RELAZIONE ILLUSTRATIVA

1. Premessa

L'articolo 16 della legge 21 febbraio 2024, n. 15, recante «Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea», di seguito «legge di delegazione europea 2022-2023», dispone la «Delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/2554, 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, (UE) n. 909/2014 E (UE) 2016/1011, e per il recepimento della direttiva (UE) 2022/2556, che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario, di seguito, «regolamento DORA» e «direttiva DORA».

Il regolamento DORA, pubblicato il 22 dicembre 2022 nella *Gazzetta Ufficiale* dell'Unione europea, è stato approvato contestualmente alla direttiva europea volta a modificare la normativa settoriale già vigente in materia. Gli atti normativi in oggetto fanno 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 e si inserisce in un lavoro più ampio per rafforzare la *cybersecurity* nei servizi finanziari.

DORA, infatti, è finalizzato a realizzare un quadro normativo armonizzato e rafforzato da applicare, garantendo la proporzionalità, pressoché a tutto il settore finanziario, nonché ai fornitori critici di servizi relativi alle Tecnologie dell'Informazione e della Comunicazione (TIC).

Il regolamento DORA, inoltre, costituisce *lex specialis* rispetto alla direttiva (UE) 2022/2555 (cd. direttiva NIS 2) relativa a misure per un livello comune elevato di cybersicurezza nell'Unione.

In particolare, il regolamento DORA 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, alle istituzioni finanziarie che rientrano nell'ambito di applicazione del regolamento;

- obblighi di segnalazione di incidenti rilevanti connessi alle TIC secondo criteri, modelli e meccanismi uniformi e semplificati;

- test di resilienza operativa digitale 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 alle entità finanziarie, tramite la previsione di requisiti di gestione dei rischi da parte delle entità finanziarie e di un quadro di sorveglianza diretta dei fornitori terzi critici di servizi TIC;

- condivisione delle informazioni tra le Autorità competenti.

Il regolamento DORA sarà applicabile dal 17 gennaio 2025, così come la correlata direttiva.

Al fine di disporre delle necessarie misure di adeguamento dell'ordinamento italiano al regolamento DORA, nonché di recepire la direttiva DORA, il decreto legislativo in esame dà attuazione alle disposizioni non direttamente applicabili contenute in DORA, prevedendo al contempo i necessari interventi di adeguamento della normativa nazionale vigente, in osservanza dei principi e criteri direttivi contenuti nella delega di cui alla legge di delegazione europea 2022-2023.

Il decreto legislativo presentato su proposta del Ministro per gli affari europei, il Sud, le politiche di coesione e il PNRR e del Ministro dell'economia e delle finanze è composto da 14 articoli, così di seguito suddivisi:

- Capo I: «Disposizioni generali»;
- Capo II: «Autorità competenti e cooperazione»;
- Capo III: «Disposizioni applicabili a intermediari finanziari e Bancoposta»;
- Capo IV: «Poteri di vigilanza e sanzioni»;
- Capo V: «Modificazioni e integrazioni della normativa di settore e disposizioni di coordinamento»;
- Capo VI: «Disposizioni finali».

2. Disposizioni recate dal decreto legislativo

Il Capo I contiene le «Disposizioni generali» e si compone di due articoli.

Nel dettaglio, l'**articolo 1,** relativo alle definizioni, rinvia alle definizioni contenute negli articoli 2, paragrafo 2, e 3 del regolamento (UE) 2022/2554, nel testo unico delle leggi in materia bancaria e creditizia di cui al decreto legislativo 1° settembre 1993, n. 385 (TUB), nel testo unico delle disposizioni in materia di intermediazione finanziaria di cui al decreto legislativo 24 febbraio 1998, n. 58 (TUF), nel Codice delle assicurazioni private di cui al decreto legislativo 7 settembre 2005, n. 209 (CAP) e nel decreto legislativo 5 dicembre 2005, n. 252, recante «Disciplina delle forme pensionistiche complementari».

L'**articolo 2** definisce, al **comma 1**, l'oggetto e l'ambito di applicazione del decreto legislativo, specificando che lo stesso detta le disposizioni necessarie all'adeguamento del quadro normativo nazionale al regolamento DORA e al recepimento della direttiva DORA, nonché a garantire il coordinamento con le disposizioni settoriali vigenti. In linea con il criterio di delega recato all'articolo 16, comma 2, lettera *c-bis*), della legge di delegazione europea 2022-2023, come modificata dall'articolo 15 della legge 28 giugno 2024, n. 90, il **comma 2** chiarisce che all'interno del decreto sono individuate anche le disposizioni applicabili, in quanto compatibili, agli intermediari finanziari iscritti nell'albo previsto dall'articolo 106 del TUB, di seguito «intermediari finanziari», nonché alla società Poste italiane S.p.a. per l'attività del Patrimonio Bancoposta, di cui al regolamento di cui al decreto del Presidente della Repubblica 14 marzo 2001, n. 144, di seguito «Bancoposta». Il **comma 3** chiarisce, invece, l'interazione tra la disciplina recata dal presente decreto e quella contenuta nel decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, in materia di perimetro di sicurezza nazionale cibernetica; a questo proposito, in coerenza con quanto previsto dall'articolo 1, paragrafo 3, del regolamento DORA, si prevede che: "[r]esta fermo quanto stabilito dal decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, in materia di perimetro di sicurezza nazionale

cibernetica, nei confronti dei soggetti di cui all'articolo 1, comma 2-bis, del medesimo decreto-legge n. 105 del 2019".

Il **Capo II** prevede disposizioni relative alle «Autorità competenti e cooperazione» e si compone di tre articoli.

L'**articolo 3**, **comma 1**, richiama l'articolo 46 del regolamento DORA, ai sensi del quale la Banca d'Italia, la Consob, l'IVASS e la COVIP sono le Autorità competenti per il rispetto degli obblighi posti dal medesimo regolamento a carico dei soggetti vigilati dalle medesime Autorità, secondo le rispettive attribuzioni di vigilanza. Il **comma 2** esplicita che, in linea con l'articolo 46, paragrafo 1, lettera *a*) del regolamento DORA e il quadro normativo nazionale di riferimento, la Banca d'Italia è l'Autorità competente per il rispetto degli obblighi posti dal regolamento DORA a carico di Cassa depositi e prestiti S.p.A.

Il **comma 3** del medesimo articolo stabilisce, in linea con quanto previsto dal criterio di delega recato dall'articolo 16, comma 2, lettera *c-bis*), della legge di delegazione europea 2022-2023, che la Banca d'Italia è l'Autorità competente per il rispetto degli obblighi posti dal decreto in esame a carico degli intermediari finanziari e di Bancoposta.

Per quanto riguarda la partecipazione al forum di sorveglianza di cui all'articolo 32 del regolamento DORA, il **comma 4** individua la Banca d'Italia quale Autorità competente interessata il cui membro del personale è il rappresentante di alto livello del forum, la Consob quale Autorità competente che partecipa in qualità di osservatore su base permanente con un proprio rappresentante e – tenuto conto della possibilità che le riunioni del forum riguardino profili di competenza di più Autorità competenti DORA – prevede, altresì, la possibilità che, a seconda della tematica trattata, anche l'IVASS e la COVIP partecipino al forum in qualità di osservatori con un proprio rappresentante.

Il **comma 5** precisa che le modalità di partecipazione e lo scambio di informazioni relative al forum di sorveglianza potranno essere disciplinate attraverso i protocolli di intesa di cui all'articolo 5, comma 1, del decreto.

L'**articolo 4** detta disposizioni relative alla ricezione delle segnalazioni dei gravi incidenti TIC e delle notifiche volontarie delle minacce informatiche significative.

L'articolo 19, paragrafo 1, del regolamento DORA, stabilisce che le entità finanziarie debbano segnalare i gravi incidenti TIC all'autorità competente interessata di cui all'articolo 46, prevedendo ulteriormente che, nel caso in cui un'entità finanziaria sia soggetta alla vigilanza di più di un'autorità nazionale competente DORA ai sensi dell'articolo 46 del regolamento DORA, gli Stati membri debbano designare un'unica autorità competente quale responsabile dell'espletamento delle funzioni e dei compiti previsti dall'articolo 19 del regolamento. Coerentemente con tale previsione, la competenza a ricevere le segnalazioni dei gravi incidenti TIC e le notifiche volontarie relative alle minacce significative è attribuita:

- al **comma 1, lettera *a*)**, alla Banca d'Italia, con riferimento agli enti creditizi, agli istituti di pagamento, compresi gli istituti di pagamento esentati a norma della direttiva (UE) 2015/2366, ai prestatori di servizi di informazione sui conti, agli istituti di moneta elettronica, compresi gli istituti di moneta elettronica esentati a norma della direttiva 2009/110/CE, alle imprese di

investimento, ai fornitori di servizi per le cripto-attività autorizzati a norma del regolamento (UE) 1114/2023 (MiCAR) ed agli emittenti di token collegati ad attività, alle controparti centrali, ai gestori di fondi di investimento alternativi, alle società di gestione, ai fornitori di servizi di *crowdfunding*, nonché da parte di sedi di negoziazione all'ingrosso di titoli di Stato, a Cassa depositi e prestiti S.p.A., agli intermediari finanziari e a Bancoposta;

- al **comma 1, lettera *b*)**, alla Consob con riferimento a depositari centrali e sedi di negoziazione, ad esclusione di quelle all'ingrosso di titoli di Stato;
- al **comma 1, lettera *c*)**, all'IVASS con riferimento alle imprese di assicurazione e di riassicurazione e agli intermediari assicurativi, agli intermediari riassicurativi e agli intermediari assicurativi a titolo accessorio;
- al **comma 1, lettera *d*)**, alla COVIP con riferimento agli enti pensionistici aziendali o professionali.

Il **comma 2** prevede, invece, che nel caso in cui le entità finanziarie siano vigilate da più Autorità competenti DORA, l'Autorità ricevente, individuata ai sensi del comma 1, trasmetta tempestivamente alle altre Autorità competenti DORA la notifica iniziale e ciascuna relazione di cui all'articolo 19, paragrafo 4, del regolamento DORA relative ai gravi incidenti TIC, nonché le notifiche volontarie relative alle minacce informatiche significative, secondo le modalità definite nei protocolli di intesa. Ciò in modo da evitare la duplicazione di oneri informativi a carico delle entità finanziarie sottoposte alla vigilanza di più Autorità competenti DORA, secondo quanto previsto dal citato articolo 19, paragrafo 1, del regolamento DORA.

Il **comma 3** dispone, inoltre, che gli enti creditizi e le infrastrutture di mercato di cui all'allegato I della direttiva (UE) 2022/2555 (NIS2), nonché i soggetti appartenenti al settore bancario e delle infrastrutture dei mercati finanziari identificati come critici ai sensi della direttiva (UE) 2022/2557 (CER), forniscono anche al CSIRT Italia la notifica iniziale dei gravi incidenti TIC e ciascuna relazione successiva, secondo i modelli e i termini previsti ai sensi della disciplina di cui al regolamento DORA, in linea con quanto contemplato dall'articolo 19, paragrafo 1, comma 6, del regolamento DORA.

In base al **comma 4** del decreto in esame, in caso di notifica su base volontaria delle minacce informatiche significative, le entità finanziarie possono trasmettere la notifica anche a CSIRT Italia, in linea con quanto previsto dall'articolo 19, paragrafo 2, comma 3, del regolamento DORA. Le informazioni trasmesse a CSIRT Italia in tema di segnalazioni di incidenti gravi e di notifica volontaria delle minacce sono coperte da segreto d'ufficio.

Tenuto conto del ruolo del Ministero dell'economia e delle finanze nei confronti dei mercati regolamentati all'ingrosso di titoli di Stato, il **comma 5** stabilisce che la Banca d'Italia trasmetta al citato Ministero la notifica iniziale, le relazioni relative ai gravi incidenti TIC e le notifiche volontarie relative alle minacce informatiche significative contestualmente alla trasmissione alla Consob ai sensi del comma 2.

L'**articolo 5** disciplina le modalità di cooperazione tra le Autorità interessate dal presente decreto. In particolare, il **comma 1** prevede che le Autorità competenti DORA individuino forme di coordinamento operativo e informativo tramite uno o più protocolli d'intesa. All'interno di tali protocolli sono definite, tra le altre, forme di condivisione tempestiva e completa delle informazioni

sui gravi incidenti TIC che riguardano entità finanziarie che rientrano nell'alveo della vigilanza da parte di più autorità (è il caso, ad esempio, degli enti creditizi che prestano servizi di investimento).

