quasi incidenti significativi, come avviene attualmente per gli incidenti informatici. La BCE suggerisce che vi dovrebbe essere un maggiore coordinamento tra la proposta di regolamento e la proposta di direttiva NIS2 al fine di chiarire l'esatto ambito di applicazione delle segnalazioni a cui una determinata entità finanziaria può essere soggetta ai sensi questi due, distinti ma connessi, atti legislativi dell'Unione. Allo stesso tempo, sarebbe necessario definire i «quasi incidenti» e sviluppare disposizioni che ne chiariscano la significatività.

1.4 La BCE accoglie con favore l'incoraggiamento delle entità finanziarie a condividere tra loro, su base volontaria, informazioni di intelligence sulle minacce informatiche al fine di rafforzare e potenziare le loro posizioni di resilienza informatica. La BCE stessa ha supportato l'iniziativa guidata dal mercato per la condivisione delle informazioni di intelligence sulle minacce informatiche (Cyber threat Intelligence Information Sharing Initiative, CIISI-EU) e ha reso disponibili i modelli per chiunque al fine di realizzare e promuovere una tale iniziativa ([12]).

1.5 La BCE sostiene la cooperazione tra le autorità competenti ai fini della proposta di regolamento, le autorità europee di vigilanza (AEV) e i gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRTS) ([13]). È essenziale scambiare informazioni al fine di garantire la resilienza operativa dell'Unione, in quanto la condivisione delle informazioni e la cooperazione tra le autorità possono contribuire a prevenire gli attacchi informatici e a ridurre la diffusione delle minacce connesse alle TIC. Sarebbe opportuno promuovere una comprensione comune dei rischi connessi alle TIC e garantire una valutazione coerente di tali rischi in tutta l'Unione. È della massima importanza che le autorità competenti scambino le informazioni con il punto di contatto unico ([14]) e con i CSIRT nazionali ([15]) solo in presenza di meccanismi di classificazione e condivisione delle informazioni chiaramente definiti, accompagnati da adeguate garanzie per garantire la riservatezza.

1.6 Infine, la BCE accoglierebbe con favore l'introduzione, nel quadro della proposta di regolamento, di norme in materia di dati personali e di conservazione dei dati. La durata del periodo di conservazione dovrebbe tenere conto dell'indagine, dell'ispezione, della richiesta di informazioni, della comunicazione, della pubblicazione, dell'esame, della verifica, della valutazione e dell'elaborazione dei piani di sorveglianza o di vigilanza che le autorità competenti possono dover svolgere nell'ambito dei rispettivi obblighi e doveri previsti dalla proposta di regolamento. A tale riguardo, un periodo di conservazione di 15 anni sarebbe adeguato. Questo

([6]) Cfr. l'articolo 3, paragrafo 15, della proposta di regolamento.
([7]) Cfr. l'articolo 31, paragrafo 1, lettera d), della proposta di regolamento.
([8]) Cfr. l'articolo 15, paragrafo 3, della direttiva NIS.
([9]) COM (2020) 823 final.
([10]) Eventi che avrebbero potenzialmente potuto causare un danno, ma che è stato efficacemente evitato prima che si verificasse; cfr. il considerando n. 39 della direttiva NIS2.
([11]) Cfr. articolo 11 della direttiva NIS2.
([12]) Cyber threat Intelligence Information Sharing Initiative (CIISI-EU), disponibile sul sito Internet della BCE all'indirizzo www.ecb.europa.eu.
([13]) Cfr. l'articolo 42 della proposta di regolamento.
([14]) Cfr. l'articolo 8, paragrafo 3, della direttiva NIS.
([15]) Cfr. anche gli articoli 11, 26 e 27 della direttiva NIS2.

periodo di conservazione dei dati potrebbe essere abbreviato o esteso, a seconda dei casi specifici. A tale proposito, la BCE suggerisce che gli organi legislativi dell'Unione, nella formulazione della pertinente disposizione sui dati personali e sulla conservazione dei dati, tengano conto anche del principio della minimizzazione dei dati, nonché dell'ulteriore trattamento a fini di archiviazione nell'interesse pubblico, di ricerca scientifica o storica o a fini statistici ([16]).

2. **Osservazioni specifiche sulla sorveglianza e la compensazione e il regolamento dei titoli**

2.1 *Competenze di sorveglianza del SEBC e dell'Eurosistema*

2.1.1 In stretta connessione con suoi compiti fondamentali di politica monetaria, il trattato e lo statuto del Sistema europeo di banche centrali e della Banca centrale europea (di seguito, lo «statuto del SEBC») prevedono che l'Eurosistema conduca la sorveglianza sui sistemi di compensazione e di pagamento. Ai sensi del quarto trattino dell'articolo 127, paragrafo 2, del trattato, come riflesso nell'articolo 3.1 dello statuto del SEBC, uno dei compiti fondamentali del SEBC è quello di promuovere il regolare funzionamento dei sistemi di pagamento. Nell'assolvimento di tale compito fondamentale, la BCE e le banche centrali nazionali possono accordare facilitazioni, e la BCE può stabilire regolamenti, al fine di assicurare sistemi di compensazione e di pagamento efficienti e affidabili all'interno dell'Unione e nei rapporti con i paesi terzi ([17]). In virtù del suo ruolo di sorveglianza, la BCE ha adottato il regolamento (UE) n. 795/2014 della Banca centrale europea (BCE/2014/28) (di seguito il «regolamento SPIS») ([18]). Il regolamento SPIS attua, in forma prescrittiva, i principi per le infrastrutture dei mercati finanziari emanati ad aprile 2012 dal Comitato sui sistemi di pagamento e di regolamento (Committee on Payment and Settlement Systems) e dall'Organizzazione internazionale delle commissioni dei valori mobiliari (International Organization of Securities Commissions) ([19]), che sono giuridicamente vincolanti e riguardano i sistemi di pagamento di importo rilevante e quelli al dettaglio di importanza sistemica, gestiti da una banca centrale dell'Eurosistema o da un soggetto privato. Il quadro di riferimento per le politiche di sorveglianza dell'Eurosistema ([20]) identifica gli strumenti di pagamento come parte integrante dei sistemi di pagamento e li include pertanto nell'ambito della sua sorveglianza. Il quadro di sorveglianza per gli strumenti di pagamento è attualmente in fase di revisione ([21]). In tale quadro, uno strumento di pagamento (ad esempio carta, bonifico, addebito diretto, trasferimento di moneta elettronica e token di pagamento digitale ([22])) è definito come un dispositivo personalizzato (o un insieme di dispositivi) e/o una serie di procedure concordate tra l'utente di servizi di pagamento e il prestatore di servizi di pagamento utilizzato per disporre un trasferimento di valore ([23]).

2.1.2 Alla luce di quanto precede, la BCE accoglie con favore l'esclusione dall'articolo relativo all'ambito di applicazione della proposta di regolamento degli operatori dei sistemi come definiti all'articolo 2, lettera p), della direttiva 98/26/CE del Parlamento europeo e del Consiglio ([24]), sui sistemi di pagamento (compresi quelli gestiti dalle banche centrali), sui sistemi di pagamento e sugli accordi di pagamento in vista dell'applicazione

([16]) Cfr. articoli 4, lettera b), e 13 del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

([17]) Cfr. articolo 22 dello statuto del SEBC.

([18]) Regolamento (CE) n .795/2014 della Banca centrale europea, del 3 luglio 2014, sugli obblighi di sorveglianza relativi a sistemi di pagamento di importanza sistemica (BCE/2014/28) (GU L 217 del 23.7.2014, pag. 16).

([19]) Disponibile sul sito internet della Banca dei regolamenti internazionali all'indirizzo www.bis.org.

([20]) Eurosystem oversight policy framework, Revised version (luglio 2016) disponibile sul sito Internet della BCE all'indirizzo www.ecb.europa.eu.

([21]) Cfr. quadro di riferimento rivisto e consolidato dell'Eurosistema per la sorveglianza di strumenti, schemi e meccanismi di pagamento elettronico (quadro di riferimento PISA) di ottobre 2021 (Eurosystem oversight framework for electronic payment instruments, schemes and arrangements, PISA framework), disponibile sul sito Internet della BCE all'indirizzo www.ecb.europa.eu.

