PARERE DELLA BANCA CENTRALE EUROPEA

dell'11 aprile 2022

su una 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

(CON/2022/14)

(2022/C 233/03)

Introduzione e base giuridica

In data 16 dicembre 2020, la Commissione europea ha adottato una 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 ([1]) (di seguito la «proposta di direttiva»). Il 3 dicembre 2021 il Consiglio dell'Unione europea ha approvato il suo orientamento generale sulla proposta di direttiva ([2]). La Banca centrale europea (BCE) è competente a formulare un parere in virtù dell'articolo 127, paragrafo 4, secondo comma, del trattato sul funzionamento dell'Unione europea, in quanto la proposta di direttiva contiene disposizioni che rientrano nella sua sfera di competenza, in particolare la promozione del regolare funzionamento dei sistemi di pagamento, il contributo alla buona conduzione delle politiche perseguite dalle competenti autorità per quanto riguarda la stabilità del sistema finanziario e i compiti della BCE relativi alla vigilanza prudenziale degli enti creditizi ai sensi dell'articolo 127, paragrafo 2, 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.

Osservazioni di carattere generale

La BCE sostiene fermamente gli obiettivi della proposta di direttiva di aumentare il livello di resilienza informatica (ciberresilienza) in tutti i settori pertinenti, ridurre le disomogeneità nel mercato interno e migliorare il livello di consapevolezza situazionale e la capacità collettiva di preparazione e risposta, garantendo una cooperazione efficiente nell'Unione.

La BCE riconosce l'importanza di mantenere forti legami tra la proposta di direttiva e il settore finanziario, che dovrebbe continuare a far parte dell'ecosistema delle reti e dei sistemi informativi (NIS) per promuovere la valutazione coerente dei rischi associati alle tecnologie dell'informazione e della comunicazione (TIC) nell'Unione, l'effettivo scambio di informazioni intersettoriale e la collaborazione nella gestione delle minacce informatiche. A tal fine, le autorità competenti ai sensi della proposta di regolamento del Parlamento europeo e del Consiglio relativo alla resilienza operativa digitale per il settore finanziario ([3]) (di seguito, la «proposta di regolamento DORA») dovrebbero poter partecipare alle discussioni strategiche delle politiche e ai lavori tecnici del gruppo di cooperazione NIS, nonché scambiare informazioni e cooperare ulteriormente con i punti di contatto unici e con i team nazionali di risposta agli incidenti di sicurezza informatica di cui alla proposta di direttiva ([4]).

1. Ambito di applicazione della proposta di direttiva

1.1 La BCE evince che, per quanto riguarda i soggetti del settore finanziario, la proposta di regolamento DORA sarà considerata una normativa settoriale che introduce obblighi di gestione dei rischi di cibersicurezza e di segnalazione degli incidenti i cui effetti siano almeno equivalenti a quelli degli obblighi di cui alla proposta di direttiva ([5]). Pertanto, le disposizioni della proposta di direttiva riguardanti la gestione dei rischi di cibersicurezza, gli obblighi di segnalazione, la condivisione delle informazioni, la vigilanza e l'esecuzione non si applicano ai soggetti finanziari contemplati nella proposta di regolamento DORA ([6]). Come chiarito nei considerando della proposta di direttiva,

([1]) COM (2020) 823 final.
([2]) Disponibile sul sito internet del Consiglio all'indirizzo www.consilium.europa.eu
([3]) COM(2020) 595 final.
([4]) Cfr. paragrafo 1.5 del Parere CON/2021/20 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 (GU C 343 del 26.8.2021, pag. 1). Tutti i pareri della BCE sono pubblicati su EUR-Lex. Articoli 17, paragrafo 5, e 42 della proposta di regolamento DORA; articolo 11 della proposta di direttiva.
([5]) Articolo 2, paragrafo 6, della proposta di direttiva.
([6]) Considerando 13 e articolo 2, paragrafo 6, della proposta di direttiva.

invece delle disposizioni stabilite dalla proposta di direttiva dovrebbero applicarsi quelle della proposta di regolamento DORA relative alle misure di gestione dei rischi relativi alle TIC, alla gestione degli incidenti connessi alle TIC e alla segnalazione degli incidenti, nonché alle prove di resilienza operativa digitale, agli accordi di condivisione delle informazioni e al rischio di terze parti relativo alle TIC ([7]).