In attuazione di quanto previsto dall'articolo 47 del regolamento DORA, il **comma 2** prevede la conclusione di specifici protocolli di intesa tra le Autorità competenti DORA e l'Agenzia per la cybersicurezza nazionale; con le medesime finalità di cooperazione e coordinamento delle rispettive attività di vigilanza. Prevede, infine, la stipula di un protocollo d'intesa tra le Autorità competenti DORA con il Corpo della Guardia di finanza per la disciplina dello scambio di informazioni relative alle segnalazioni di gravi incidenti TIC e alla notifica volontaria delle minacce informatiche significativa, per finalità di prevenzione, accertamento e repressione degli illeciti di natura economico finanziaria.

Tra l'altro, la disposizione è volta a prevedere mirate forme di raccordo informativo tra le autorità competenti DORA e la Guardia di finanza. Tale intervento:

- è strettamente legato al fatto che gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici attinenti al settore finanziario possano derivare da attacchi esterni compiuti da soggetti non interessati solo a «*testare*» la vulnerabilità dei livelli di sicurezza degli stessi, ma anche ad acquisire la disponibilità di dati ed elementi informativi di carattere strategico, in grado di minare gli interessi economico-finanziari del Paese e suscettibili di essere sfruttati per fini illeciti, *in primis*, nel settore dei mercati finanziari e mobiliari (si considerino, a titolo esemplificativo, le fattispecie di *insider trading* di operazioni di società che gestiscono *assets* strategici del Paese), nonché in quello fiscale, doganale, della spesa pubblica e in materia di valuta, titoli, valori e mezzi di pagamento;
- garantisce il coinvolgimento della Guardia di finanza, quale istituzione cui è normativamente riconosciuta la competenza per la ricerca, la prevenzione e il contrasto degli illeciti economico finanziari perpetrati sfruttando i mezzi tecnologici e informatici.

  Si fa riferimento, in particolare:

  - ✓ all'art. 2 del d.lgs. n. 68 del 2001, che demanda al Corpo i compiti di prevenzione, ricerca e repressione delle violazioni in materia, tra l'altro, di:

    (i) imposte dirette e indirette, tasse, contributi, monopoli fiscali e ogni altro tributo, di tipo erariale o locale;

    (ii) diritti doganali, di confine e altre risorse proprie nonché uscite del bilancio dell'Unione europea e ogni altra entrata tributaria, anche a carattere sanzionatorio o di diversa natura, di spettanza erariale o locale;

    (iii) risorse e mezzi finanziari pubblici impiegati a fronte di uscite del bilancio pubblico nonché di programmi pubblici di spesa, nonché entrate ed uscite relative alle gestioni separate nel comparto della previdenza, assistenza e altre forme obbligatorie di sicurezza sociale pubblica;

    (iv) valute, titoli, valori e mezzi di pagamento nazionali, europei ed esteri, nonché movimentazioni finanziarie e di capitali;

    (v) mercati finanziari e mobiliari, ivi compreso l'esercizio del credito e la sollecitazione del pubblico risparmio;

(vi) diritti d'autore, know-how, brevetti, marchi ed altri diritti di privativa industriale, relativamente al loro esercizio e sfruttamento economico e ogni altro interesse economico-finanziario nazionale o dell'Unione europea;

- ✓ alla direttiva sui comparti di specialità delle forze di polizia e sulla razionalizzazione dei presidi di polizia di cui al decreto del Ministro dell'interno 15 agosto 2017, discendente dal d.lgs. n. 177 del 2016, che:

  (i) al paragrafo 1.4 («Sicurezza postale e delle comunicazioni»), attribuisce alla Guardia di finanza, «tenuto conto delle attribuzioni di polizia tributaria, economico-finanziaria, valutaria e amministrativa conferite dall'art. 2 del decreto legislativo 19 marzo 2001, n. 68, dalle normative specifiche di settore e dall'art. 2 del decreto legislativo 19 agosto 2016, n. 177», la competenza per «per la ricerca, la prevenzione e il contrasto degli illeciti perpetrati sfruttando i mezzi tecnologici e informatici nei settori dell'evasione fiscale, degli illeciti doganali e in materia di accise, delle frodi nell'impiego di risorse pubbliche nazionali e comunitarie, degli illeciti che interessano i mercati finanziari e mobiliari, in materia di valuta, titoli, valori e mezzi di pagamento, ivi comprese le condotte di contraffazione, nonché di contraffazione di marchi, brevetti, indicazioni di origine e qualità e del diritto d'autore, (anche) attraverso il Nucleo Speciale Frodi Tecnologiche»;

  (ii) al paragrafo 1.7 («Sicurezza nella circolazione dell'euro e degli altri mezzi di pagamento»), riconosce che la Guardia di finanza:

  - è responsabile «nel settore della tutela dei mezzi di pagamento, essendo ad essa demandati, per effetto dell'assetto ordinamentale intervenuto con il d.lgs. n. 68/2001 e delle disposizioni contemplate dal decreto legge 25 settembre 2001, n. 350, convertito in legge 23 novembre 2001, n. 409, e dal decreto legislativo 21 novembre 2007, n. 231, compiti di prevenzione e contrasto delle violazioni in materia di valuta, titoli, valori, mezzi di pagamento nazionali, europei ed esteri, movimentazioni finanziarie e di capitali»;
  - «è parte integrante dell'UCAMP - Unità deputata all'analisi dell'impatto del fenomeno della falsificazione monetaria e degli altri mezzi di pagamento sul sistema economico e finanziario ed allo sviluppo di forme di prevenzione in via amministrativa - e partecipa al sistema di coordinamento interforze per gli aspetti di prevenzione e contrasto delle frodi sui mezzi di pagamento»;
  - in relazione a tali prerogative, «vede valorizzata, per effetto del d.lgs. n. 68/2001 e del d.lgs. 177/2016, la sua funzione di prevenzione e contrasto al riciclaggio, alla falsificazione della moneta, alle frodi concernenti i mezzi e i sistemi di pagamento diversi dal contante, nonché all'usura nell'ipotesi di coinvolgimento diretto di intermediari finanziari e bancari».

La disposizione non amplia il novero dei settori in cui si troverebbe a operare la Guardia di finanza, ma ha lo scopo di fornire alla medesima dei preziosi «*input*» informativi idonei a rendere più efficace ed efficiente il proprio dispositivo di contrasto al crimine economico-finanziario; inoltre è pienamente coerente con l'articolo 19, paragrafo 6, lettera e) del Regolamento DORA, laddove si prevede che «*i dettagli del grave incidente TIC*» siano condivisi da parte delle Autorità competenti DORA con le «*altre pertinenti autorità pubbliche ai sensi del diritto nazionale*», in cui è ricompresa, per i motivi innanzi esposti, anche la Guardia di finanza.

Il **comma 3** prevede che le informazioni su minacce, vulnerabilità e incidenti informatici, acquisite dall'ACN ai sensi del decreto legislativo in esame (notifiche degli operatori di cui all'articolo 4 e altre informazioni pertinenti ricevute da ACN da parte delle Autorità competenti DORA sulla base delle intese di cui al comma 2 dell'articolo 5), siano trasmesse agli organismi di informazione per la sicurezza di cui alla legge n. 124 del 2007 per le loro finalità istituzionali, sulla base di intesa tra l'ACN e gli stessi organismi di *intelligence.*

Tale disposizione si pone in linea e a completamento di analoghe previsioni inserite in altri ambiti normativi di recepimento e adeguamento rispetto alla legislazione europea in materia di sicurezza informatica e delle infrastrutture - decreti legislativi n. 134 del 2024 e n. 138 del 2024, di recepimento, rispettivamente, della direttiva CER (articoli 5, comma 11, 8, comma 7 e 16, comma 7) e della direttiva NIS2 (articolo 17, comma 5) - volte a prevedere l'acquisizione da parte degli organismi di *intelligence* di informazioni ricevute da ACN da parte dei soggetti tenuti agli obblighi informativi CER e NIS2.

La trasmissione delle informazioni agli OO.I.S. risulta anche coerente con il sistema del regolamento DORA, atteso che lo stesso prevede, in particolare (articolo 19, paragrafo 6, lettera *e*), la trasmissione di informazioni di interesse in materia di incidenti informatici, oltre che alle autorità specificamente indicate, *ex multis*, ad altre pertinenti autorità pubbliche ai sensi del diritto nazionale.

Il **comma 4** dispone che, qualora l'Agenzia per la cybersicurezza nazionale, in sede di vigilanza o di esecuzione, venga a conoscenza di una violazione degli obblighi di segnalazione di cui al decreto in esame da parte di un'entità finanziaria, ne informi senza indebito ritardo le Autorità competenti DORA (circostanza che può verificarsi, ad esempio, nel caso di incidenti che coinvolgono fornitori terzi critici ai sensi del regolamento DORA che siano stati identificati come soggetti essenziali o importanti ai sensi della direttiva NIS2).

In linea con quanto previsto dall'articolo 16, comma 2, lettera *c-bis*), della legge di delegazione europea 2022-2023, come modificata dall'articolo 15 della legge 28 giugno 2024, n. 90, il **Capo III** contiene le «Disposizioni del regolamento DORA applicabili a intermediari finanziari e Bancoposta» ed è costituito da due articoli.

L'**articolo 6** detta le disposizioni applicabili agli intermediari finanziari. Per ragioni di proporzionalità, richiamando le disposizioni del regolamento DORA rilevanti, il **comma 1** dispone che gli intermediari finanziari siano soggetti all'ICT *risk management framework* «semplificato» previsto dall'articolo 16 del regolamento DORA per le entità finanziarie di minori dimensioni o complessità.

Il **comma 2** dispone che per gli intermediari finanziari che si qualificano come «microimprese» ai sensi dell'articolo 3, paragrafo 1, punto 60), del regolamento DORA (in quanto occupino meno di 10 dipendenti e realizzino un fatturato annuo e/o totale di bilancio annuo non superiore a 2 milioni di euro) non si applica l'articolo 24 in materia di requisiti generali per lo svolgimento dei test di resilienza operativa digitale, in quanto a tali soggetti si applica la disciplina *ad hoc* prevista dal successivo articolo 25, paragrafo 3, del regolamento DORA.

Il **comma 3** rinvia alla potestà regolamentare della Banca d'Italia l'eventuale individuazione di una categoria di intermediari finanziari da considerarsi «significativi» (anche per tipologia di attività svolte), a cui applicare l'ICT *risk management framework* completo, in luogo di quello semplificato.

L'**articolo 7** individua le disposizioni applicabili a Bancoposta, prevedendo che sia soggetto alla stessa disciplina applicabile alle banche (ossia l'ICT *risk management framework* completo, la disciplina sulla segnalazione degli incidenti TIC e quella relativa ai test di resilienza operativa digitale).

Il **Capo IV** disciplina «Poteri di vigilanza e sanzioni» ed è composto da tre articoli. Al fine di garantire il corretto esercizio dei compiti previsti dal regolamento DORA, dagli atti delegati e dalle norme tecniche di regolamentazione e di attuazione di tale regolamento, nonché dal decreto in esame e dalle relative disposizioni attuative, le Autorità competenti DORA devono essere dotate dei poteri necessari per vigilare, indagare e imporre sanzioni.

L'**articolo 8, comma 1,** attribuisce alle Autorità competenti DORA poteri di vigilanza nei confronti delle entità soggette all'applicazione della relativa disciplina e nei confronti dei fornitori terzi di servizi TIC a supporto di funzioni essenziali o importanti di tali entità, secondo le rispettive competenze, richiamando i poteri indicati dall'articolo 50, paragrafo 2 (poteri minimi: ad esempio, l'accesso a qualsiasi documento o dato pertinente per l'esecuzione dei propri compiti; effettuare ispezioni e indagini) , e dall'articolo 42, paragrafo 6 (ad esempio, imporre all'entità finanziaria la sospensione temporanea dell'utilizzo o dell'introduzione di un servizio prestato da un fornitore terzo critico di servizi TIC), del regolamento DORA, nonché quelli attribuiti dalla normativa di settore.