([22]) Un token di pagamento digitale è una rappresentazione digitale di valore garantita da crediti o attività registrati altrove e che consente il trasferimento di valore tra utenti finali. A seconda della struttura sottostante, i token di pagamento digitali possono prevedere un trasferimento di valore senza necessariamente coinvolgere un soggetto terzo centrale e/o utilizzare conti di pagamento.

([23]) «Un trasferimento di valore» «L'atto, disposto dal pagatore o per suo conto o dal beneficiario, di trasferimento di fondi o token di pagamento digitale o di collocamento o ritiro di contante su/da un conto utente, indipendentemente da eventuali obblighi sottostanti tra il pagatore e il beneficiario. Il trasferimento può coinvolgere un singolo prestatore di servizi di pagamento o più di uno». Questa definizione di «trasferimento di valore» ai sensi del quadro di riferimento PISA si discosta dalla definizione di trasferimento di «fondi» ai sensi della direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE (GU L 337 del 23.12.2015, pag. 35). Un «trasferimento di valore» nel contesto di uno «strumento di pagamento» quale definito in detta direttiva può riferirsi solo a un trasferimento di «fondi». Ai sensi di detta direttiva, i «fondi» non comprendono i token di pagamento digitali a meno che i token possano essere classificati come moneta elettronica (o, più ipoteticamente, come moneta scritturale).

([24]) Direttiva 98/26/CE del Parlamento europeo e del Consiglio, del 19 maggio 1998, concernente il carattere definitivo del regolamento nei sistemi di pagamento e nei sistemi di regolamento titoli (GU L 166 dell'11.6.1998, pag. 45).

dei quadri di sorveglianza summenzionati. Per tali motivi, le competenze del SEBC ai sensi del trattato e le competenze dell'Eurosistema ai sensi del regolamento SPIS dovrebbero essere chiaramente esplicitate nei considerando della proposta di regolamento.

2.1.3 Analogamente, la BCE accoglie con favore l'esclusione dall'applicazione del quadro di sorveglianza stabilito nella proposta di regolamento dei fornitori terzi di servizi di TIC che sono soggetti ai quadri di sorveglianza istituiti a supporto dei compiti di cui all'articolo 127, paragrafo 2, del trattato ([25]). A tale riguardo, la BCE desidera sottolineare che le banche centrali del SEBC operanti nell'esercizio delle loro funzioni monetarie ([26]) e l'Eurosistema nel fornire servizi tramite TARGET2, TARGET2-Securites (T2S) ([27]) e il servizio di regolamento dei pagamenti istantanei in TARGET (TARGET Instant Payment Settlement, TIPS) ([28]) non rientrano nell'articolo relativo all'ambito di applicazione della proposta di regolamento, né possono essere considerate fornitori terzi di servizi di TIC e quindi potenzialmente classificati come fornitori terzi di servizi di TIC critici ai fini della proposta di regolamento. L'Eurosistema sorveglia T2S in relazione al suo mandato di assicurare sistemi di compensazione e di pagamento efficienti e affidabili. Inoltre, l'ESMA ha chiarito che T2S non è un fornitore di servizi critici ([29]) ai sensi del regolamento (UE) n. 909/2014 del Parlamento europeo e del Consiglio ([30]) (di seguito, il «regolamento sui CSD»). Di conseguenza, la sicurezza organizzativa e operativa, l'efficienza e la resilienza di T2S sono garantite attraverso il quadro giuridico, regolamentare e operativo applicabile e i dispositivi di governance concordati di T2S, anziché attraverso il regolamento sui CSD.

2.1.4 Inoltre, il quadro di riferimento per le politiche di sorveglianza dell'Eurosistema ([31]) ricomprende i fornitori di servizi critici come la Society for Worldwide Interbank Financial Telecommunication (SWIFT). La SWIFT è una società cooperativa a responsabilità limitata con sede in Belgio, che fornisce servizi di messaggistica sicura a livello internazionale. La Nationale Bank van België/Banque Nationale de Belgique funge da autorità di sorveglianza capofila di SWIFT e svolge, sulla base di un accordo di sorveglianza cooperativa, la sorveglianza nei confronti di SWIFT, in collaborazione con le altre banche centrali del G10, compresa la BCE. Le autorità di sorveglianza del G10 riconoscono che il fulcro della sorveglianza è il rischio operativo di SWIFT, in quanto è considerato la principale categoria di rischio attraverso cui SWIFT potrebbe comportare un rischio sistemico per il sistema finanziario dell'Unione. A tale riguardo, il gruppo di sorveglianza cooperativa di SWIFT ha elaborato una serie specifica di principi e aspettative di alto livello che si applicano a SWIFT, quali l'identificazione e la gestione dei rischi, la sicurezza delle informazioni, l'affidabilità e la resilienza, la pianificazione tecnologica e la comunicazione con gli utenti. Le autorità di sorveglianza del G10 si aspettano che SWIFT aderisca agli orientamenti del Comitato per i pagamenti e le infrastrutture di mercato (CPMI) e dell'Organizzazione internazionale delle commissioni sui valori mobiliari (IOSCO) sulla ciberresilienza ([32]), nonché ad altre norme internazionali in materia di sicurezza delle TIC che, considerate nel loro insieme, superano i requisiti stabiliti nella proposta di regolamento.

2.1.5 Non è certo che SWIFT e forse altri fornitori di servizi soggetti al quadro di riferimento per le politiche di sorveglianza dell'Eurosistema possano essere sottoposti alla proposta di regolamento quali fornitori terzi di servizi ICT qualora prestino servizi non ricompresi nell'articolo 127, paragrafo 2, del trattato. La BCE accoglie pertanto con grande favore il fatto che i fornitori di servizi già soggetti al quadro di riferimento per le politiche di sorveglianza dell'Eurosistema, tra cui, ma non solo, SWIFT, siano esclusi dall'ambito di applicazione del quadro di riferimento per la sorveglianza stabilito dalla proposta di regolamento.

([25]) Cfr. l'articolo 28, paragrafo 5, della proposta di regolamento.

([26]) Cfr. il paragrafo 1.3 del parere della Banca centrale europea, del 19 febbraio 2021, su una proposta di regolamento relativo ai mercati delle cripto-attività e che modifica la Direttiva (UE) 2019/1937 (CON/2021/4). Tutti i pareri della BCE sono pubblicati su EUR-Lex.

([27]) Cfr. l'allegato II bis dell'indirizzo BCE/2012/27 della Banca centrale europea, del 5 dicembre 2012, relativo ad un sistema di trasferimento espresso transeuropeo automatizzato di regolamento lordo in tempo reale (TARGET2) (GU L 30 del 30.1.2013, pag. 1); l'indirizzo BCE/2012/13 della Banca centrale europea, del 18 luglio 2012, relativo a TARGET2-Securities (GU L 215 dell'11.8.2012, pag. 19); la decisione BCE/2011/20 della Banca centrale europea, del 16 novembre 2011, recante disposizioni e procedure dettagliate per l'applicazione dei criteri di idoneità dei depositari centrali di titoli all'accesso ai servizi di TARGET2-Securities (GU L 319 del 2.12.2011, pag. 117). Cfr. anche il contratto quadro per T2S e il contratto collettivo.

([28]) Cfr. l'allegato II ter della decisione BCE/2012/27.

([29]) Cfr. l'articolo 30, paragrafo 5, del regolamento (UE) n. 909/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, relativo al miglioramento del regolamento titoli nell'Unione europea e ai depositari centrali di titoli e recante modifica delle direttive 98/26/CE e 2014/65/UE e del regolamento (UE) n. 236/2012 (GU L 257 dell'28.8.2014, pag. 1) e l'articolo 68 del regolamento delegato (UE) 2017/392 della Commissione, dell'11 novembre 2016, che integra il regolamento (UE) n. 909/2014 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione in materia di autorizzazione, vigilanza e requisiti operativi per i depositari centrali di titoli (GU L 65 del 10.3.2017, pag. 48).