1.2 La BCE rileva inoltre che il Consiglio, nel proprio orientamento generale sulla proposta di direttiva, propone una modifica volta a escludere dall'applicazione della proposta di direttiva i «soggetti che svolgono attività nel settore giudiziario, dei parlamenti o delle banche centrali» ([8]). La BCE è consapevole del fatto che la modifica proposta si estenderebbe a tutti i compiti e competenze fondamentali del Sistema europeo di banche centrali (SEBC), come stabilito all'articolo 127, paragrafo 2, del trattato e all'articolo 3, paragrafo 1 dello Statuto del Sistema europeo di banche centrali e della Banca centrale europea (di seguito lo «Statuto del SEBC»), quali la promozione del regolare funzionamento dei sistemi di pagamento. A tale riguardo, si ritiene che le infrastrutture dei mercati finanziari possedute e gestite dall'Eurosistema, come TARGET2 e TARGET2-Securities, rientrino nell'esclusione delle banche centrali dall'ambito di applicazione della proposta di direttiva, proposta dal Consiglio.

2. **Competenze di sorveglianza del SEBC e dell'Eurosistema**

2.1 Unitamente all'obiettivo primario del SEBC di mantenere la stabilità dei prezzi e in conformità all'articolo 127, paragrafo 2, del trattato, uno dei compiti fondamentali da assolvere attraverso il SEBC è quello di promuovere il regolare funzionamento dei sistemi di pagamento ([9]). 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 ([10]). Nell'esercizio del suo ruolo di sorveglianza, la BCE ha adottato il regolamento della Banca centrale europea (UE) n. 795/2014 (BCE/2014/28) ([11]) (di seguito, il «regolamento SPIS»), che traduce i Principi CPSS-IOSCO per le infrastrutture dei mercati finanziari ([12]) in una legge direttamente applicabile. Il regolamento SPIS stabilisce requisiti sia per i sistemi di pagamento di importo rilevante che per quelli al dettaglio di importanza sistemica, siano essi di proprietà pubblica o privata. I requisiti previsti dal regolamento SPIS comprendono già, tra l'altro, la gestione del rischio operativo e l'istituzione di un quadro per la ciberresilienza ([13]).

2.2 Oltre ai sistemi di pagamento di importanza sistemica, la sorveglianza dell'Eurosistema riguarda i sistemi di pagamento non di importanza sistemica, gli strumenti di pagamento elettronico, gli schemi e le disposizioni, nonché altre infrastrutture e fornitori di servizi critici, come stabilito nel quadro di riferimento della politica di sorveglianza dell'Eurosistema ([14]). I sistemi di pagamento e gli altri dispositivi oggetto della sorveglianza dell'Eurosistema non sono espressamente inclusi nell'ambito di applicazione della proposta di direttiva ([15]). Allo stesso tempo, dal momento che la proposta di direttiva è uno strumento di armonizzazione minima ([16]), la normativa di attuazione adottata dagli Stati membri potrebbe poi sovrapporsi alla competenza dell'Eurosistema in materia di sorveglianza. Per evitare che ciò accada, le competenze del SEBC ai sensi del trattato e dello Statuto del SEBC, nonché le competenze dell'Eurosistema ai sensi del regolamento SPIS e, in generale, del quadro di riferimento della politica di sorveglianza dell'Eurosistema, dovrebbero essere espressamente riconosciute nei considerando della proposta di direttiva.