Il **comma 2** specifica che, ai fini dell'esercizio dei poteri di cui al comma 1, le Autorità competenti DORA possono effettuare accessi e ispezioni presso i fornitori terzi di servizi TIC a supporto di funzioni essenziali o importanti delle entità soggette all'applicazione della relativa disciplina, nonché convocare gli amministratori, i sindaci e il personale dei medesimi fornitori e richiedere loro di fornire informazioni e di esibire documenti. Specifica, inoltre, che restano impregiudicati i poteri di cui le predette Autorità, dispongono già in forza di talune disposizioni della legislazione bancaria, finanziaria e assicurativa, nonché dell'articolo 22 della legge n. 262 del 2005.

In linea con i criteri contenuti nella legge di delegazione europea 2022-2023, l'**articolo 9** dispone che le Autorità competenti DORA possono, nell'ambito delle rispettive competenze, emanare disposizioni attuative del decreto in esame e del regolamento DORA, anche al fine di tenere conto degli orientamenti delle Autorità europee di vigilanza, nonché delle disposizioni riguardanti le modalità di esercizio dei poteri di vigilanza.

L'**articolo 10** disciplina le sanzioni da applicare in caso di inosservanza di specifiche disposizioni del regolamento DORA e delle relative norme tecniche di regolamentazione e attuazione, ovvero in caso di omessa collaborazione o mancato seguito dato nell'ambito di un'indagine, di un'ispezione o di una richiesta ai sensi dell'articolo 8. Ciò, nel rispetto dei limiti edittali e delle procedure previste dalle disposizioni nazionali che disciplinano l'irrogazione delle sanzioni da parte delle diverse Autorità competenti DORA, così come previsto dai criteri della legge di delegazione europea 2022-2023. In particolare, apporta modifiche alla disciplina nazionale di settore (decreto legislativo 1° settembre 1993, n. 395; decreto legislativo 24 febbraio 1998, n. 58; decreto legislativo 9 settembre 2005, n. 209; decreto legislativo 5 dicembre 2005, n. 252; decreto legislativo 5 settembre 2024, n. 129) introducendo delle sanzioni amministrative pecuniarie graduate in due fasce di gravità a seconda del tipo di obbligo violato previsto dal regolamento (UE) 2022/2554.

Il **comma 1** Modifica il testo unico bancario e, in particolare, l'articolo 144 relativo alle sanzioni comminabili alle persone giuridiche (banche, intermediari finanziari, istituti di pagamento, istituti di moneta elettronica e i rispettivi fornitori di TIC). Tra queste, è incluso Bancoposta in virtù del richiamo all'articolo 144 del TUB recato dall'articolo 2, comma 3, del d.P.R. n. 144 del 2001, relativo alle norme sui servizi Bancoposta. Inoltre, l'articolo 144-*ter* disciplina le sanzioni applicabili alle persone fisiche in ordine alle violazioni disciplinate all'articolo 144 del TUB.

Il **comma 2** modifica il testo unico delle disposizioni in materia di intermediazione finanziaria ai sensi degli articoli 8 e 2 della legge 6 febbraio 1996, n. 52 di cui al decreto legislativo 24 febbraio 1998, n. 58 introducendo il nuovo articolo 190-*bis*.3 recante «Sanzioni amministrative relative alle violazioni delle disposizioni previste dal regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022 e dalle relative norme tecniche di regolamentazione e attuazione» che prevede l'applicazione di sanzioni sia nei confronti delle persone giuridiche, sia nei confronti delle persone fisiche graduate sulla base di due fasce di gravità.

Il **comma 3** modica il codice delle assicurazioni private e, in particolare:

- l'articolo 310 prevedendo sanzioni amministrative pecuniarie, articolate in due fasce di gravità a seconda dell'obbligo violato, nei confronti delle imprese di assicurazione, delle imprese di riassicurazione e dei relativi fornitori terzi di servizi TIC di cui all'articolo 3, punto 19), del regolamento (UE) 2022/2554;
- l'articolo 311-*sexies* relativo al regime sanzionatorio applicabile alle persone fisiche;
- l'articolo 324 concernente le sanzioni applicabili a intermediari assicurativi, a intermediari riassicurativi, a intermediari assicurativi a titolo accessorio e ai relativi fornitori terzi di servizi TIC di cui all'articolo 3, punto 19), del regolamento (UE) 2022/2554 e alle persone fisiche che in essi operano.

Il **comma 4** modifica l'articolo 19-*quater* del decreto legislativo n. 252 del 2005 prevedendo sanzioni amministrative pecuniarie nei confronti dei componenti degli organi di amministrazione e di controllo, dei direttori generali, dei titolari delle funzioni fondamentali, dei responsabili delle forme pensionistiche complementari, dei liquidatori e dei commissari straordinari nominati per lo scioglimento del fondo, , che, in relazione alle rispettive competenze, non osservino le disposizioni del regolamento DORA e le relative norme tecniche di regolamentazione e attuazione ovvero omettano di collaborare o di dare seguito nell'ambito di un'indagine, di un'ispezione o di una richiesta ai sensi dell'articolo 8 del presente decreto.

Il **comma 5** introduce il nuovo articolo 37-*bis* al decreto legislativo n. 129 del 2004 recante «Sanzioni amministrative relative alle violazioni delle disposizioni previste dal regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022 e dalle relative norme tecniche di regolamentazione e attuazione» che prevede l'applicazione di sanzioni sia nei confronti dei prestatori di servizi in cripto-attività, degli emittenti di *token* collegati ad attività e dei rispettivi fornitori terzi di servizi TIC di cui all'articolo 3, punto 19), del citato regolamento (UE) 2022/2554 siano essi persone giuridiche o persone fisiche. Tali sanzioni vengono graduate sulla base di due fasce di gravità.

Il **comma 6** stabilisce che, laddove le violazioni di al presente articolo siano connotate da scarsa offensività o pericolosità, possa essere disposta l'applicazione di misure di riparazione previste

dall'articolo 50, paragrafo 4, lettere *a*) ed *e*), del regolamento DORA (ovverosia l'ordine di porre termine alla violazione e la dichiarazione pubblica) in luogo dell'irrogazione delle sanzioni amministrative pecuniarie.

Inoltre, il **comma 7** attribuisce alle Autorità competenti DORA il potere di richiedere la cessazione temporanea o permanente di qualsiasi pratica o comportamento che considerino contrari alle disposizioni del regolamento stesso e prevenirne la reiterazione.

Il **comma 8** rinvia ai criteri indicati dall'articolo 51, paragrafo 2, del regolamento DORA, per la definizione dell'importo e della tipologia di sanzioni amministrative o misure di riparazione da applicare. In particolare, nell'esercizio del potere sanzionatorio le Autorità competenti DORA tengono conto, tra l'altro:

a) della rilevanza, della gravità e della durata della violazione;

b) del grado di responsabilità della persona fisica o giuridica responsabile della violazione;

c) della solidità finanziaria della persona fisica o giuridica responsabile;

d) dell'importanza degli utili realizzati o delle perdite evitate da parte della persona fisica o giuridica responsabile, nella misura in cui possano essere determinati;

e) delle perdite subite da terzi a causa della violazione, nella misura in cui possano essere determinate;

f) del livello di cooperazione che la persona fisica o giuridica responsabile ha dimostrato nei confronti dell'autorità competente, ferma restando la necessità di garantire la restituzione degli utili realizzati o delle perdite evitate da tale persona fisica o giuridica;

g) delle precedenti violazioni commesse dalla persona fisica o giuridica responsabile.

Il **comma 9** dispone che i provvedimenti di applicazione delle sanzioni, dopo la comunicazione al destinatario, vengano pubblicati senza ritardo e per estratto nel sito internet dell'Autorità competente DORA che lo ha adottato, secondo quanto previsto dall'articolo 54 del regolamento DORA.

Il **Capo V** contiene le «Ulteriori modificazioni e integrazioni della normativa di settore e disposizioni di coordinamento» e si compone di cinque articoli, che recepiscono (articoli da 11 a 14) le modifiche apportate dalla direttiva DORA alle direttive 2014/65/UE, 2009/138/CE, (UE) (UE) 2016/2341 e 2014/59/UE e introducono (articolo 15) alcune disposizioni di coordinamento con il decreto legislativo 4 settembre 2024, n. 138, recante il recepimento della direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione.

Nello specifico, gli **articoli da 11 a 14** dispongono le necessarie modifiche alla disciplina contenuta rispettivamente nel testo unico delle disposizioni in materia di intermediazione finanziaria di cui al decreto legislativo 24 febbraio 1998, n. 58 (articolo 11), nel Codice delle assicurazioni private di cui al decreto legislativo 9 settembre 2005, n. 209 (articolo 12), nel decreto legislativo 5 dicembre 2005, n. 252, recante «Disciplina delle forme pensionistiche complementari» (articolo 13) e nel decreto legislativo 16 novembre 2015, n. 180, che reca disposizioni di attuazione della direttiva 2014/59/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, che istituisce un quadro di risanamento e risoluzione degli enti creditizi e delle imprese di investimento (articolo 14).

Per quanto riguarda gli interventi della direttiva DORA sulle direttive 2009/65/CE, 2011/61/UE, 2013/36/UE e 2015/2366/UE, le relative modifiche saranno effettuate con normativa secondaria della

Banca d'Italia recante le disposizioni di attuazione delle citate direttive, in coerenza con l'impianto adottato dall'ordinamento interno in sede di recepimento di tali atti europei e in linea con i criteri contenuti nella Legge di delegazione europea 2022-2023.

L'**articolo 15** chiarisce che, in attuazione della scelta contenuta nei criteri di delega – che assoggettano Bancoposta a disposizioni della disciplina unionale equivalenti a quelle previste dal decreto di recepimento della direttiva NIS2 – tale entità finanziaria viene esentata dall'applicazione delle disposizioni del decreto di recepimento corrispondenti nel caso in cui sia identificato come soggetto essenziale o importante dei settori 3 o 4 di cui all'allegato I del decreto di recepimento della direttiva NIS2.

Infine, il **Capo VI** contiene «Disposizioni finali», contenute in due articoli.

L'**articolo 16** dispone che dal decreto in esame non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e che le amministrazioni competenti e le istituzioni pubbliche coinvolte provvedono all'attuazione delle disposizioni di cui al decreto con le risorse umane, strumentali e finanziarie previste a legislazione vigente (clausola d'invarianza).

L'**articolo 17** disciplina l'entrata in vigore, fissandola al 17 gennaio 2025, ossia dalla data di applicazione del regolamento DORA, fissata dall'articolo 64 del medesimo regolamento.

Si dispone, tuttavia, un'applicazione differita al 1° gennaio 2027 per quanto riguarda la disciplina relativa alla resilienza operativa digitale applicabile agli intermediari finanziari (contenuta nell'articolo 6, commi 1 e 2, del decreto), per accordare ad essi un congruo periodo per adattarsi alle nuove disposizioni.