([30]) Regolamento (UE) n. 909/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, relativo al miglioramento del regolamento titoli nell'Unione europea e ai depositari centrali di titoli e recante modifica delle Direttive 98/26/CE e 2014/65/UE e del Regolamento (UE) n. 236/2012 (GU L 257 del 28.8.2014, pag. 1).

([31]) Eurosystem oversight policy framework, versione rivista (luglio 2016), disponibile sul sito Internet della BCE all'indirizzo www.ecb.europa.eu.

([32]) Disponibile sul sito Internet della Banca dei regolamenti internazionali all'indirizzo www.bis.org.

2.2 *Competenze del SEBC nel settore del regolamento titoli*

2.2.1 I depositari centrali di titoli (CSD) sono infrastrutture dei mercati finanziari (IMF) rigorosamente regolamentate e soggette alla vigilanza di diverse autorità a norma del regolamento sui CSD, che stabilisce i requisiti relativi al regolamento degli strumenti finanziari, nonché le norme sull'organizzazione e la conduzione dei CSD. Inoltre, i CDS dovrebbero prendere atto degli orientamenti del Comitato per i pagamenti e le infrastrutture di mercato (CPIM) e dell'International Organization of Securities Commissions (IOSCO) sulla ciberresilienza, che sono stati resi operativi dal documento «Eurosystem Cyber Resilience Oversight Expectations for financial market infrastructures» (dicembre 2018) ([33]). Oltre alle competenze di vigilanza conferite alle autorità nazionali competenti (ANC) ai sensi del regolamento sui CSD, i membri del SEBC agiscono in qualità di «autorità competenti», nella loro qualità di autorità di sorveglianza dei sistemi di regolamento titoli gestiti dai CSD, banche centrali che emettono le valute più rilevanti nelle quali avviene il regolamento e banche centrali nei cui libri contabili è regolata la parte in contante delle operazioni ([34]). A tale riguardo, in base al considerando n. 8 del regolamento sui CSD, il regolamento dovrebbe applicarsi lasciando impregiudicate le competenze della BCE e delle banche centrali nazionali al fine di garantire la solidità e l'efficienza dei sistemi di compensazione e di pagamento all'interno dell'Unione e in altri paesi. In base al considerando n. 8, inoltre, il regolamento sui CSD non dovrebbe impedire ai membri del SEBC di accedere alle informazioni pertinenti all'esercizio delle loro funzioni ([35]), compresa la sorveglianza dei CSD e di altre IMF ([36]).

2.2.2 Inoltre, i membri del SEBC spesso agiscono come agenti di regolamento per la parte in contante delle operazioni in titoli e l'Eurosistema offre servizi di regolamento tramite T2S ai CSD. La sorveglianza esercitata dall'Eurosistema su T2S è connessa al suo mandato di assicurare sistemi di compensazione e di pagamento efficienti e solidi, mentre le autorità competenti e rilevanti dei CSD mirano a garantirne il regolare funzionamento, la sicurezza e l'efficienza dei regolamenti e il corretto funzionamento dei mercati finanziari nelle rispettive giurisdizioni.

2.2.3 Ai sensi della proposta di regolamento ([37]), le banche centrali del SEBC non sono coinvolte nell'elaborazione delle norme tecniche riguardanti la specificazione dei rischi relativi alle TIC. Analogamente, ai sensi della proposta di regolamento ([38]), le autorità competenti non sono informate in merito agli incidenti relativi alle TIC. La banca centrale del SEBC dovrebbe mantenere lo stesso livello di coinvolgimento attualmente previsto dal regolamento sui CSD e le autorità rilevanti dovrebbero essere informate degli incidenti relativi alle TIC. L'Eurosistema è l'autorità rilevante per tutti i CSD dell'area dell'euro e per diversi altri CSD dell'Unione. Le banche centrali del SEBC dovrebbero essere informate in merito agli incidenti relativi alle TIC che sono rilevanti per l'esercizio delle loro funzioni, compresa la sorveglianza dei CSD e di altre IMF. I rischi a cui sono esposti i CSD, compresi i rischi relativi alle TIC, hanno la potenzialità di minacciare il buon funzionamento dei CSD. Pertanto, i rischi relativi alle TIC sono importanti per le autorità rilevanti, alle quali dovrebbe essere fornita una panoramica completa e dettagliata di tali rischi al fine di valutarli e influenzare l'approccio di gestione dei rischi dei CSD. La proposta di regolamento non dovrebbe prevedere requisiti meno restrittivi per quanto riguarda i rischi relativi alle TIC rispetto a quelli previsti dal regolamento sui CSD e dalle relative norme tecniche di regolamentazione attuali.

2.2.4 Inoltre, gli organi legislativi dell'Unione dovrebbero chiarire l'interazione tra la proposta di regolamento ([39]) e le norme tecniche di regolamentazione che integrano il regolamento sui CSD. In particolare, non è chiaro se un CSD debba essere esentato dall'obbligo di avere un proprio sito secondario nel caso in cui il suo fornitore terzo di servizi di TIC mantenga un tale sito ([40]) Nel caso in cui un CSD sia esentato dall'obbligo di mantenere un sito

([33]) Disponibile sul sito della BCE all'indirizzo www.ecb.europa.eu.

([34]) Cfr. l'articolo 12 del regolamento (UE) n. 909/2014.

([35]) Cfr. anche l'articolo 13, l'articolo 17, paragrafo 4, e l'articolo 22, paragrafo 6, del regolamento (UE) n. 909/2014.

([36]) Cfr. il paragrafo 7.3 del parere della Banca centrale europea del 6 aprile 2017 relativo all'identificazione e alla vigilanza delle infrastrutture critiche ai fini della sicurezza della tecnologia informatica (CON/2017/10), il paragrafo 7.2 del parere della Banca centrale europea dell'8 novembre 2018 sulla designazione di servizi essenziali e di operatori di servizi essenziali ai fini della sicurezza delle reti e dei sistemi informativi (CON/2018/47), il paragrafo 3.5.2 del parere della Banca centrale europea del 2 maggio 2019 relativo alla sicurezza delle reti e dei sistemi informativi (CON/2019/17), il paragrafo 3.5.2 del parere della Banca centrale europea dell'11 novembre 2019 relativo alla sicurezza delle reti e dei sistemi informativi (CON/2019/38).

([37]) Cfr. l'articolo 54, paragrafo 5, della proposta di regolamento e l'articolo 45, paragrafo 7, del regolamento (UE) n. 909/2014.

([38]) Cfr. l'articolo 54, paragrafo 4, della proposta di regolamento e l'articolo 45, paragrafo 6, del regolamento (UE) n. 909/2014.

([39]) Cfr. l'articolo 11, paragrafo 5, della proposta di regolamento.

([40]) Cfr. l'articolo 78 del regolamento delegato (UE) 2017/392 della Commissione, dell'11 novembre 2016, che integra il regolamento (UE) n. 909/2014 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione in materia di autorizzazione, vigilanza e requisiti operativi per i depositari centrali di titoli (GU L 65 del 10.3.2017, pag. 48).

secondario, non è chiaro quale valore giuridico avrebbe tale obbligo. Analogamente, la proposta di regolamento ([41]) fa riferimento a obiettivi in materia di punti e tempi di ripristino di ciascuna funzione ([42]), mentre la pertinente norma tecnica di regolamentazione distingue tra funzioni critiche ([43]) e operazioni critiche ([44]) in relazione ai tempi di ripristino fissati per le operazioni critiche dei CSD. Sono necessari ulteriori chiarimenti e riflessioni da parte degli organi legislativi dell'Unione sull'interazione tra la proposta di regolamento e le norme tecniche di regolamentazione che integrano il regolamento sui CSD al fine di evitare il rischio di requisiti contrastanti. Infine, si dovrebbe chiarire che le esenzioni concesse ai CSD gestiti da determinati enti pubblici a norma del regolamento sui CSD ([45]) sono estese ai sensi della proposta di regolamento.