([7]) Considerando 13 della proposta di direttiva.
([8]) Articolo 2, paragrafo 3 bis, primo comma, lettera b), dell'orientamento generale del Consiglio sulla proposta di direttiva.
([9]) Articolo 127, paragrafo 2, del trattato e articolo 3.1 dello Statuto del SEBC.
([10]) Articolo 22 dello Statuto del SEBC.
([11]) Regolamento della Banca centrale europea (UE) n. 795/2014, del 3 luglio 2014, sui requisiti di sorveglianza per i sistemi di pagamento di importanza sistemica (BCE/2014/28) (GU L 217 del 23.7.2014, pag. 16).
([12]) Cfr. Comitato sui sistemi di pagamento e di regolamento (Committee of Payment and Settlement Systems, CPSS) e Comitato tecnico dell'Organizzazione internazionale delle commissioni sui titoli (International Organisation of Securities Commissions, IOSCO) disponibili sul sito Internet della Banca per i regolamenti internazionali all'indirizzo www.bis.org. La responsabilità D stabilisce che «tutti i membri del CPSS e della IOSCO sono tenuti ad applicare i principi alle pertinenti FMI nelle rispettive giurisdizioni nella misura massima consentita dal quadro giuridico della loro giurisdizione».
([13]) Articolo 15 del regolamento (UE) n. 795/2014 (BCE/2014/28).
([14]) Eurosystem oversight policy framework, versione rivista (luglio 2016), disponibile sul sito Internet della BCE all'indirizzo www.ecb.europa.eu.
([15]) Articolo 2 della proposta di direttiva e allegati I e II della proposta di direttiva.
([16]) Articolo 3 della proposta di direttiva.

3. **Rischio di terze parti relativo alle TIC, gestione delle crisi e degli incidenti su vasta scala, condivisione delle informazioni e strategia nazionale per la cibersicurezza**

3.1 *Gestione del rischio di terze parti relativo alle TIC*

3.1.1 La proposta di direttiva conferisce alle autorità competenti, nell'esercizio dei rispettivi poteri di esecuzione nei confronti dei soggetti essenziali, il potere di emanare istruzioni vincolanti o un'ingiunzione che impongano a tali soggetti di porre rimedio alle carenze individuate o alle violazioni degli obblighi stabiliti dalla proposta di direttiva ([17]). Al contempo, l'«Autorità di sorveglianza capofila» designata ai sensi della proposta di regolamento DORA, può impartire raccomandazioni ai fornitori terzi di servizi di TIC critici per gestire i potenziali rischi sistemici derivanti dalla diffusione delle pratiche di esternalizzazione e dalla concentrazione dei servizi di TIC forniti da terzi ([18]).

3.1.2 Considerato che un soggetto essenziale ai sensi della proposta di direttiva può essere altresì designato come fornitore terzo di servizi di TIC critici ai sensi della proposta di regolamento DORA, la BCE ribadisce ([19]) che occorre evitare la formulazione di raccomandazioni contrastanti e istruzioni vincolanti. A tale riguardo, la BCE accoglie favorevolmente l'orientamento generale del Consiglio sulla proposta di direttiva. Secondo tale orientamento le autorità competenti devono informare il «forum di sorveglianza», istituito dalla proposta di regolamento DORA, quando esercitano i propri poteri di vigilanza ed esecuzione con riferimento a un soggetto essenziale designato come fornitore terzo di servizi di TIC critici ai sensi della proposta di regolamento DORA ([20]).

3.2 *Gestione delle crisi e degli incidenti su vasta scala*

3.2.1 Ai sensi della proposta di direttiva ([21]), gli Stati membri designano una o più autorità competenti responsabili della gestione delle crisi e degli incidenti su vasta scala. Come chiarito dai considerando della proposta di direttiva, per incidente su vasta scala si dovrebbe intendere un incidente che ha un impatto significativo su almeno due Stati membri o che causa perturbazioni che superano la capacità di risposta di uno Stato membro. Gli incidenti su vasta scala possono trasformarsi in vere e proprie crisi che pregiudicano il corretto funzionamento del mercato interno ([22]).

3.2.2 Mentre le autorità competenti, designate ai sensi della proposta di regolamento DORA, rimangono responsabili della gestione degli incidenti di cibersicurezza che riguardano le entità finanziarie, la cooperazione con le strutture e le autorità istituite a norma della proposta di direttiva è di fondamentale importanza per assicurare una risposta coordinata in tutta l'Unione. A tal fine, la BCE accoglierebbe favorevolmente la partecipazione delle autorità competenti designate ai sensi della proposta di regolamento DORA, inclusa la BCE, nella Rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) ([23]), laddove gli incidenti di cibersicurezza su vasta scala incidano sul settore finanziario.