TABELLA DI CONCORDANZA AI SENSI DELL'ART. 31, COMMA 2, DELLA L. 234/2012

Norme nazionali di adeguamento/attuazione		Regolamento (UE) n. 2022/2554	Direttiva (UE) 2022/2556	Legge di delegazione europea 2022-2023[1]
Schema di decreto	**Diverso atto normativo**			
Art. 1 (Definizioni)		Art. 3		criterio di delega di cui all'articolo 16, comma 2, lett. a)
Art. 2 (Oggetto e ambito di applicazione)		Art. 1 Art. 2		criterio di delega di cui all'articolo 16, comma 2, lett. a)
Art. 3 (Autorità competenti DORA e partecipazione al forum di sorveglianza)		Art. 46 Art. 32		criterio di delega di cui all'articolo 16, comma 2, lett. b)
Art. 4 (Segnalazione dei gravi incidenti TIC e notifica volontaria delle minacce informatiche significative)		Art. 19		criterio di delega di cui all'articolo 16, comma 2, lett. a) e b)
Art. 5 (Protocolli d'intesa e scambio di informazioni)		Art. 48 Art. 47		criterio di delega di cui all'articolo 16, comma 2, lett. a)
Art. 6 (Disposizioni applicabili agli intermediari finanziari)		-		criterio di delega di cui all'articolo 16, comma 2, lett. c-bis)
Art. 7 (Disposizioni applicabili a Bancoposta)		-		criterio di delega di cui all'articolo 16, comma 2, lett. c-bis)
Art. 8 (Poteri di vigilanza e di indagine)		Art. 42, par. 6 Art. 50 Art. 51		criterio di delega di cui all'articolo 16, comma 2, lett. b) e c)
Art. 9 (Poteri regolamentari)		-		criteri di delega di cui all'articolo 16, comma 2, lett. d)

[1] Legge del 21/02/2024 n. 15 recante delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea -

Art. 10 (Sanzioni amministrative e altre misure)		Art. 50 Art. 51 Art. 54		criterio di delega di cui all'articolo 16, comma 2, lett. b) e c)
Art. 11 (Modifiche al decreto legislativo 24 febbraio 1998, n. 58)			Art. 6 (Modifiche della direttiva 2014/65/UE)	criterio di delega di cui all'articolo 16, comma 2, lett. a)
Art. 12 (Modifiche al decreto legislativo 9 settembre 2005, n. 209)			Art. 2 (Modifiche della direttiva 2009/138/CE)	criterio di delega di cui all'articolo 16, comma 2, lett. a)
Art. 13 (Modifiche al decreto legislativo 5 dicembre 2005, n. 252)			Art. 8 (Modifica della direttiva (UE) 2016/2341)	criterio di delega di cui all'articolo 16, comma 2, lett. a)
Art. 14 (Modifiche al decreto legislativo 16 novembre 2015, n. 180)			Art. 5 (Modifiche della direttiva 2014/59/UE)	criterio di delega di cui all'articolo 16, comma 2, lett. a)
Art. 15 (Disposizioni di coordinamento con il decreto legislativo [recante attuazione della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione])		Art. 1(2)		criterio di delega di cui all'articolo 16, comma 2, lett. a) e c-bis)
Art. 16 (Clausola di invarianza finanziaria)		-		articolo 16, comma 3
Art. 17 (Entrata in vigore)		Art. 64	Art. 9 (Recepimento)	criterio di delega di cui all'articolo 16, comma 2, lett. a) e c-bis)
	Art. 6 (Poteri regolamentari) D.lgs. n. 58/98		Art. 1 (Modifica della direttiva 2009/65/CE)	criterio di delega di cui all'articolo 16, comma 2, lett. a) e d)
	Art. 6 (Poteri regolamentari) D.lgs. n. 58/98		Art. 3 (Modifica della direttiva 2011/61/UE)	criterio di delega di cui all'articolo 16, comma 2, lett. a) e d)

	Art. 53 (Vigilanza regolamentare) D.lgs. 385/1993		Art. 4 (Modifiche della direttiva 2013/36/UE)	criterio di delega di cui all'articolo 16, comma 2, lett. a) e d)
	Art. 114-quaterdecies (Vigilanza) D.lgs. 385/1993		Art. 7 (Modifiche della direttiva (UE) 2015/2366)	criterio di delega di cui all'articolo 16, comma 2, lett. a) e d)

RELAZIONE TECNICA

1. Premessa

Il decreto in esame contiene disposizioni tese all'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/2554, 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, (UE) n. 909/2014 E (UE) 2016/1011, e al recepimento della direttiva (UE) 2022/2556, che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario, di seguito «regolamento DORA» e «direttiva DORA».

Il regolamento DORA, pubblicato nella Gazzetta Ufficiale dell'Unione europea il 27 dicembre 2022, fa parte del *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 ed è finalizzato a realizzare un quadro normativo armonizzato e rafforzato da applicare, garantendo la proporzionalità, pressoché a tutto il settore finanziario, nonché ai fornitori critici di servizi relativi alle Tecnologie dell'Informazione e della Comunicazione (TIC).

DORA si concentra su cinque blocchi normativi:

- 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, alle istituzioni finanziarie che rientrano nell'ambito di applicazione del regolamento;
- obblighi di segnalazione di incidenti rilevanti connessi alle TIC secondo criteri, modelli e meccanismi uniformi e semplificati;
- test di resilienza operativa digitale al fine di aggiornare e di rivedere regolarmente i sistemi e gli strumenti di risposta agli attacchi informatici o alle interruzioni TIC e di garantire, in tal modo, la resilienza operativa;
- gestione dei rischi derivanti da terze parti fornitrici di servizi TIC alle entità finanziarie, tramite la previsione di requisiti di gestione dei rischi da parte delle entità finanziarie e di un quadro di sorveglianza diretta dei fornitori terzi critici di servizi TIC;
- condivisione delle informazioni tra le entità finanziarie.

Il decreto in esame, pertanto, introduce le modifiche necessarie ad adeguare l'ordinamento nazionale alle disposizioni del regolamento DORA, nonché a dare attuazione alla correlata direttiva in osservanza ai principi e ai criteri direttivi contenuti nella delega di cui all'articolo 16 della legge di delegazione europea 2022-2023.

1. Sintesi dell'articolato e degli eventuali impatti sugli equilibri di finanza pubblica

Conformemente a quanto previsto dall'articolo 16, comma 3, della legge di delegazione europea 2022-2023, le previsioni normative di cui al presente decreto, avendo carattere esclusivamente ordinamentale, non comportano nuovi o maggiori oneri per la finanzia pubblica. Si riporta una sintesi delle disposizioni del decreto in commento, con l'indicazione dell'assenza di riflessi sulla finanza pubblica.

Il **Capo I** contiene le «Disposizioni generali». L'**articolo 1** è relativo alle definizioni, mentre l'**articolo 2** definisce l'oggetto del decreto specificando che lo stesso detta le disposizioni necessarie

all'adeguamento del quadro normativo nazionale al regolamento DORA e al recepimento della direttiva DORA, nonché a garantire il coordinamento con le disposizioni settoriali vigenti. Tutte le disposizioni del Capo I hanno carattere ordinamentale e, comunque, non comportano nuovi o maggiori oneri per la finanza pubblica.

Il **Capo II** prevede disposizioni relative alle «Autorità competenti e cooperazione» e si compone di tre articoli.

L'**articolo 3** richiama il regolamento DORA, ai sensi del quale la Banca d'Italia, la Consob, l'IVASS e la COVIP sono le Autorità competenti per il rispetto degli obblighi posti dal medesimo regolamento a carico dei soggetti vigilati dalle medesime autorità, secondo le rispettive attribuzioni di vigilanza. (le «Autorità competenti DORA»).In linea con la vigente ripartizione di competenze in materia di vigilanza, il medesimo articolo stabilisce la competenza di Banca d'Italia anche nei confronti di Cassa Depositi e Prestiti S.p.A., di Bancoposta e degli intermediari finanziari di cui all'articolo 106 del testo unico delle leggi in materia bancaria e creditizia di cui al decreto legislativo 1° settembre 1993, n. 385 (TUB). Infine, disciplina le modalità di partecipazione delle Autorità competenti DORA al forum di sorveglianza di cui all'articolo 32 del regolamento DORA.

L'**articolo 4** detta disposizioni relative alle segnalazioni dei gravi incidenti TIC e alle notifiche volontarie delle minacce informatiche significative. In particolare, il **comma 1** individua, per ogni tipologia di entità finanziaria soggetta al regolamento DORA nonché per Bancoposta e per gli intermediari finanziari, l'Autorità competente DORA destinataria delle segnalazioni e delle notifiche. il **comma 2** prevede che, nel caso in cui le entità finanziarie siano vigilate da più Autorità competenti DORA, l'autorità ricevente di cui al comma 1 trasmette tempestivamente alle altre autorità competenti la notifica iniziale e ciascuna relazione, relative ai gravi incidenti TIC, secondo le modalità definite nei protocolli di intesa. Il **comma 3** dispone, inoltre, che le segnalazioni dei gravi incidenti TIC siano fornite da alcune entità finanziarie anche al CSIRT Italia, secondo i modelli e i termini previsti ai sensi della disciplina attuativa del regolamento DORA. Il **comma 4** disciplina la notifica su base volontaria delle minacce informatiche significative, che possono essere trasmesse anche a CSIRT Italia. Il **comma 5** dispone che, nel caso delle sedi di negoziazione all'ingrosso dei titoli di Stato, la Banca d'Italia svolga le attività di informativa richiamate al comma 2 anche nei confronti del Ministero dell'economia e delle finanze.

L'**articolo 5** disciplina la cooperazione tra Autorità competenti DORA e le strutture e le autorità competenti istituite a norma della Direttiva NIS 2, e, in particolare, con l'Agenzia per la cybersicurezza nazionale, attraverso forme di coordinamento operativo e informativo regolate da uno o più protocolli d'intesa. Qualora l'Agenzia per la cybersicurezza nazionale, in sede di vigilanza o di esecuzione, venga a conoscenza di una violazione degli obblighi di segnalazione di cui al decreto in esame da parte di un'entità finanziaria, ne informa senza indebito ritardo le Autorità competenti DORA. Prevede, infine, la stipula di un protocollo d'intesa tra le Autorità competenti DORA con il Corpo della Guardia di finanza per la disciplina dello scambio di informazioni relative alle segnalazioni di gravi incidenti TIC e alla notifica volontaria delle minacce informatiche significativa, per finalità di prevenzione, accertamento e repressione degli illeciti di natura economico finanziaria.

Per quanto concerne le disposizioni di cui al Capo II, si evidenzia che la Banca d'Italia ha, ai sensi degli articoli 131 e 282 del TFUE, un bilancio autonomo e gode della più ampia indipendenza finanziaria e che la Consob, la Covip e l'Ivass provvedono autonomamente, con forme di autofinanziamento basate sulle contribuzioni dovute dai soggetti vigilati, alla copertura dei costi

derivanti dalle attività svolte. Pertanto, le Autorità sopra indicate provvedono all'attuazione dei compiti di cui al Capo II del decreto con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente, e comunque senza nuovi o maggiori oneri a carico della finanza pubblica. Con riferimento all'Agenzia per la cybersicurezza nazionale, le attività disciplinate nel presente Capo sono svolte nell'ambito delle funzioni istituzionali dell'Agenzia con risorse umane, strumentali e finanziarie disponibili a legislazione vigente e non determinano nuovi oneri per la finanza pubblica.

Prevede, inoltre, la condivisione di informazioni sulla sicurezza informatica, sulla base di intesa tra l'ACN e gli organismi di cui agli articoli 4, 6 e 7 della legge n. 124 del 2007. Da tale disposizione, atteso il carattere ordinamentale, non derivano nuovi o maggiori oneri a carico della finanza pubblica.

Infine, la disposizione prevede mirate forme di raccordo informativo tra le autorità competenti DORA e la Guardia di finanza. Tale intervento:

- è strettamente legato al fatto che gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici attinenti al settore finanziario possano derivare da attacchi esterni compiuti da soggetti non interessati solo a «*testare*» la vulnerabilità dei livelli di sicurezza degli stessi, ma anche ad acquisire la disponibilità di dati ed elementi informativi di carattere strategico, in grado di minare gli interessi economico-finanziari del Paese e suscettibili di essere sfruttati per fini illeciti, *in primis*, nel settore dei mercati finanziari e mobiliari (si considerino, a titolo esemplificativo, le fattispecie di *insider trading* di operazioni di società che gestiscono *assets* strategici del Paese), nonché in quello fiscale, doganale, della spesa pubblica e in materia di valuta, titoli, valori e mezzi di pagamento;
- garantisce il coinvolgimento della Guardia di finanza, quale istituzione cui è normativamente riconosciuta la competenza per la ricerca, la prevenzione e il contrasto degli illeciti economico finanziari perpetrati sfruttando i mezzi tecnologici e informatici.