2.3 *Competenze del SEBC nel settore della compensazione in titoli*

2.3.1 Alle banche centrali del SEBC sono attribuite competenze di sorveglianza in relazione alle controparti centrali (central counterparties, CCP). A tale riguardo, le banche centrali nazionali dell'Eurosistema spesso cooperano con le pertinenti autorità nazionali competenti nelle funzioni di sorveglianza e vigilanza delle CCP e partecipano al collegio delle rispettive CCP istituito ai sensi del regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio ([46]) (di seguito «EMIR»). I pertinenti membri dell'Eurosistema ([47]) partecipano ai collegi EMIR nella loro funzione di sorveglianza e rappresentano l'Eurosistema come banca centrale di emissione per le CCP in cui l'euro è una delle valute più rilevanti per gli strumenti finanziari compensati (e per le CCP offshore che compensano una parte significativa degli strumenti finanziari in euro). La BCE è la banca centrale di emissione per le CCP non appartenenti all'area dell'euro.

2.3.2 Ai sensi della proposta di regolamento ([48]), le banche centrali del SEBC non sono coinvolte nell'elaborazione delle norme tecniche riguardanti la specificazione dei rischi relative alle TIC. Inoltre, la proposta di regolamento ([49]) non contiene alcun riferimento ai requisiti in termini di obiettivi in materia di punti e di ripristino ai sensi dell'EMIR ([50]). L'assetto normativo proposto non dovrebbe prevedere requisiti meno restrittivi in materia di rischi relativi alle TIC rispetto a quelli attualmente esistenti. È pertanto fondamentale fissare degli obiettivi in materia di punti e tempi di ripristino al fine di disporre di un solido quadro di gestione della continuità operativa. Il mantenimento di specifici obiettivi in materia di punti e tempi di ripristino rientra anche nei principi per le infrastrutture dei mercati finanziari CPMI-IOSCO ([51]). L'attuale disposizione dell'EMIR dovrebbe essere mantenuta e la proposta di regolamento dovrebbe essere adattata di conseguenza. Le banche centrali del SEBC dovrebbero essere coinvolte nella preparazione di qualsiasi legislazione di livello secondario, nonché in ulteriori chiarimenti e riflessioni da parte degli organi legislativi dell'Unione sull'interazione tra la proposta di regolamento e le norme tecniche di regolamentazione integrative, in modo da evitare il rischio di requisiti contrastanti o che si sovrappongono.

3. **Osservazioni specifiche sugli aspetti di vigilanza prudenziale**

3.1 Il regolamento (UE) n. 1024/2013 ([52]) (di seguito il «regolamento sull'MVU») attribuisce alla BCE compiti specifici in materia di vigilanza prudenziale degli enti creditizi dell'area dell'euro e attribuisce alla BCE la responsabilità del funzionamento efficace e coerente del meccanismo di vigilanza unico (MVU) nell'ambito del quale le specifiche responsabilità di vigilanza prudenziale sono ripartite tra la BCE e le ANC partecipanti. In particolare, la BCE ha il compito di autorizzare e revocare le autorizzazioni di tutti gli enti creditizi. La BCE ha anche il compito, tra gli altri, di assicurare il rispetto della pertinente normativa dell'Unione che impone agli enti creditizi requisiti prudenziali, compreso l'obbligo di adottare solidi dispositivi di governo societario, quali solidi processi di gestione del rischio e meccanismi di controllo interno ([53]). A tal fine, alla BCE sono conferiti tutti i poteri di vigilanza per intervenire

([41]) Cfr. l'articolo 11, paragrafo 6, della proposta di regolamento.
([42]) Cfr. l'articolo 3, paragrafo 17, della proposta di regolamento.
([43]) Cfr. l'articolo 76, paragrafo 2, lettera d), del regolamento delegato (UE) 2017/392 della Commissione.
([44]) Cfr. l'articolo 78, paragrafi 2 e 3, del regolamento delegato (UE) 2017/392 della Commissione.
([45]) Cfr. l'articolo 1, paragrafo 4, del Regolamento (UE) n. 909/2014.
([46]) Regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio, del 4 luglio 2012, sugli strumenti derivati OTC, le controparti centrali e i repertori di dati sulle negoziazioni (GU L 201 del 27.7.2012, pag. 1).
([47]) Cfr. l'articolo 18, paragrafo 2, lettere g) e h), dell'EMIR.
([48]) Cfr. l'articolo 53, paragrafo 2, lettera b), e paragrafo 3, della proposta di regolamento e l'articolo 34, paragrafo 3, dell'EMIR.
([49]) Cfr. l'articolo 53, paragrafo 2, lettera a), della proposta di regolamento.
([50]) Cfr. l'articolo 34 dell'EMIR.
([51]) Cfr. Principi per le infrastrutture dei mercati finanziari CPIM-IOSCO disponibili sul sito Internet della Banca dei regolamenti internazionali all'indirizzo www.bis.org.
([52]) Regolamento (UE) n. 1024/2013 del Consiglio, del 15 ottobre 2013, che attribuisce alla Banca centrale europea compiti specifici in merito alle politiche in materia di vigilanza prudenziale degli enti creditizi (GU L 287 del 29.10.2013, pag. 63).
([53]) Cfr. l'articolo 4, paragrafo 1, lettera e) e l'articolo 6, paragrafo 4, del regolamento (UE) n. 1024/2013.

nell'attività degli enti creditizi, poteri che sono necessari al fine dell'esercizio delle sue funzioni. La BCE e le ANC rilevanti sono pertanto le autorità competenti che esercitano determinati poteri di vigilanza prudenziale ai sensi del regolamento n. 2013/575/UE del Parlamento europeo e del Consiglio ([54]) (di seguito «regolamento sui requisiti patrimoniali») e della direttiva n. 2013/36/UE del Parlamento europeo e del Consiglio ([55]) (di seguito «direttiva sui requisiti patrimoniali»).

3.2 La proposta di regolamento precisa che sarebbe opportuno perfezionare il codice unico e il sistema di vigilanza per coprire la resilienza operativa digitale e la sicurezza delle TIC, ampliando i mandati delle autorità di vigilanza finanziaria incaricate di monitorare e tutelare la stabilità finanziaria e l'integrità del mercato ([56]). L'obiettivo è promuovere un quadro generale per i rischi operativi o relativi alle TIC attraverso l'armonizzazione delle principali prescrizioni sulla resilienza operativa digitale per tutte le entità finanziarie ([57]). In particolare, la proposta di regolamento mira a consolidare e aggiornare le prescrizioni in materia di rischi relativi alle TIC trattati finora separatamente in diversi atti legislativi ([58]).

3.3 I requisiti concernenti i rischi relativi alle TIC per il settore finanziario sono attualmente rinvenibili in una serie di atti legislativi dell'Unione, tra cui la direttiva sui requisiti patrimoniali, e in strumenti normativi non vincolanti (come gli orientamenti dell'ABE), oltre a essere eterogenei e talvolta incompleti. In alcuni casi, il rischio relativo alle TIC è stato affrontato solo implicitamente come parte del rischio operativo, mentre in altri casi non è stato affrontato del tutto. Si dovrebbe ovviare a tale situazione allineando la proposta di regolamento con tali atti. A tal fine, la proposta di direttiva modificativa formula una serie di modifiche che appaiono necessarie per apportare chiarezza e coerenza giuridiche in relazione all'applicazione delle prescrizioni sulla resilienza operativa digitale. Tuttavia, le modifiche alla direttiva sui requisiti patrimoniali attualmente suggerite dalla proposta di direttiva modificativa ([59]) si riferiscono solo alle disposizioni sui piani di emergenza e di continuità operativa ([60]), dato che, presumibilmente, esse fungono implicitamente da base per affrontare la gestione dei rischi relativi alle TIC.

3.4 Inoltre, la proposta di regolamento ([61]) prevede che le entità finanziarie, compresi gli enti creditizi, predispongono quadri di gestione e di controllo interni che garantiscano una gestione efficace e prudente di tutti i rischi relativi alle TIC. La proposta di regolamento ([62]) prevede l'applicazione a livello individuale e consolidato dei requisiti ivi stabiliti, ma senza un sufficiente coordinamento con la normativa settoriale cui si fa riferimento. Infine, ai sensi della proposta di regolamento ([63]), fatte salve le disposizioni sul quadro di sorveglianza per i fornitori terzi di servizi di TIC critici di cui alla proposta di regolamento ([64]), il rispetto degli obblighi ivi stabiliti è assicurato, per gli enti creditizi, dall'autorità competente designata in conformità dell'articolo 4 della direttiva sui requisiti patrimoniali, fatti salvi i compiti specifici conferiti alla BCE dal regolamento sull'MVU.