3.3 *Condivisione delle informazioni*

3.3.1 Come già indicato, la BCE sostiene con forza la cooperazione tra le autorità competenti designate ai sensi della proposta di regolamento DORA e le strutture e le autorità istituite ai sensi della proposta di direttiva. In particolare, la condivisione delle informazioni tra le autorità può consentire l'apprendimento intersettoriale, contribuire a prevenire e a gestire in modo efficace gli attacchi informatici e promuovere una valutazione coerente dei rischi connessi alle TIC in tutta l'Unione. Cionondimeno, la BCE sottolinea che lo scambio di informazioni dovrebbe avvenire in presenza di meccanismi di classificazione e condivisione delle informazioni chiaramente definiti, accompagnati da adeguate garanzie per assicurare la riservatezza ([24]). La BCE accoglie favorevolmente

([17]) Articolo 29, paragrafo 4, lettera b) della proposta di direttiva.
([18]) Articolo 31 della proposta di regolamento DORA.
([19]) Cfr. paragrafo 1.2 del parere CON/2021/20.
([20]) Articolo 29, paragrafo 10 dell'orientamento generale del Consiglio sulla proposta di direttiva.
([21]) Articolo 7, paragrafo 1 della proposta di direttiva.
([22]) Considerando 27 della proposta di direttiva.
([23]) Articolo 14 della proposta di direttiva.
([24]) Cfr. paragrafo 1.5 del parere CON/2021/20.

l'orientamento generale del Consiglio sulla proposta di direttiva, che propone lo scambio regolare di informazioni pertinenti tra le autorità ([25]), l'introduzione di accordi di cooperazione che specifichino un meccanismo per lo scambio di informazioni ([26]), e la trasmissione automatica e diretta delle segnalazioni di incidenti ([27]). A tale riguardo si dovrebbe assicurare che le informazioni riservate di cui alle disposizioni sul segreto professionale ai sensi della proposta di regolamento DORA ([28]) o della pertinente normativa settoriale ([29]) possano essere scambiate con le autorità competenti di cui alla proposta di direttiva solo nella misura in cui tale scambio sia necessario affinché le autorità competenti applichino le disposizioni della proposta di direttiva ([30]).

3.4 *Strategia nazionale per la cibersicurezza*

3.4.1 Ai sensi della proposta di direttiva, gli Stati membri adottano una strategia nazionale per la cibersicurezza che definisce obiettivi strategici e adeguate misure strategiche e normative al fine di raggiungere e mantenere un livello elevato di cibersicurezza ([31]). Come chiarito nei considerando della proposta di direttiva, gli Stati membri dovrebbero inoltre continuare a includere il settore finanziario nelle rispettive strategie di cibersicurezza ([32]). Indicativamente, nell'ambito delle loro strategie nazionali per la cibersicurezza, gli Stati membri dovrebbero adottare misure relative alla cibersicurezza nella catena di approvvigionamento dei prodotti e dei servizi delle TIC utilizzati da soggetti per la fornitura dei loro servizi. Per quanto riguarda il settore finanziario, le strategie nazionali per la cibersicurezza dovrebbero essere coerenti con il quadro normativo derivante dalla proposta di regolamento DORA. A tal riguardo, la BCE ritiene che siano necessari ulteriori chiarimenti per garantire che le strategie nazionali per la cibersicurezza siano coerenti con la normativa settoriale.

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, l'11 aprile 2022

La presidente della BCE
Christine LAGARDE

([25]) Articolo 11, paragrafo 5 dell'orientamento generale del Consiglio sulla proposta di direttiva.
([26]) Considerando 23bis dell'orientamento generale del Consiglio sulla proposta di direttiva.
([27]) Considerando 13 dell'orientamento generale del Consiglio sulla proposta di direttiva
([28]) Articolo 49 della proposta di regolamento DORA.
([29]) Articoli da 53 a 62 della 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, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE (GU L 176, 27.6.2013, pag. 338).
([30]) Articoli 2, paragrafo 5 e 11, paragrafo 4, della proposta di direttiva.
([31]) Articolo 5 della proposta di direttiva.
([32]) Considerando 13 della proposta di direttiva.