  Si fa riferimento, in particolare:

  - ✓ all'art. 2 del d.lgs. n. 68 del 2001, che demanda al Corpo i compiti di prevenzione, ricerca e repressione delle violazioni in materia, tra l'altro, di:

    (i) imposte dirette e indirette, tasse, contributi, monopoli fiscali e ogni altro tributo, di tipo erariale o locale;

    (ii) diritti doganali, di confine e altre risorse proprie nonché uscite del bilancio dell'Unione europea e ogni altra entrata tributaria, anche a carattere sanzionatorio o di diversa natura, di spettanza erariale o locale;

    (iii) risorse e mezzi finanziari pubblici impiegati a fronte di uscite del bilancio pubblico nonché di programmi pubblici di spesa, nonché entrate ed uscite relative alle gestioni separate nel comparto della previdenza, assistenza e altre forme obbligatorie di sicurezza sociale pubblica;

    (iv) valute, titoli, valori e mezzi di pagamento nazionali, europei ed esteri, nonché movimentazioni finanziarie e di capitali;

    (v) mercati finanziari e mobiliari, ivi compreso l'esercizio del credito e la sollecitazione del pubblico risparmio;

    (vi) diritti d'autore, know-how, brevetti, marchi ed altri diritti di privativa industriale, relativamente al loro esercizio e sfruttamento economico e ogni altro interesse economico-finanziario nazionale o dell'Unione europea;

- ✓ alla direttiva sui comparti di specialità delle forze di polizia e sulla razionalizzazione dei presidi di polizia di cui al decreto del Ministro dell'interno 15 agosto 2017, discendente dal d.lgs. n. 177 del 2016, che:

  (i) al paragrafo 1.4 («Sicurezza postale e delle comunicazioni»), attribuisce alla Guardia di finanza, «tenuto conto delle attribuzioni di polizia tributaria, economico-finanziaria, valutaria e amministrativa conferite dall'art. 2 del decreto legislativo 19 marzo 2001, n. 68, dalle normative specifiche di settore e dall'art. 2 del decreto legislativo 19 agosto 2016, n. 177», la competenza per «per la ricerca, la prevenzione e il contrasto degli illeciti perpetrati sfruttando i mezzi tecnologici e informatici nei settori dell'evasione fiscale, degli illeciti doganali e in materia di accise, delle frodi nell'impiego di risorse pubbliche nazionali e comunitarie, degli illeciti che interessano i mercati finanziari e mobiliari, in materia di valuta, titoli, valori e mezzi di pagamento, ivi comprese le condotte di contraffazione, nonché di contraffazione di marchi, brevetti, indicazioni di origine e qualità e del diritto d'autore, (anche) attraverso il Nucleo Speciale Frodi Tecnologiche»;

  (ii) al paragrafo 1.7 («Sicurezza nella circolazione dell'euro e degli altri mezzi di pagamento»), riconosce che la Guardia di finanza:

  - è responsabile «nel settore della tutela dei mezzi di pagamento, essendo ad essa demandati, per effetto dell'assetto ordinamentale intervenuto con il d.lgs. n. 68/2001 e delle disposizioni contemplate dal decreto legge 25 settembre 2001, n. 350, convertito in legge 23 novembre 2001, n. 409, e dal decreto legislativo 21 novembre 2007, n. 231, compiti di prevenzione e contrasto delle violazioni in materia di valuta, titoli, valori, mezzi di pagamento nazionali, europei ed esteri, movimentazioni finanziarie e di capitali»;
  - «è parte integrante dell'UCAMP - Unità deputata all'analisi dell'impatto del fenomeno della falsificazione monetaria e degli altri mezzi di pagamento sul sistema economico e finanziario ed allo sviluppo di forme di prevenzione in via amministrativa - e partecipa al sistema di coordinamento interforze per gli aspetti di prevenzione e contrasto delle frodi sui mezzi di pagamento»;
  - in relazione a tali prerogative, «vede valorizzata, per effetto del d.lgs. n. 68/2001 e del d.lgs. 177/2016, la sua funzione di prevenzione e contrasto al riciclaggio, alla falsificazione della moneta, alle frodi concernenti i mezzi e i sistemi di pagamento diversi dal contante, nonché all'usura nell'ipotesi di coinvolgimento diretto di intermediari finanziari e bancari».

La disposizione non amplia il novero dei settori in cui si troverebbe a operare la Guardia di finanza, ma ha lo scopo di fornire alla medesima dei preziosi «*input*» informativi idonei a rendere più efficace ed efficiente il proprio dispositivo di contrasto al crimine economico-finanziario; inoltre è pienamente coerente con l'articolo 19, paragrafo 6, lettera e) del Regolamento DORA, laddove si prevede che «*i dettagli del grave incidente TIC*» siano condivisi da parte delle Autorità competenti DORA con le «*altre pertinenti autorità pubbliche ai sensi del diritto nazionale*», in cui è ricompresa, per i motivi innanzi esposti, anche la Guardia di finanza.

Il coinvolgimento della Guardia di finanza non comporta nuovi o maggiori oneri finanziari tenuto conto che la stessa svolgerà gli approfondimenti connessi a tali incidenti nell'ambito della propria ordinaria attività d'istituto, utilizzando le segnalazioni ricevute al fine di meglio orientare le

tipiche attività di polizia economico-finanziaria che le sono già demandate verso le fenomenologie di frode - che interessano lo specifico comparto - maggiormente rilevanti e articolate. Inoltre, non incide in alcun modo sulle prerogative e lo svolgimento delle funzioni attribuite ad altre Amministrazioni competenti in materia di «*cybersicurezza*», ponendosi, anzi, a indispensabile completamento del dispositivo di contrasto degli illeciti sottesi agli incidenti TIC nel settore finanziario, sotto il profilo – rientrante, come detto, nella diretta competenza della Guardia di finanza - della prevenzione e repressione dei fenomeni criminosi di matrice economico-finanziaria.

In linea con quanto previsto all'articolo 16, comma 2, lettera *c-bis*), della legge di delegazione europea 2022-2023, come modificata dall'articolo 15 della legge 28 giugno 2024, n. 90, il **Capo III** contiene le «Disposizioni del regolamento DORA applicabili a intermediari finanziari e Bancoposta» ed è costituito da due articoli.

In particolare, **gli articoli 6 e 7** chiariscono quali disposizioni del regolamento DORA si applichino, a seconda della complessità del soggetto e del livello di rischio ICT dell'attività svolta, a queste due categorie di intermediari (intermediari finanziari e Bancoposta). In linea con il principio di proporzionalità richiamato nei criteri di delega, l'articolo 6, comma 3, rimette alla potestà regolamentare della Banca d'Italia l'eventuale individuazione di una categoria di intermediari finanziari da considerarsi «significativi» (anche per tipologia di attività svolte), a cui applicare l'ICT *risk management framework* completo, in luogo di quello semplificato.

La Banca d'Italia ha, ai sensi degli articoli 131 e 282 del TFUE, un bilancio autonomo e gode della più ampia indipendenza finanziaria. Pertanto, Banca d'Italia provvede all'attuazione dei compiti di vigilanza disciplinati dal Capo III con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri a carico della finanza pubblica.

Il **Capo IV** si occupa dei «Poteri di vigilanza e sanzioni» e si compone di tre articoli, con l'obiettivo di dotare le Autorità competenti DORA di tutti i poteri necessari per garantire il corretto esercizio dei compiti previsti dal regolamento DORA, dagli atti delegati e dalle norme tecniche di regolamentazione e di attuazione di tale regolamento, nonché dal decreto in esame e dalle relative disposizioni attuative.

L'**articolo 8** definisce, al comma 1, i poteri di vigilanza e di indagine delle Autorità competenti DORA nei confronti delle entità finanziarie e dei fornitori terzi di servizi TIC a supporto di funzioni essenziali o importanti; il comma 2 specifica che, ai fini dell'esercizio di tali poteri, le Autorità competenti DORA possono effettuare accessi e ispezioni presso i fornitori terzi di servizi TIC a supporto di funzioni essenziali o importanti delle entità finanziarie, nonché convocare gli amministratori, i sindaci e il personale dei medesimi fornitori e richiedere loro di fornire informazioni e di esibire documenti.

L'**articolo 9** dispone che le Autorità competenti DORA possano, nell'ambito delle rispettive competenze, emanare disposizioni attuative del presente decreto e del regolamento DORA, anche per tener conto degli orientamenti delle Autorità europee di vigilanza, nonché delle disposizioni riguardanti le modalità di esercizio dei poteri di vigilanza.

L'**articolo 10** apporta modifiche alla disciplina nazionale di settore (decreto legislativo 1° settembre 1993, n. 395; decreto legislativo 24 febbraio 1998, n. 58; decreto legislativo 9 settembre 2005, n. 209;

decreto legislativo 5 dicembre 2005, n. 252; decreto legislativo 5 settembre 2024, n. 129) introducendo delle sanzioni amministrative pecuniarie graduate in due fasce di gravità a seconda del tipo di obbligo violato previsto dal regolamento (UE) 2022/2554. Dispone, infine, che i provvedimenti di applicazione delle sanzioni, dopo la comunicazione al destinatario, siano pubblicati senza ritardo e per estratto nel sito internet dell'Autorità competente DORA che lo ha adottato.

Anche per quanto concerne le disposizioni di cui al Capo IV, si evidenzia che la Banca d'Italia ha, ai sensi degli articoli 131 e 282 del TFUE, un bilancio autonomo e gode della più ampia indipendenza finanziaria e che la Consob, la Covip e l'Ivass provvedono autonomamente, con forme di autofinanziamento basate sulle contribuzioni dovute dai soggetti vigilati, alla copertura dei costi derivanti dalle attività svolte.

Pertanto, le Autorità sopra indicate esercitano i poteri di vigilanza e di indagine, regolamentari e sanzionatori di cui agli articoli 8, 9 e 10 del decreto in esame con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente, e comunque senza nuovi o maggiori oneri a carico della finanza pubblica.

Si precisa, inoltre, che le sanzioni disciplinate dal presente decreto sono di nuova istituzione e che i proventi da esse derivanti sono versati al bilancio dello Stato.

Nel dettaglio:

- per le sanzioni applicate dalla Banca d'Italia, secondo la procedura sanzionatoria di cui all'articolo 145 del decreto legislativo n. 385 del 1993 (TUB), la destinazione al bilancio dello Stato deriva dall'applicazione del comma 9, secondo periodo, del richiamato articolo 145 TUB, in base al quale «I proventi derivanti dalle sanzioni previste dal presente titolo affluiscono al bilancio dello Stato»;
- per le sanzioni applicate dalla COVIP, secondo la procedura sanzionatoria di cui all'articolo 19-*quinquies* del decreto legislativo 5 dicembre 2005, n. 252, la destinazione al bilancio dello Stato deriva dall'applicazione del comma 7 del richiamato articolo 19-*quinquies*, che letteralmente fa riferimento ai «I proventi derivanti dalle sanzioni previste dal presente titolo affluiscono al bilancio dello Stato»;
- per le sanzioni applicate dall'IVASS, secondo la procedura di cui agli articoli 311-*septies*, 324-*octies* e 324-*novies* del decreto legislativo n. 209 del 2005 (CAP), la destinazione al bilancio dello Stato deriverebbe dalla circostanza che trattasi di sanzioni di natura diversa rispetto a quelle per cui è espressamente prevista nel CAP la destinazione a CONSAP;
- per le sanzioni applicate dalla Consob e dalla Banca d'Italia, secondo la procedura sanzionatoria di cui all'articolo 195 del decreto legislativo n. 58 del 1998 (TUF) la destinazione è analogamente il bilancio dello Stato.

Il **Capo V** contiene «Ulteriori modificazioni e integrazioni della normativa di settore e disposizioni di coordinamento» che recepiscono le modifiche apportate dalla direttiva DORA alle direttive 2009/138/CE, 2014/65/UE e (UE) 2016/2341 e introducono alcune disposizioni di coordinamento con il decreto legislativo 4 settembre 2024, n. 138, recante il recepimento della direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione. Tutte le modifiche ivi contenute sono di natura ordinamentale e, pertanto, non comportano nuovi o maggiori oneri per la finanza pubblica.

Infine, il **Capo VI** contiene «Disposizioni finali». L'**articolo 16** dispone che dal decreto in esame non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e che le amministrazioni competenti e le istituzioni pubbliche coinvolte provvedono all'attuazione delle disposizioni di cui al presente decreto con le risorse umane, strumentali e finanziarie previste a legislazione vigente (clausola d'invarianza finanziaria), in linea con quanto previsto dall'articolo 16, comma 3, della legge di delegazione europea 2022-2023. Infine, **articolo 17** regola l'entrata in vigore e l'efficacia differita dell'articolo 6, commi 1 e 2, del presente decreto.

Ministero
dell'Economia e delle Finanze

DIPARTIMENTO DELLA RAGIONERIA GENERALE DELLO STATO

VERIFICA DELLA RELAZIONE TECNICA

La verifica della presente relazione tecnica, effettuata ai sensi e per gli effetti dell'art. 17, comma 3, della legge 31 dicembre 2009, n. 196 ha avuto esito Positivo.

Il Ragioniere Generale dello Stato

Firmato digitalmente

ANALISI TECNICO-NORMATIVA (ATN)

Amministrazione proponente: Ministero dell'economia e delle finanze

Titolo: Schema di Decreto legislativo, recante «*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/2554, 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, (UE) n. 909/2014 e (UE) 2016/1011, e per il recepimento della direttiva (UE) 2022/2556, che modifica le direttive 2009/65/CE, 2009/138/ce, 2011/61/CE, 2013/36/ UE, 2014/59/ UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario*».