3.5 Alla luce di quanto precede, la BCE evince che, per quanto riguarda gli enti creditizi, e fatte salve le disposizioni della proposta di regolamento relative al quadro di sorveglianza per i fornitori terzi di servizi di TIC critici ([65]), la proposta di regolamento intende stabilire un quadro di governance interna prudenziale per la gestione del rischio relativo alle TIC che sarà integrato nel quadro generale di governance interna ai sensi della direttiva sui requisiti patrimoniali. Inoltre, data la natura prudenziale del quadro proposto, le autorità competenti responsabili della vigilanza sul rispetto degli obblighi stabiliti del quadro proposto, compresa la BCE, saranno le autorità responsabili della vigilanza bancaria conformemente al regolamento sull'MVU.

([54]) Regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento e che modifica il Regolamento (UE) n. 648/2012 (GU L 176 del 26.6.2013, pag. 1).

([55]) Direttiva 2013/36/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE (GU L 176 del 27.6.2013, pag. 338).

([56]) Cfr. considerando n. 8 della proposta di regolamento.

([57]) Cfr. considerando n. 11 della proposta di regolamento.

([58]) Cfr. considerando n. 12 della proposta di regolamento.

([59]) Cfr. i considerando n. 4 e n. 5 della proposta di direttiva modificativa.

([60]) Cfr. l'articolo 85 della direttiva sui requisiti patrimoniali.

([61]) Cfr. l'articolo 4, paragrafo 1, della proposta di regolamento.

([62]) Cfr. l'articolo 25, paragrafi 3 e 4, della proposta di regolamento.

([63]) Cfr. l'articolo 41 della proposta di regolamento.

([64]) Cfr. la sezione II del capo V della proposta di regolamento.

([65]) Cfr. la sezione II del capo V della proposta di regolamento.

3.6 Gli organi legislativi dell'Unione possono pertanto voler prendere in considerazione i seguenti suggerimenti al fine aumentare la chiarezza e il coordinamento tra la proposta di regolamento e la direttiva sui requisiti patrimoniali. In primo luogo, i requisiti previsti dalla proposta di regolamento possono essere espressamente qualificati come prudenziali, come è stato fatto, tra l'altro, nel regolamento sui CSD ([66]). In secondo luogo, si potrebbe ampliare la formulazione dei considerando della proposta di direttiva modificativa ([67]), dato che i requisiti previsti dalla proposta di regolamento vanno al di là della sola fase dei piani di emergenza e di continuità operativa. Nel complesso, le misure di governance dei rischi relativi alle TIC rientrano nell'ambito più generale dei solidi dispositivi di governance di cui all'articolo 74 della direttiva sui requisiti patrimoniali ([68]). In terzo luogo, la proposta di regolamento ([69]) dovrebbe essere modificata al fine di richiamare nei considerando la competenza della BCE in materia di vigilanza prudenziale degli enti creditizi ai sensi del trattato e del regolamento sull'MVU. In quarto luogo, dovrebbe essere rivisto il riferimento all'applicazione a livello individuale e consolidato dei requisiti ivi previsti ([70]), in quanto i livelli subconsolidati e consolidati non sono definiti nella proposta di regolamento e alcuni tipi di intermediari non sono soggetti a vigilanza su base consolidata ai sensi della legislazione pertinente (ad esempio gli istituti di pagamento). Inoltre, il livello di applicazione dei requisiti previsti dalla proposta di regolamento dovrebbe derivare esclusivamente dalla legislazione applicabile a ciascun tipo di entità finanziaria. Nel caso degli enti creditizi, è previsto un chiaro collegamento tra la direttiva sui requisiti patrimoniali e la proposta di regolamento, per cui i requisiti previsti dalla proposta di regolamento si applicherebbero automaticamente a livello individuale, subconsolidato o consolidato ([71]), a seconda dei casi. Infine, gli organi legislativi dell'Unione potrebbero prendere in considerazione la possibilità di prevedere un regime transitorio per gestire il periodo compreso tra l'entrata in vigore della proposta di regolamento e l'entrata in vigore delle norme tecniche di regolamentazione previste nella proposta di regolamento, dato che alcuni intermediari, compresi gli enti creditizi, sono già soggetti a norme sui rischi relativi alle TIC che sono applicabili a settori specifici e sono più dettagliate rispetto alle disposizioni generali della proposta di regolamento.

3.7 Ai sensi del regolamento sull'MVU, alla BCE è stato conferito il compito di assicurare il rispetto, da parte degli enti creditizi, dei requisiti del diritto dell'Unione che impongono agli enti creditizi di dotarsi di solidi processi di gestione del rischio e meccanismi di controllo interno ([72]). Ciò significa che la BCE deve assicurare che gli enti creditizi attuino politiche e processi per valutare e gestire la loro esposizione al rischio operativo, compreso il rischio di modello, e per coprire gli eventi di elevata gravità e di scarsa frequenza. Gli enti creditizi sono tenuti a precisare cosa costituisca il rischio operativo ai fini di tali politiche e procedure ([73]).

3.8 Nel luglio 2017 il Consiglio direttivo della Banca centrale europea (BCE) ha adottato il quadro per la segnalazione degli incidenti informatici dell'MVU (di seguito il «Quadro di riferimento»), sulla base di un progetto del Consiglio di vigilanza in conformità dell'articolo 26, paragrafo 8, e dell'articolo 6, paragrafo 2, del regolamento sull'MVU e dell'articolo 21, paragrafo 1, del regolamento (UE) n. 468/2014 della Banca centrale europea (ECB/2014/17) ([74]). Il Quadro di riferimento consiste in una richiesta vincolante (decisioni individuali indirizzate agli enti creditizi) di informazioni e/o segnalazioni sulla base dell'articolo 10 del regolamento sull' MVU ([75]). Alcuni paesi dispongono già di un processo di segnalazione degli incidenti che impone agli enti creditizi di segnalare tutti gli incidenti informatici significativi alle rispettive ANC. In tali paesi, gli enti creditizi significativi segnaleranno ancora gli incidenti alle ANC, che li trasmetteranno senza indebito ritardo alla BCE per conto dei soggetti vigilati. Pertanto, le decisioni di cui sopra sono indirizzate anche a tali autorità nazionali competenti affinché trasmettano tali

([66]) Cfr. titolo del capo II, sezione 4, «Requisiti prudenziali» del regolamento sui CSD.

([67]) Cfr. considerando n. 4 della proposta di direttiva modificativa.

([68]) L'articolo 85 della direttiva 2013/36/UE è una mera specificazione. A tale riguardo, si vedano anche le pagine 4, 11 e 37 degli orientamenti dell'Autorità bancaria europea sulla gestione dei rischi relativi alle TIC e di sicurezza (Guidelines on ICT and security risk management) del 29 novembre 2019 (di seguito gli «orientamenti ABE»), in cui la base giuridica generale è espressamente contenuta nell'articolo 74 della direttiva 2013/36/UE.

([69]) Cfr. l'articolo 41, paragrafo 1, della proposta di regolamento.

([70]) V. l'articolo 25, paragrafi 3 e 4, della proposta di regolamento.

([71]) Cfr. l'articolo 109 della direttiva sui requisiti patrimoniali.

([72]) Cfr. l'articolo 4, paragrafo 1, lettera e), del regolamento sull'MVU.

([73]) Cfr. l'articolo 85 della direttiva sui requisiti patrimoniali.

([74]) Regolamento (UE) n. 468/2014 della Banca centrale europea, del 16 aprile 2014, che istituisce il quadro di cooperazione nell'ambito del Meccanismo di vigilanza unico tra la Banca centrale europea e le autorità nazionali competenti e con le autorità nazionali designate (Regolamento quadro sull'MVU) (BCE/2014/17) (GU L 141 del 14.5.2014, pag. 1).