Referente ATN: Ufficio legislativo economia del Ministero dell'economia e delle finanze.

PARTE I - ASPETTI TECNICO-NORMATIVI DI DIRITTO INTERNO

1) ***Obiettivi e necessità dell'intervento normativo. Coerenza con il programma di governo.***

Il decreto in esame dispone l'adeguamento della normativa nazionale al regolamento (UE) 2022/2554, relativo alla resilienza operativa digitale per il settore finanziario di seguito, «**regolamento DORA»** e recepisce la direttiva (UE) 2022/2556, che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per i profili relativi alla resilienza operativa digitale di seguito, **«direttiva DORA»**, alla luce dei principi e criteri direttivi declinati all'articolo 16 della legge 21 febbraio 2024 n. 15, recante «Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea», di seguito «legge di delegazione europea 2022-2023».

L'articolo 16 della legge di delegazione europea 2022-2023 è stato modificato dall'articolo 15 della legge 28 giugno 2024, n. 90, che ha introdotto al comma 2 la nuova lettera c-*bis*), al fine di delegare il Governo ad apportare alla disciplina applicabile agli intermediari finanziari iscritti nell'albo previsto dall'articolo 106 del testo unico delle leggi in materia bancaria e creditizia di cui al decreto legislativo 1° settembre 1993, n. 385, di seguito «intermediari finanziari», nonché alla società Poste italiane Spa per l'attività del Patrimonio Bancoposta di cui al decreto del Presidente della Repubblica 14 marzo 2001, n. 144, di seguito «Bancoposta», le occorrenti modifiche e integrazioni, per conseguire un livello elevato di resilienza operativa digitale e assicurare la stabilità del settore finanziario nel suo complesso, definendo, tra l'altro, presidi in materia di resilienza operativa digitale equivalenti a quelli stabiliti dal regolamento DORA.

Considerato il contesto normativo nazionale e la recente evoluzione della regolamentazione europea con l'adozione del regolamento e della direttiva DORA, con l'introduzione della nuova disciplina si intende conseguire i seguenti obiettivi: consentire l'applicazione delle previsioni europee relative alla resilienza operativa digitale ed estendere l'applicazione di presidi equivalenti a quelli previsti dal Regolamento DORA anche agli intermediari finanziari e a Bancoposta. Ciò per consentire al sistema finanziario italiano nel suo complesso di essere in linea con l'evoluzione tecnologica nello scenario competitivo globale e atto ad affrontarne le relative sfide.

Le disposizioni recate dal provvedimento, alla luce delle considerazioni sopra espresse, appaiono pienamente coerenti con il programma di Governo.

In aggiunta, si rileva come l'intervento normativo di adeguamento e di recepimento si renda necessario e debba essere completato in tempo utile per l'applicazione della disciplina unionale, prevista per il prossimo 17 gennaio 2025.

2) ***Analisi del quadro normativo nazionale.***

Il provvedimento in esame dispone l'adeguamento della normativa nazionale alle previsioni del regolamento DORA e recepisce la direttiva DORA, al fine di creare un quadro nazionale sulla resilienza operativa digitale del settore finanziario in linea con le previsioni del legislatore europeo. Le modifiche contenute nel presente decreto rappresentano, pertanto, il presupposto necessario per garantire la piena operatività della disciplina DORA in Italia e rispondono all'esigenza di adattare l'ordinamento italiano alla mutata cornice normativa eurounitaria.

Il provvedimento dispiega i suoi effetti su un numero ampio di soggetti la cui attività è attualmente disciplinata da diverse fonti di diritto nazionale.

Rilevano in particolare:

- il decreto legislativo 1° settembre 1993, n. 385, recante «Testo unico delle leggi in materia bancaria e creditizia»;
- il decreto legislativo 24 febbraio 1998, n. 58, recante «Testo unico delle disposizioni in materia di intermediazione finanziaria, ai sensi degli articoli 8 e 21 della legge 6 febbraio 1996, n. 52»;
- il decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, recante «Disposizioni urgenti per favorire lo sviluppo e per la correzione dell'andamento dei conti pubblici»;
- il decreto legislativo 9 settembre 2005, n. 209, recante il «Codice delle assicurazioni private»;
- il decreto legislativo 5 dicembre 2005, n. 252, recante la «Disciplina delle forme pensionistiche complementari»;

- il decreto legislativo 16 novembre 2015, n. 180, recante «Attuazione della direttiva 2014/59/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, che istituisce un quadro di risanamento e risoluzione degli enti creditizi e delle imprese di investimento e che modifica la direttiva 82/891/CEE del Consiglio, e le direttive 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE e 2013/36/UE e i regolamenti (UE), n. 1093/2010 e (UE) n. 648/2012, del Parlamento europeo e del Consiglio»
- il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, recante «Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica»;
- il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale»;
- il decreto legislativo 4 settembre 2024, n. 138, recante «Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148»;
- la legge 28 giugno 2024, n. 90, recante «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» e, in particolare, l'articolo 15 che ha modificato l'articolo 16, comma 2, della legge 21 febbraio 2024, n. 15;

  il decreto legislativo 5 settembre 2024, n. 129, recante «Adeguamento della normativa nazionale al regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937.

3) ***Incidenza delle norme proposte sulle leggi e i regolamenti vigenti.***

Il presente decreto incide direttamente sui seguenti decreti legislativi vigenti: decreto legislativo 1° settembre 1993, n. 395; decreto legislativo 24 febbraio 1998, n. 58; decreto legislativo 9 settembre 2005, n. 209; decreto legislativo 5 dicembre 2005, n. 252; decreto legislativo 5 settembre 2024, n. 129; decreto legislativo 16 novembre 2015, n. 180, in quanto modifica alcune disposizioni attuative di previsioni delle direttive 2014/65/UE, 2009/138/CE, (UE) 2016/2341 e 2014/59/UE che sono state modificate dalla direttiva DORA.

In particolare:

- con l'articolo 10 del decreto si apportano modifiche alla disciplina nazionale di settore (decreto legislativo 1° settembre 1993, n. 395; decreto legislativo 24 febbraio 1998, n. 58; decreto legislativo 9 settembre 2005, n. 209; decreto legislativo 5 dicembre 2005, n. 252; decreto legislativo 5 settembre 2024, n. 129) introducendo delle sanzioni amministrative pecuniarie graduate in due fasce di gravità a seconda del tipo di obbligo violato previsto dal regolamento (UE) 2022/2554.
- con l'articolo 11 del decreto si apportano talune modifiche al decreto legislativo 24 febbraio 1998, n. 58, disponendo:
  - all'articolo 65 (che disciplina i requisiti organizzativi per i mercati regolamentati), al comma 1:
    i) la sostituzione della lettera b): tale modifica è volta a specificare che i rischi ai quali sono esposti i mercati regolamentari e relativamente ai quali devono adottare procedure rientrano anche i rischi informatici ai sensi del capo II del regolamento DORA;
    ii) l'abrogazione della lettera c) (in base alla quale il mercato regolamentato dispone di misure per garantire una gestione sana delle operazioni tecniche del sistema, comprese misure di emergenza efficaci per far fronte ai rischi di disfunzione del sistema). Tale abrogazione è disposta in attuazione dell'articolo 6, paragrafo 3 lettera b) della direttiva DORA;
  - all'articolo 65-sexies (che disciplina i requisiti dei sistemi multilaterali di negoziazione e dei sistemi organizzati di negoziazione), si dispone la sostituzione del comma 1, al fine di prevedere che tali sistemi istituiscano e mantengano la loro resilienza operativa conformemente agli obblighi stabiliti al capo II del regolamento DORA, per assicurare che i loro sistemi di negoziazione: a) siano resilienti e abbiano capacità sufficiente per gestire i picchi di volume di ordini e messaggi; b) siano in grado di garantire negoziazioni ordinate in condizioni di mercato critiche; c) siano pienamente testati per garantire il rispetto delle condizioni di cui alle lettere a) e b); d) siano soggetti a efficaci disposizioni in materia di continuità operativa, compresi politica e piani di continuità operativa delle tecnologie dell'informazione e della comunicazione e piani di risposta e di ripristino relativi alle tecnologie dell'informazione e della comunicazione istituiti ai sensi dell'articolo 11 del regolamento DORA, per assicurare la continuità dei servizi in caso di malfunzionamento dei loro sistemi di negoziazione;
- con l'articolo 12 si interviene sull'articolo 30 del decreto legislativo 7 settembre 2005, n. 209, al fine di sostituire l'attuale comma 4 (che attualmente prevede che l'impresa adotta misure

ragionevoli idonee a garantire la continuità e la regolarità dell'attività esercitata, inclusa l'elaborazione di piani di emergenza e che a tal fine, utilizza adeguati e proporzionati sistemi, risorse e procedure interne); la sostituzione è volta a specificare che l'impresa, in particolare, istituisce e gestisce sistemi informatici e di rete conformemente al regolamento DORA;

- con l'articolo 13 si interviene sull'articolo 4-bis del decreto legislativo 5 dicembre 2005, n. 252 (che disciplina i requisiti generali in materia di sistema di governo). Si sostituisce l'attuale comma 6 (in base al quale i fondi pensione di cui al comma 1 della medesima previsione adottano misure appropriate atte a garantire la continuità e la regolarità dello svolgimento delle loro attività, tra cui l'elaborazione di piani di emergenza e a tal fine utilizzano sistemi, risorse e procedure adeguati e proporzionati) al fine di specificare che, in particolare, i fondi pensione istituiscono e gestiscono sistemi informatici e di rete conformemente al regolamento DORA, ove applicabile;
- con l'articolo 14 si interviene sul decreto legislativo 16 novembre 2015, n. 180, al fine di modificare:
  - l'articolo 102 del medesimo decreto, che reca disposizioni relative al contenuto dei piani di risoluzione, in particolare intervenendo:
    - ✓ sul relativo comma 3, lettera c), in base alla quale il piano comprende laddove possibile e opportuno, in forma quantificata la dimostrazione di come le funzioni essenziali e le linee di operatività principali possano essere separate dalle altre funzioni, sul piano giuridico ed economico, nella misura necessaria, in modo da garantirne la continuità in caso di dissesto della banca, per introdurre un riferimento alla *resilienza operativa digitale*;
    - ✓ sul relativo comma 3, lettera r), che attualmente richiede una descrizione delle operazioni e dei sistemi essenziali per assicurare la continuità del funzionamento dei processi operativi della banca, per introdurre un riferimento ai sistemi informatici e di rete di cui al regolamento DORA;
  - l'articolo 104, comma 1, lettera c), che reca disposizioni in merito agli elementi da considerare nell'ambito della valutazione di risolvibilità di una banca o di un gruppo, e attualmente prevede che fermo restando quanto previsto dalle norme tecniche di attuazione adottate dalla Commissione europea, per valutare la risolvibilità di una banca o di un gruppo siano esaminati l'efficacia, anche in caso di risoluzione della banca/gruppo, dei contratti di servizio, l'adeguatezza dei presidi di governo adottati dalla banca/gruppo per assicurare che tali contratti siano adempiuti nella misura e secondo la qualità concordata, nonché la presenza di procedure per trasferire a terzi i servizi forniti

in virtù di tali accordi, in caso di separazione delle funzioni essenziali o delle linee di operatività principali. Con la modifica apportata dal decreto si introduce un riferimento agli accordi contrattuali per l'utilizzo di servizi TIC, come definiti all'articolo 3, punto 21), del regolamento DORA.

Per quanto riguarda gli interventi della direttiva DORA sulle direttive 2009/65/CE, 2011/61/UE, 2013/36/UE e 2015/2366/UE, le necessarie modifiche saranno apportate con interventi specifici alla normativa secondaria della Banca d'Italia, che attualmente reca le relative disposizioni di attuazione, in coerenza con l'impianto adottato dall'ordinamento interno in sede di recepimento di tali atti europei e in linea con i criteri contenuti nella legge di delegazione europea 2022-2023.

4) ***Analisi della compatibilità dell'intervento con i principi costituzionali.***
Non si rilevano profili di incompatibilità con i principi costituzionali.

5) ***Analisi delle compatibilità dell'intervento con le competenze e le funzioni delle regioni ordinarie e a statuto speciale nonché degli enti locali.***
Non si rilevano profili di incompatibilità con le competenze e le funzioni delle regioni ordinarie e a statuto speciale nonché degli enti locali, anche in considerazione del fatto che la materia rientra tra quelle in cui lo Stato ha legislazione esclusiva ai sensi dell'articolo 117, secondo comma, lettera *e)* della Costituzione.