([75]) In particolare, un incidente informatico (una identificata possibile violazione della sicurezza delle informazioni, sia dolosa che accidentale) deve essere segnalato alla BCE se è soddisfatta almeno una delle seguenti condizioni: (1) l'impatto finanziario potenziale è pari a 5 milioni di euro o pari allo 0,1 % del capitale primario di classe 1 (Common Equity Tier 1, CET1); (2) l'incidente è reso pubblico o causa danni d'immagine; (3) l'incidente è stato segnalato al Chief Information Officer (CIO) al di fuori delle normali segnalazioni; (4) la banca ha notificato l'incidente alle squadre CERT/ai CSIRT, a un'agenzia di sicurezza o alla polizia; (5) sono state avviate procedure di ripristino in caso di disastro o di continuità operativa o è stata presentata una richiesta di indennizzo di assicurazione informatica; (6) si è verificata una violazione dei requisiti giuridici o regolamentari; oppure (7) la banca utilizza la valutazione di esperti e criteri interni (compreso un potenziale impatto sistemico) e decide di informare la BCE.

informazioni alla BCE sulla base del Quadro di riferimento. La BCE sostiene gli sforzi degli organi legislativi dell'Unione volti a promuovere l'armonizzazione e la razionalizzazione, tra l'altro, dell'insieme di norme e obblighi applicabili agli enti creditizi in materia di segnalazione degli incidenti. In considerazione di ciò, la BCE è pronta a modificare (ed eventualmente abrogare) il Quadro di riferimento, ove necessario, alla luce dell'eventuale adozione della proposta di regolamento.

4. **Osservazioni specifiche sulla gestione dei rischi relativi alle TIC, la segnalazione degli incidenti, i test di resilienza operativa e i rischi relativi alle TIC derivanti da terzi**

4.1 *Gestione dei rischi relativi alle TIC*

4.1.1 La BCE accoglie con favore l'introduzione da parte della proposta di regolamento di un quadro solido e completo per la gestione dei rischi relativi alle TIC che comprende gli orientamenti CPMI-IOSCO sulla ciberresilienza ed è strettamente allineato alle migliori pratiche, tra cui il documento «Eurosystem Cyber Resilience Oversight Expectations for FMIs».

4.1.2 La BCE sostiene l'idea che le entità finanziarie debbano effettuare valutazioni del rischio in occasione di ogni «modifica di rilievo» dell'infrastruttura della rete e del sistema informativo ([76]). Ciò detto, la proposta di regolamento non contiene alcuna definizione di «modifica di rilievo», il che crea un indesiderato margine di discrezionalità per interpretazioni divergenti da parte delle entità finanziarie che potrebbero in ultima analisi ostacolare gli obiettivi di armonizzazione della proposta di regolamento. Ai fini della certezza del diritto, gli organi legislativi dell'Unione potrebbero voler prendere in considerazione l'introduzione di una definizione di «modifica di rilievo» nella proposta di regolamento.

4.1.3 La BCE sostiene in generale l'idea che le entità finanziarie diverse dalle microimprese segnalino alle autorità competenti i costi e le perdite rilevanti causati dalle perturbazioni a livello di TIC e dagli incidenti connessi alle TIC ([77]). Tuttavia, per garantire l'efficacia complessiva del sistema ed evitare la possibilità di sommergere le autorità competenti e le entità finanziarie con un eccessivo numero di segnalazioni, l'introduzione di soglie pertinenti, eventualmente di natura quantitativa, potrebbe essere utilmente esaminata dagli organi legislativi dell'Unione.

4.1.4 La BCE riconosce la possibilità che le entità finanziarie deleghino a imprese interne o esterne al gruppo i compiti di verifica della conformità alle prescrizioni in materia di gestione dei rischi relativi alle TIC, previa approvazione delle autorità competenti ([78]). Allo stesso tempo, è importante che gli organi legislativi dell'Unione chiariscano in che modo l'approvazione da parte delle autorità competenti sarebbe concessa nei casi in cui un'entità finanziaria sia soggetta a più autorità competenti. Ciò potrebbe verificarsi quando un'entità finanziaria è un ente creditizio, un fornitore di servizi per le cripto-attività e/o un prestatore di servizi di pagamento. Infine, per quanto riguarda l'identificazione e la classificazione che le entità finanziarie devono effettuare ai sensi della proposta di regolamento ([79]), la BCE ritiene prudente, ai fini della classificazione delle attività, che la proposta di regolamento imponga anche alle entità finanziarie di tenere conto della criticità di tali attività (ossia se sostengono funzioni essenziali).

4.2 *Segnalazione degli incidenti*

4.2.1 La BCE accoglie con favore gli sforzi delineati nella proposta di regolamento per armonizzare il quadro di segnalazione degli incidenti relativi alle TIC all'interno dell'Unione e per adoperarsi per una segnalazione centralizzata degli incidenti gravi connessi alle TIC ([80]). L'introduzione di un quadro armonizzato per la segnalazione di incidenti gravi connessi alle TIC ([81]) alle autorità competenti in linea di principio semplificherebbe e armonizzerebbe l'onere di segnalazione delle entità finanziarie, compresi gli enti creditizi. Le autorità competenti trarrebbero vantaggio dal più ampio campo di applicazione degli incidenti contemplati, andando oltre gli incidenti informatici attualmente contemplati dai quadri di riferimento esistenti ([82]). La futura adozione della proposta di regolamento richiederebbe un riesame e un'eventuale abrogazione dei quadri di riferimento esistenti, compreso il quadro per la segnalazione degli incidenti informatici dell'MVU. Ciò detto, al fine di conseguire una reale razionalizzazione e il pieno allineamento in tutti i quadri di riferimento, è fondamentale garantire che l'ambito di

([76]) Cfr. l'articolo 7, paragrafo 3, della proposta di regolamento.
([77]) Cfr. l'articolo 10, paragrafo 9, della proposta di regolamento.
([78]) Cfr. l'articolo 5, paragrafo 10, della proposta di regolamento.
([79]) Cfr. l'articolo 7 della proposta di regolamento.
([80]) Cfr. l'articolo 19 della proposta di regolamento.
([81]) Cfr. l'articolo 3, paragrafi 7, 17 e 18, della proposta di regolamento.
([82]) Cfr. ad esempio il Quadro di riferimento.

applicazione delle disposizioni in materia di segnalazione degli incidenti di cui alla proposta di regolamento, comprese tutte le definizioni, le soglie e i parametri di segnalazione pertinenti, sia pienamente allineato ai pertinenti quadri di riferimento. In particolare, è della massima importanza garantire l'allineamento tra, da un lato, la proposta di regolamento e, dall'altro, la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio ([83]) (di seguito la «PSD2») e gli orientamenti dell'ABE sulla segnalazione degli incidenti gravi (di seguito gli «orientamenti dell'ABE»). La proposta di direttiva modificativa ([84]) contiene modifiche alla PSD2 in relazione alla delimitazione della segnalazione degli incidenti tra la proposta di regolamento e la PSD2, che interesserebbe principalmente i prestatori di servizi di pagamento, che potrebbero anche essere autorizzati come enti creditizi, nonché le autorità competenti. Vi è una mancanza di chiarezza per quanto riguarda il processo di notifica degli incidenti e vi è una potenziale sovrapposizione tra alcuni degli incidenti che devono essere segnalati a norma sia della proposta di regolamento che degli orientamenti dell'ABE.

4.2.2 Le procedure di notifica degli incidenti gravi previste, rispettivamente, dalla proposta di regolamento ([85]), dalla PSD2 e dai corrispondenti orientamenti dell'ABE imporrebbero ai prestatori di servizi di pagamento di presentare una relazione sull'incidente alla rispettiva autorità competente una volta che l'incidente è stato classificato. Di fatto, le relazioni iniziali non colgono l'essenza, la causa o l'area funzionale interessata dall'incidente e i prestatori di servizi di pagamento possono essere in grado di operare tali distinzioni solo in una fase successiva, quando saranno disponibili informazioni più dettagliate sull'incidente. Di conseguenza, le relazioni iniziali degli incidenti potrebbero essere presentate ai sensi sia della proposta di regolamento che degli orientamenti dell'ABE oppure i prestatori di servizi di pagamento potrebbero decidere per un quadro di segnalazione unico e correggere le loro comunicazioni in una data successiva. La stessa incertezza (per quanto riguarda, ad esempio, la causa alla radice di un incidente) può riflettersi anche nelle relazioni intermedie e finali. Ciò aumenterebbe ancora una volta la possibilità di presentare relazioni parallele alle autorità competenti ai sensi della proposta di regolamento e della PSD2.

4.2.3 Alcuni incidenti che possono essere classificati come incidenti connessi alle TIC possono anche avere un impatto su altri settori e, di conseguenza, dovrebbero essere notificati ai sensi degli orientamenti dell'ABE. Ciò può verificarsi quando un incidente ha un impatto dal punto di vista delle TIC ma, al tempo stesso, ha influenzato direttamente anche la prestazione di servizi di pagamento e/o altre aree o canali funzionali non connessi alle TIC. Inoltre, vi potrebbero essere casi in cui non è possibile distinguere tra incidenti operativi e incidenti connessi alle TIC. Inoltre, nel caso in cui la stessa entità finanziaria sia un ente creditizio significativo e un prestatore di servizi di pagamento, ai sensi della proposta di regolamento la stessa entità dovrebbe segnalare due volte l'incidente relativo alle TIC, essendo soggetto a due autorità competenti. Alla luce di quanto precede, la proposta di regolamento dovrebbe spiegare più chiaramente in che modo l'interazione tra la PSD2 e gli orientamenti dell'ABE dovrebbe funzionare nella pratica. Più significativamente, sarebbe importante che, ai fini dell'armonizzazione e della razionalizzazione degli obblighi di segnalazione, gli organi legislativi dell'Unione riflettessero sulle questioni residuali della doppia segnalazione e che chiarissero se la proposta di regolamento, da un lato, e la PSD2 e gli orientamenti dell'ABE, dall'altro, coesisterebbero oppure se dovrebbe esistere un'unica serie di obblighi di segnalazione degli incidenti.

4.2.4. La proposta di regolamento introduce l'obbligo per le autorità competenti ([86]), dopo aver ricevuto una relazione, di accusare ricevuta della notifica e di inviare 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. Ciò significherebbe che le autorità competenti dovrebbero contribuire attivamente alla gestione e alla riparazione degli incidenti, valutando al contempo anche la risposta agli incidenti critici di un'entità sottoposta a vigilanza. La BCE sottolinea che la responsabilità e la titolarità della riparazione e delle conseguenze di un incidente dovrebbero spettare esclusivamente e chiaramente all'entità finanziaria interessata. La BCE proporrebbe pertanto di limitare i riscontri e gli orientamenti ai soli riscontri e orientamenti prudenziali di alto livello. Riscontri più ampi richiederebbero professionisti specializzati con conoscenze tecniche molto rilevanti che normalmente non sono disponibili nel bacino di capacità a disposizione delle autorità prudenziali.

4.3 *Test di resilienza operativa digitale*

4.3.1 La BCE accoglie con favore le prescrizioni stabilite dalla proposta di regolamento ([87]) con riguardo ai test di resilienza operativa digitale nell'entità finanziarie e la necessità che ciascuna istituzione disponga di un proprio programma di test. La proposta di regolamento ([88]) descrive diversi tipi di test come indicativi per le entità finanziarie. I tipi di test non sono molto chiari e alcuni test, come i test di compatibilità, i questionari o i test basati

([83]) Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE (GU L 337 del 23.12.2015, pag. 35).

([84]) Cfr. l'articolo 7, paragrafo 9, della proposta di direttiva.

([85]) Cfr. l'articolo 17, paragrafo 3, della proposta di regolamento.

([86]) Cfr. l'articolo 20 della proposta di regolamento.

([87]) Cfr. gli articoli 21 e 22 della proposta di regolamento.

([88]) Cfr. l'articolo 22, paragrafo 1, della proposta di regolamento.

su scenari, sono soggetti a interpretazione da parte delle AEV, delle autorità competenti o delle entità finanziarie. Inoltre, non vi sono indicazioni sulla frequenza di ciascun test. Un possibile approccio potrebbe essere che la proposta di regolamento stabilisca prescrizioni generiche in materia di test, con una descrizione più precisa dei tipi di test nelle norme tecniche di regolamentazione e di attuazione.

4.3.2 I test di penetrazione basati su minacce sono uno strumento potente per testare le difese e la preparazione in materia di sicurezza. La BCE incoraggia pertanto i test di penetrazione basati su minacce da parte delle entità finanziarie. Con questo strumento vengono testate non solo le misure tecniche, ma anche il personale e i processi. I risultati di questi test possono aumentare notevolmente la consapevolezza in materia di sicurezza da parte dell'alta dirigenza all'interno delle entità sottoposte a verifica. Il quadro di riferimento European Framework for Threat Intelligence Based Ethical Red-teaming (TIBER-EU) ([89]) e altri test di penetrazione basati su minacce già disponibili al di fuori dell'Unione sono strumenti primari per le entità stesse per valutare, testare, mettere in pratica e migliorare la loro posizione di resilienza informatica e le loro difese.

4.3.3 Nella maggior parte degli Stati membri in cui è stato attuato il quadro di riferimento TIBER-EU, le autorità di sorveglianza e di vigilanza non svolgono un ruolo attivo nell'attuazione di un programma TIBER-XX localizzato e il gruppo informatico TIBER (TCT) è stabilito in quasi tutti i casi in maniera indipendente da tali funzioni. Per questo motivo, i test avanzati di cui alla proposta di regolamento ([90]), sotto forma di test di penetrazione basati su minacce, dovrebbero essere attuati come strumento per rafforzare l'ecosistema finanziario e aumentare la stabilità finanziaria piuttosto che come strumento puramente di vigilanza. Inoltre, non è necessario sviluppare un nuovo quadro di riferimento per i test avanzati di ciberresilienza, dal momento che gli Stati membri hanno già ampiamente adottato il quadro di riferimento TIBER-EU, al momento l'unico quadro nell'Unione.

4.3.4 Le prescrizioni per i tester non dovrebbero essere contenute nel corpo principale della proposta di regolamento, in quanto il settore dei test di penetrazione basati su minacce è ancora in fase di sviluppo e l'innovazione potrebbe essere ostacolata dall'imposizione di prescrizioni specifiche. Ciò detto, la BCE è del parere che, al fine di garantire un elevato grado di indipendenza nell'esecuzione dei test, le entità finanziarie non dovrebbero impiegare o appaltare tester dipendenti o assunti a contratto da entità finanziarie appartenenti al proprio gruppo o altrimenti posseduti e/o controllati dalle entità finanziarie da sottoporre a test

4.3.5 Al fine di ridurre il rischio di frammentazione e assicurare l'armonizzazione, la proposta di regolamento dovrebbe imporre un quadro per i test di penetrazione basati su minacce applicabile al settore finanziario in tutta l'Unione. La frammentazione può comportare un aumento dei costi e del fabbisogno di risorse tecniche, operative e finanziarie, sia per le autorità competenti che per le istituzioni finanziarie. Tale aumento dei costi e dei fabbisogni può in ultima analisi avere un impatto negativo sul mutuo riconoscimento dei test. Questa mancanza di armonizzazione e le conseguenti questioni relative al mutuo riconoscimento sono particolarmente critiche per le entità finanziarie, che possono essere titolari di licenze multiple e/o operare in molteplici ordinamenti nell'Unione. Le norme tecniche di regolamentazione e di attuazione, che devono essere elaborate per i test di penetrazione basati su minacce ai sensi della proposta di regolamento, dovrebbero essere conformi al quadro di riferimento TIBER-UE. Inoltre, la BCE accoglie con favore l'opportunità di essere coinvolta nella preparazione di tali norme tecniche di regolamentazione e attuazione in cooperazione con le AEV.

4.3.6 Il coinvolgimento attivo delle autorità competenti nei test potrebbe determinare un potenziale conflitto di interessi con l'altra funzione da essi svolta, vale a dire la valutazione del quadro in materia di test dell'entità finanziaria. In tale contesto, la BCE propone di eliminare dalla proposta di regolamento qualsiasi obbligo per le autorità competenti in merito alla convalida dei documenti e al rilascio di un attestato per un test di penetrazione basati su minacce.