6) ***Verifica della compatibilità con i principi di sussidiarietà, differenziazione ed adeguatezza sanciti dall'articolo 118, primo comma, della Costituzione.***
Non si rilevano profili di incompatibilità con i principi di sussidiarietà, differenziazione e adeguatezza sanciti dall'articolo 118, primo comma, della Costituzione.

7) ***Verifica dell'assenza di rilegificazioni e della piena utilizzazione delle possibilità di delegificazione e degli strumenti di semplificazione normativa.***
Non sono previste rilegificazioni di norme delegificate. Lo schema di decreto ha a oggetto materie non suscettibili di ulteriore delegificazione, né di applicazione di strumenti di semplificazione normativa.

8) ***Verifica dell'esistenza di progetti di legge vertenti su materia analoga all'esame del Parlamento e relativo stato dell'iter.***

Non si riscontrano progetti di legge attualmente vertenti su materia analoga all'esame del Parlamento.

9) ***Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi di costituzionalità sul medesimo o analogo oggetto.***

Non risultano indicazioni delle linee prevalenti della giurisprudenza e non sono pendenti giudizi di costituzionalità sul medesimo o analogo oggetto.

PARTE II - CONTESTO NORMATIVO DELL'UNIONE EUROPEA E INTERNAZIONALE

10) ***Analisi della compatibilità dell'intervento con l'ordinamento dell'Unione europea.***

Al fine di disporre delle necessarie misure di adeguamento dell'ordinamento italiano al regolamento DORA, e di recepire la direttiva DORA, che modifica una serie di direttive settoriali, il decreto in commento, da un lato, dà attuazione alle disposizioni non direttamente applicabili contenute in DORA e, dall'altro lato, garantisce i necessari interventi di adeguamento della normativa nazionale vigente ai fini del recepimento della direttiva, in ossequio ai principi e criteri direttivi contenuti nella delega di cui al richiamato articolo 16 della legge di delegazione europea 2022-2023.

Il provvedimento, quindi, è compatibile con l'ordinamento dell'Unione europea.

11) ***Verifica dell'esistenza di procedure di infrazione da parte della Commissione Europea sul medesimo o analogo oggetto.***

Non risultano procedure di infrazione da parte della Commissione europea sul medesimo o analogo oggetto.

12) ***Analisi della compatibilità dell'intervento con gli obblighi internazionali.***

Il provvedimento legislativo in esame non presenta profili di incompatibilità con gli obblighi internazionali.

13) ***Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte di Giustizia dell'Unione europea sul medesimo o analogo oggetto.***

Non risultano indicazioni sulle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte di Giustizia delle Comunità europee sul medesimo o analogo oggetto.

14) ***Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte Europea dei Diritti dell'uomo sul medesimo o analogo oggetto.***

Non risultano pendenti giudizi dinanzi alla Corte europea dei diritti dell'uomo sul medesimo o analogo oggetto.

15) ***Eventuali indicazioni sulle linee prevalenti della regolamentazione sul medesimo oggetto da parte di altri Stati membri dell'Unione europea.***

Non risultano indicazioni sulle linee prevalenti della regolamentazione sul medesimo oggetto da parte di altri Stati membri dell'Unione europea.

PARTE III - ELEMENTI DI QUALITA' SISTEMATICA E REDAZIONALE DEL TESTO

1) ***Individuazione delle nuove definizioni normative introdotte dal testo, della loro necessità, della coerenza con quelle già in uso.***

L'intervento normativo, in piena coerenza con le indicazioni della normativa nazionale e comunitaria, fa proprie alcune delle definizioni ivi contenute, in particolare quelle di cui articoli 2, paragrafo 2, e 3 del regolamento DORA.

Per evitare appesantimenti del testo e migliorare la leggibilità complessiva del decreto, introduce talune definizioni corrispondenti agli acronimi comunemente utilizzati per identificare gli atti normativi di settore (quali le definizioni di TUB, TUF e CAP per indicare rispettivamente il decreto legislativo 1° settembre 1993, n. 385, il decreto legislativo 24 febbraio 1998, n. 58 e il decreto legislativo 7 settembre 2005, n. 209); per le medesime finalità introduce la definizione di «Bancoposta», «Autorità nazionale competente NIS», «CSIRT Italia», «regolamento DORA» e «direttiva DORA». Introduce, altresì, una definizione di «autorità competenti DORA» al fine di individuare unitariamente le autorità competenti ai sensi dell'articolo 46 del regolamento DORA e la Banca d'Italia quale autorità competente su intermediari finanziari e Bancoposta (in quanto assoggettati a una disciplina equivalente a quella dettata dal regolamento DORA).

Il decreto rinvia, per quanto non diversamente previsto, alle definizioni dei citati atti normativi di settore e del decreto legislativo 5 dicembre 2005, n. 252.

2) ***Verifica della correttezza dei riferimenti normativi contenuti nel progetto, con particolare riguardo alle successive modificazioni ed integrazioni subite dai medesimi.***

È stato verificato che i riferimenti normativi contenuti nel provvedimento in esame sono corretti.

3) ***Ricorso alla tecnica della novella legislativa per introdurre modificazioni ed integrazioni a disposizioni vigenti.***

Si evidenzia come il decreto in commento sia adottato sulla base della delega normativa di cui all'articolo 16 della legge di delegazione europea 2022-2023. Pertanto, il ricorso allo strumento normativo in esame è dettato dalla necessità di dare seguito all'indicazione del legislatore. Per quanto concerne, poi, l'incidenza delle norme proposte sulle disposizioni vigenti, si rimanda a quanto dettagliato nella Parte I, punto 3).

4) ***Individuazione di effetti abrogativi impliciti di disposizioni dell'atto normativo e loro traduzione in norme abrogative espresse nel testo normativo.***

Non si ravvisano effetti abrogativi impliciti nelle disposizioni del decreto.

5) ***Individuazione di disposizioni dell'atto normativo aventi effetto retroattivo o di reviviscenza di norme precedentemente abrogate o di interpretazione autentica o derogatorie rispetto alla normativa vigente.***

Il provvedimento in esame non contiene disposizioni aventi effetto retroattivo o di reviviscenza di norme precedentemente abrogate o di interpretazione autentica o derogatorie rispetto alla normativa vigente.

6) ***Verifica della presenza di deleghe aperte sul medesimo oggetto, anche a carattere integrativo o correttivo.***

Non risultano ulteriori deleghe aperte sul medesimo oggetto del presente articolato.

7) ***Indicazione degli eventuali atti successivi attuativi e dei motivi per i quali non è possibile esaurire la disciplina con la normativa proposta e si rende necessario il rinvio a successivi provvedimenti attuativi; verifica della congruità dei termini previsti per la loro adozione***

L'articolo 9 (Poteri regolamentari) del decreto attribuisce alla Banca d'Italia, alla Consob, all'IVASS e alla Covip il potere di emanare disposizioni attuative del decreto e del regolamento DORA anche per tener conto degli orientamenti delle Autorità europee di vigilanza, nonché di adottare disposizioni riguardanti le modalità di esercizio dei poteri di vigilanza.

Il rinvio a successivi provvedimenti attuativi si rende necessario per consentire alle Autorità di poter adattare la disciplina primaria emanando disposizioni di rango secondario, anche in previsione di indicazioni in materia che potranno essere emanate dalle Autorità europee di vigilanza nel futuro, nonché di definire le modalità di esercizio dei propri poteri di vigilanza. Ciò risulta in linea con quanto previsto anche in altri atti normativi nazionali di adeguamento a regolamenti unionali di settore. La

potestà conferita è ad esercizio eventuale, pertanto non sono previsti dei termini per l'adozione dei relativi provvedimenti.

8) ***Verifica della piena utilizzazione e dell'aggiornamento di dati e di riferimenti statistici attinenti alla materia oggetto del provvedimento, ovvero indicazione della necessità di commissionare all'Istituto nazionale di statistica apposite elaborazioni statistiche con correlata indicazione nella relazione economico-finanziaria della sostenibilità dei relativi costi.***

Con riferimento alla materia oggetto del provvedimento in esame, si evidenzia come non si necessiti di dati e di riferimenti statistici per la natura stessa del decreto, che è atto necessario ai fini dell'adeguamento a un regolamento unionale e al recepimento della correlata direttiva.

ANALISI DI IMPATTO DELLA REGOLAMENTAZIONE (A.I.R.)

(Ai sensi dell'Allegato 2 della direttiva del PCM del 16 febbraio 2018)

Provvedimento: schema di decreto legislativo recante «disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/2554, 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, (UE) n. 909/2014 e (UE) 2016/1011, e per il recepimento della direttiva (UE) 2022/2556, che modifica le direttive 2009/65/CE, 2009/138/ce, 2011/61/CE, 2013/36/ UE, 2014/59/ UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario».

Amministrazione competente: Ministero dell'economia e delle finanze

Referente AIR: Ufficio legislativo economia

Allegato*:* Sintesi Impact Assessment.

SINTESI DELL'AIR E PRINCIPALI CONCLUSIONI

In linea con i principi e i criteri direttivi declinati dall'articolo 16 della legge 21 febbraio 2024, n. 15 di seguito «legge di delegazione europea 2022-2023», il decreto in esame introduce le disposizioni necessarie per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario «**regolamento DORA»** e per il recepimento della direttiva (UE) 2022/2556, che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario «**direttiva DORA**». In linea con quanto previsto dall'articolo 16, comma 2, lettera c-*bis)*, della legge di delegazione europea 2022-2023, come modificata dall'articolo 15 della legge 28 giugno 2024, n. 90, il decreto in esame estende l'applicazione di alcune disposizioni del regolamento DORA ad altri soggetti che operano nel settore finanziario a livello nazionale (gli intermediari finanziari iscritti nell'albo previsto dall'articolo 106 del decreto legislativo 1° settembre 1993, n. 385, di seguito «intermediari finanziari» e la società Poste italiane S.p.a. per l'attività del Patrimonio Bancoposta, di cui al regolamento recante norme sui servizi di bancoposta di cui al decreto del Presidente della Repubblica 14 marzo 2001, n. 144, di seguito «Bancoposta»).

1. CONTESTO E PROBLEMI DA AFFRONTARE

Il provvedimento in oggetto contiene, primariamente, le modifiche necessarie ad adeguare la normativa nazionale al regolamento DORA e a recepire la direttiva DORA, che riguardano la maggioranza delle entità finanziarie che operano ai sensi della legislazione unionale. Parallelamente, in linea con quanto previsto dai criteri di delega e al fine di garantire un elevato livello di sicurezza cibernetica del sistema finanziario italiano, il provvedimento dispone l'applicazione di alcuni dei presidi stabiliti dal regolamento DORA, nel rispetto del principio di proporzionalità, anche a due categorie di soggetti che operano ai sensi della legislazione finanziaria nazionale (intermediari finanziari e Bancoposta).

In quanto funzionali a garantire l'adeguamento dell'ordinamento nazionale alle nuove regole europee, le modifiche contenute nel presente schema di decreto rappresentano il presupposto necessario per

garantire la piena conformità dell'ordinamento al nuovo quadro normativo euro-unitario. Esso è stato modificato a seguito delle iniziative del *Digital Financial Package* della Commissione europea con l'obiettivo di rafforzare la resilienza operativa digitale del settore finanziario sulla base di due principali argomentazioni: il mercato finanziario è il principale utilizzatore di infrastrutture per le tecnologie dell'informazione e della comunicazione (TIC) al mondo, rappresentando circa un quinto di tutta la spesa IT, e la dipendenza di questo settore dalle TIC è destinata ad aumentare ulteriormente con l'uso crescente di modelli e tecnologie emergenti, quali le DLT e l'intelligenza artificiale.

Come indicato nell'*Impact assessment* a corredo della proposta della Commissione europea del 24 settembre 2020 ivi allegato, l'iniziativa unionale prende, dunque, le mosse dalla constatazione che la maggiore dipendenza dalle TIC pone nuove sfide in termini di resilienza operativa e il crescente livello di digitalizzazione dei servizi finanziari rende il sistema finanziario sempre più vulnerabile agli incidenti operativi e agli attacchi informatici. Le imprese che operano nel settore finanziario sono risultate essere trecento volte più a rischio di essere bersaglio di attacchi informatici rispetto a qualsiasi altro settore economico[1].