4.4 Rischi relativi alle TIC derivanti da terzi

4.4.1 La BCE accoglie con favore l'introduzione di una serie completa di principi chiave e di un solido quadro di sorveglianza per identificare e gestire i rischi relativi alle TIC derivanti dai fornitori terzi di servizi di TIC, indipendentemente dal fatto che appartengano allo stesso gruppo di entità finanziarie. Ciò detto, al fine di ottenere un'efficace individuazione e gestione dei rischi relativi alle TIC, è importante identificare e classificare correttamente, tra l'altro, i fornitori terzi di servizi di TIC critici. A tale riguardo, sebbene l'introduzione di atti delegati ([91]) che integrino i criteri da utilizzare ai fini della classificazione ([92]) sia accolta con favore, la BCE dovrebbe essere consultata prima dell'adozione di tali atti delegati.

([89]) Disponibile sul sito della BCE all'indirizzo www.ecb.europa.eu.
([90]) Articoli 23 e 24 della proposta di regolamento.
([91]) Cfr. l'articolo 28, paragrafo 3, della proposta di regolamento.
([92]) Cfr. l'articolo 28, paragrafo 2, della proposta di regolamento.

4.4.2 Per quanto riguarda la struttura del quadro di sorveglianza ([93]), sono necessari ulteriori chiarimenti in merito al ruolo che deve svolgere il comitato congiunto. Al tempo stesso, la BCE accoglie con favore la sua inclusione nel forum di sorveglianza in qualità di osservatore, in quanto tale ruolo le fornirà lo stesso accesso alla documentazione e alle informazioni dei membri con diritto di voto ([94]). La BCE desidera richiamare l'attenzione degli organi legislativi dell'Unione sul fatto che la BCE, in qualità di osservatore, contribuirebbe ai lavori del forum di sorveglianza sia in qualità di banca centrale di emissione, responsabile della vigilanza sulle infrastrutture di mercato, sia in qualità di autorità di vigilanza prudenziale degli enti creditizi. Inoltre, la BCE rileva che, oltre ad essere un osservatore nel forum di sorveglianza, la BCE, in qualità di autorità competente, farebbe anche parte del gruppo di esaminatori congiunto. A tale riguardo, gli organi legislativi dell'Unione potrebbero riflettere ulteriormente sulla composizione dei gruppi di esaminatori congiunti ([95]) in modo da garantire un coinvolgimento adeguatamente importante delle pertinenti autorità competenti. Analogamente, la BCE ritiene che il numero massimo di partecipanti ai gruppi di esaminatori congiunti dovrebbe essere aumentato, tenendo conto della criticità, della complessità e della portata dei servizi di TIC forniti da terzi.

4.4.3 La BCE osserva che, ai sensi della proposta di regolamento, l'autorità di sorveglianza capofila può impedire ai fornitori terzi di servizi di TIC critici di concludere ulteriori contratti di subappalto nei casi in cui i) il subappaltatore designato sia un fornitore terzo di servizi di TIC o un subappaltatore di TIC stabilito in un paese terzo e ii) il subappalto riguardi una funzione critica o importante dell'entità finanziaria. La BCE desidera sottolineare che tali poteri possono essere esercitati solo dall'autorità di sorveglianza capofila nel contesto di contratti di subappalto in cui un fornitore terzo di servizi di TIC critico subappalta una funzione critica o importante a un soggetto giuridico distinto stabilito in un paese terzo. La BCE comprende che l'autorità di sorveglianza capofila non potrebbe esercitare poteri analoghi per impedire a un fornitore terzo di servizi di TIC critico di esternalizzare funzioni critiche o importanti dell'entità finanziaria a strutture di tale fornitore di servizi situate in un paese terzo. Potrebbe accadere, ad esempio, che, da un punto di vista operativo, i dati e/o le informazioni critici possano essere conservati o trattati da strutture situate al di fuori dello Spazio economico europeo (SEE). In tal caso, i poteri dell'autorità di sorveglianza capofila possono non conferire competenze adeguate alle autorità competenti per accedere a tutte le informazioni, i locali, le infrastrutture e il personale rilevanti per lo svolgimento di tutte le funzioni critiche o importanti dell'entità finanziaria. Al fine di garantire che la capacità delle autorità competenti di svolgere i propri compiti senza ostacoli sia conservata, la BCE suggerisce di conferire all'autorità di sorveglianza capofila il potere di limitare anche l'uso, da parte di fornitori terzi di servizi di TIC critici, di strutture situate al di fuori del SEE. Tale potere potrebbe essere esercitato nei casi specifici in cui non sono in vigore accordi amministrativi con le autorità del paese terzo interessato come previsto dalla proposta di regolamento ([96]), o i rappresentanti dei fornitori di servizi TIC essenziali non forniscono sufficienti rassicurazioni, nel quadro del paese terzo interessato, in merito all'accesso alle informazioni, ai locali, alle infrastrutture e al personale necessari per svolgere compiti di vigilanza o di vigilanza.

4.4.4 Infine, imporre alle autorità competenti di dare seguito alle raccomandazioni dell'autorità di sorveglianza capofila ([97]) potrebbe rischiare di rivelarsi inefficace, in quanto le autorità competenti potrebbero non avere una visione olistica dei rischi generati da ciascun fornitore terzo di servizi di TIC critico. Inoltre, le autorità competenti possono essere tenute ad adottare misure nei confronti delle loro entità finanziarie sottoposte a vigilanza qualora le raccomandazioni non siano prese in considerazione dai fornitori terzi di servizi critici. Ai sensi della proposta di regolamento ([98]), le autorità competenti possono chiedere alle entità finanziarie sottoposte alla loro vigilanza di sospendere temporaneamente il servizio critico prestato dal fornitore terzo o di risolvere i contratti in essere con fornitori terzi di servizi critici. È difficile tradurre il previsto processo di follow-up in azioni concrete. In particolare, non è chiaro se un'entità finanziaria sottoposta a vigilanza sarà in grado di sospendere o risolvere un contratto con un fornitore terzo di servizi critico. Ciò è dovuto al fatto che il fornitore terzo di servizi di TIC critico potrebbe essere un fornitore significativo per tale entità finanziaria, o ai costi e ai danni, contrattuali o di altro tipo, che l'entità finanziaria potrebbe subire a seguito di tale sospensione o risoluzione. Inoltre, tale approccio non favorisce la convergenza della vigilanza, in quanto le autorità competenti possono interpretare la stessa raccomandazione in modo divergente. Ciò potrebbe, in ultima analisi, ostacolare la prevista armonizzazione e l'approccio coerente nel monitoraggio dei rischi critici relativi alle TIC derivanti da terzi a livello dell'Unione. Alla luce di quanto precede, gli organi legislativi dell'Unione possono valutare la possibilità di concedere alle autorità di vigilanza poteri di esecuzione specifici nei confronti dei fornitori terzi di servizi di TIC critici, tenendo conto dei limiti imposti dalla dottrina *Meroni*, parzialmente mitigati dalla Corte di giustizia nella sua sentenza nella causa ESMA ([99]).

([93]) Cfr. l'articolo 29 della proposta di regolamento.
([94]) Cfr. l'articolo 29, paragrafo 3, della proposta di regolamento.
([95]) Cfr. l'articolo 35 della proposta di regolamento.
([96]) Cfr. l'articolo 39, paragrafo 1, della proposta di regolamento.
([97]) V. l'articolo 29, paragrafo 4, e l'articolo 37 della proposta di regolamento.
([98]) Cfr. l'articolo 37, paragrafo 3, della proposta di regolamento.
([99]) Cfr. sentenza della Corte del 22 gennaio 2014, Regno Unito / Parlamento e Consiglio (causa C-270/12, EU:C:2014:18).

Quando la BCE raccomanda di modificare la proposta di regolamento, indica in un separato documento di lavoro tecnico specifiche proposte redazionali, accompagnate da note esplicative. Il documento di lavoro tecnico è disponibile in lingua inglese sul sito Internet EUR-Lex.

Fatto a Francoforte sul Meno, il 4 giugno 2021.

La Presidente della BCE
Christine LAGARDE