Rispetto a tale analisi di impatto, i *trend* recenti di rischio per il sistema finanziario nazionale e per quello europeo confermano, anche in relazione all'accresciuto livello di rischio geo-politico e alle tensioni internazionali, l'esposizione del settore ai rischi *cyber-ICT* in generale e agli attacchi di tipo più grave quali i *ransomware*.

Dalla relazione annuale dell'Agenzia per la Cybersicurezza Nazionale (ACN) sul 2023 emerge un fortissimo aumento degli incidenti segnalati nel 2023 (303, contro 126 nel 2022), che ha interessato tutti i settori economici[2]. Il numero di attacchi di tipo *ransomware*, che costituisce il fenomeno più allarmante, è aumentato del 27 per cento, interessando sia le PMI sia le grandi imprese.

Le segnalazioni inviate alla Banca d'Italia dalle banche e dai prestatori di servizi di pagamento confermano la forte accelerazione del numero di incidenti cyber l'anno scorso: 30 segnalazioni di attacchi, contro 13 nel 2022. I casi più frequenti hanno riguardato la disponibilità di servizi offerti alla clientela (cosiddetti attacchi *Denial Of Service*), talvolta attuati da soggetti che appaiono riconducibili a Governi di Paesi extraeuropei.

Inoltre, incidenti recenti alla catena di fornitura assicurata da operatori a livello globale confermano l'importanza di rafforzare il quadro di sorveglianza sui fornitori critici del settore ICT.

Questi aspetti sono anche sotto esame da parte delle autorità di vigilanza del settore finanziario: nell'ambito del loro più ampio mandato di garantire la stabilità e l'integrità del sistema finanziario, infatti, tali autorità richiedono in misura crescente ai soggetti vigilati di gestire efficacemente le proprie capacità di resilienza operativa, in particolare, per affrontare i rischi relativi alle TIC e alla sicurezza e attenuarne gli impatti. Il rischio ICT è, infatti, una delle principali componenti del rischio operativo, che le autorità di vigilanza prudenziale valutano e monitorano costantemente nell'ambito del loro mandato.

Il panorama normativo dell'Unione in materia di servizi finanziari precedente al pacchetto DORA comprendeva già disposizioni in materia di resilienza operativa, concernenti anche le componenti di rischio relative alle TIC e la sicurezza (in particolare, per le infrastrutture dei mercati finanziari che erano soggetti a norme particolarmente rigorose). Tuttavia, in altre parti dell'*acquis* del settore finanziario, le norme sulle TIC e sui rischi per la sicurezza sono risultate più generiche, e per alcune specifiche tematiche non adeguatamente cogenti.

Nel complesso, le disposizioni previgenti sono apparse incoerenti e frammentate in termini di ambito di applicazione, granularità e specificità.

[1] Cfr. Commission Staff Working Document Impact Assessment Report, ivi allegato, p. 8
[2] Cfr. Agenzia per la cybersicurezza nazionale (ACN), "Relazione annuale al Parlamento, 2023".

In altri termini, la risposta dell'UE alle crescenti esigenze di resilienza operativa e digitale a livello orizzontale e settoriale si è basata su un'armonizzazione minima, lasciando, così, spazio alle interpretazioni nazionali oppure si è rivelata troppo generica e con un'applicazione limitata o parziale, regolamentando solo alcune componenti della resilienza operativa digitale (ad esempio, la gestione dei rischi relativi alle TIC, la segnalazione degli incidenti e i rischi relativi alle TIC derivanti da terzi), trascurandone altre (ad esempio, i test di resilienza).

Le lacune e le incoerenze del precedente regime hanno provocato la proliferazione di iniziative nazionali[3] e di approcci di vigilanza (ad esempio, per quanto riguarda la dipendenza da soggetti terzi nel settore delle TIC) non coordinati, dando luogo a sovrapposizioni, duplicazione di requisiti ed elevati costi amministrativi e di *compliance* per le imprese finanziarie che operano su base transfrontaliera o impedendo di individuare e affrontare in maniera complessiva o per i profili di tipo *cross-border* i rischi relativi alle TIC. Nel complesso, la stabilità e l'integrità del settore finanziario sono risultate non adeguatamente garantite e il mercato unico dei servizi finanziari è rimasto esposto a possibili rischi di frammentazione rispetto alla loro resilienza e continuità; di conseguenza la tutela dei consumatori e degli investitori presentava margini di miglioramento.

Si è imposta, dunque, l'esigenza di un aggiornamento, di una razionalizzazione e di un'armonizzazione a livello dell'Unione di tali requisiti e dell'insieme di strumenti di vigilanza/monitoraggio delle autorità di vigilanza finanziaria.

Tali obiettivi sono stati perseguiti col regolamento DORA e la correlata direttiva, nonché con i progetti di norme tecniche di regolamentazione e di attuazione sviluppate dalle tre Autorità di supervisione europee[4], le cui disposizioni si applicheranno dal prossimo 17 gennaio 2025.

Il regolamento DORA prevede, in particolare:

- 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, alle entità finanziarie che rientrano nell'ambito di applicazione del regolamento;
- obblighi di segnalazione di incidenti rilevanti connessi alle TIC secondo criteri, modelli e meccanismi uniformi;
- test di resilienza operativa digitale al fine di aggiornare e di rivedere regolarmente i sistemi e gli strumenti di risposta agli attacchi informatici o alle interruzioni TIC e di garantire in tal modo la resilienza operativa;
- gestione dei rischi derivanti da soggetti che forniscono servizi TIC alle entità finanziarie, tramite la previsione di requisiti di gestione dei rischi da parte delle entità finanziarie e di un quadro di sorveglianza diretta dei fornitori terzi critici di servizi TIC;
- meccanismi di condivisione delle informazioni tra le Autorità competenti e tra gli stessi operatori.

2. OBIETTIVI DELL'INTERVENTO E RELATIVI INDICATORI

2.1 Obiettivi generali e specifici

Alla luce del contesto e dei problemi da affrontare come descritti nella Sezione 1, l'obiettivo, generale, della disciplina in commento è quello di aumentare la resilienza operativa digitale delle

[3] Ad esempio, il quadro nazionale di regolamentazione già vigente per il settore finanziario, con particolare riferimento ai comparti bancario, assicurativo e delle infrastrutture di mercato, fissava alcuni requisiti in larga parte compatibili con quanto previsto in DORA. In tal senso, la normativa DORA non costituisce una novità assoluta nel panorama attuale.
[4] Tali progetti di norme sono in corso di adozione da parte della Commissione europea.

entità finanziarie. Ulteriori obiettivi specifici sono quelli di razionalizzare e aggiornare la previgente normativa finanziaria dell'Unione e introdurre nuovi requisiti allo scopo di migliorare la gestione dei rischi relativi alle TIC da parte delle entità finanziarie; incrementare il patrimonio informativo delle autorità di vigilanza per quanto concerne minacce e incidenti;·migliorare i test che le imprese finanziarie effettuano sui propri sistemi di TIC; e migliorare la vigilanza sui rischi derivanti dalla dipendenza delle imprese finanziarie dai fornitori terzi di servizi TIC.

Più in dettaglio, come evidenziato nell'*Impact assessment* della Commissione europea allegato, l'obiettivo di rafforzare la resilienza operativa digitale si è estrinsecato in tre obiettivi generali

- *ridurre il rischio di perturbazioni e instabilità finanziarie*, che si è tradotto nei seguenti obiettivi specifici:
  - affrontare i rischi relativi alle TIC in modo più completo e rafforzare il livello generale di resilienza digitale del settore finanziario;
  - consentire alle autorità di vigilanza finanziaria di accedere alle informazioni sugli incidenti connessi alle TIC;
  - garantire che le entità finanziarie valutino l'efficacia delle loro misure preventive e di resilienza e individuino le vulnerabilità delle TIC;
  - rafforzare le norme per la sorveglianza indiretta dei fornitori terzi di servizi TIC;
  - consentire una sorveglianza diretta delle attività dei fornitori terzi critici di servizi TIC;
  - incentivare lo scambio di informazioni sulle minacce nel settore finanziario.
- *ridurre gli oneri amministrativi e incrementare l'efficacia della vigilanza*: il perseguimento di questo obiettivo richiede la razionalizzazione e la semplificazione degli obblighi di segnalazione degli incidenti e l'introduzione di un quadro coerente per i test di resilienza operativa digitale, che contribuisce a ridurre i costi derivanti dai test multipli. Ciò si traduce nei seguenti obiettivi specifici:
  - razionalizzare la segnalazione degli incidenti relativi alle TIC e affrontare il problema della sovrapposizione dei requisiti;
  - ridurre la frammentazione del mercato unico e consentire l'accettazione transfrontaliera dei risultati dei test;
- *aumentare la protezione dei consumatori e degli investitori*: le misure previste sono rivolte alle entità finanziarie. Tuttavia, il rafforzamento della resilienza operativa digitale dei singoli operatori e quella complessiva del settore finanziario dell'Unione contribuisce anche ad aumentare la protezione dei consumatori e degli investitori.

La disciplina normativa in commento, quale intervento di adeguamento al regolamento DORA e di recepimento della direttiva DORA, prende da quest'ultimo tutti gli obiettivi generali e speciali. Inoltre, in stretta aderenza a quanto previsto dall'articolo 16, comma 2, lettera *c-bis*) della legge di delegazione europea 2022-2023, persegue l'ulteriore obiettivo di apportare alla disciplina applicabile agli intermediari finanziari e a Bancoposta le occorrenti modifiche e integrazioni per conseguire un livello di resilienza operativa digitale elevato ed equivalente a quello definito dal regolamento DORA per gli altri soggetti operanti nel sistema finanziario nazionale, nel rispetto del principio di proporzionalità.

2.2 Indicatori e valori di riferimento

Tenuto conto degli obiettivi generali e specifici sopra riportati, nonché del contesto normativo europeo di riferimento, il grado di raggiungimento degli obiettivi potrà essere verificato sulla base dei seguenti indicatori e valori di riferimento, a titolo non esaustivo:

- numero complessivo dei gravi incidenti TIC segnalati (e dei relativi impatti, secondo le rilevazioni armonizzate in ambito europeo/definite negli RTS) e delle minacce informatiche significative notificate alle autorità di vigilanza e relativa tempestività e qualità delle informazioni riportate;
- numero e rilevanza delle entità finanziarie che partecipano a meccanismi di condivisione volontaria di informazioni e analisi delle minacce informatiche;
- numero di test di penetrazione basati su minacce (TLPT) effettuati rispetto agli obblighi di DORA;
- numero di violazioni della normativa riscontrate successivamente all'introduzione delle nuove disposizioni;
- numero dei procedimenti sanzionatori avviati ed esito dei medesimi.

3. OPZIONI DI INTERVENTO E VALUTAZIONE PRELIMINARE

Si evidenzia, preliminarmente, come la valutazione delle opzioni di intervento abbia tenuto in considerazione il contesto di partenza e i problemi da affrontare descritti nella Sezione 1. Per l'effetto, l'opzione di non intervento, ossia lo scenario base, non è stata ritenuta percorribile, in quanto la modifica normativa in commento rappresenta il presupposto necessario per consentire l'adeguamento dell'ordinamento al regolamento DORA e al recepimento della direttiva DORA. A tale considerazione, si aggiunga che l'opzione di non intervento avrebbe reso di fatto non raggiungibili gli obiettivi generali e specifici indicati nella precedente Sezione 2, vanificando la stessa *ratio* fondatrice della disciplina unionale.

A livello europeo, tutte le opzioni di intervento sono state oggetto di valutazione da parte della Commissione europea nel citato *Impact assessment*. È stata, innanzitutto, considerata l'opzione «nessun intervento»: in tale scenario, le norme sulla resilienza operativa avrebbero continuato a fondarsi sull'attuale insieme di disposizioni dell'UE in materia di servizi finanziari, in parte sulla direttiva NIS e sui regimi nazionali vigenti o futuri.

L'opzione 1 prevedeva un intervento limitato all'introduzione di una riserva di capitale aggiuntiva per rafforzare la capacità delle imprese finanziarie di assorbire le perdite collegate alla mancanza di resilienza operativa.

L'opzione 2 (poi prescelta), prospettava l'adozione di un atto sulla resilienza operativa digitale dei servizi finanziari, con introduzione di un quadro globale a livello dell'UE applicabile a tutte le entità finanziarie regolamentate, che affrontasse in modo più completo i rischi relativi alle TIC; consentisse alle autorità di vigilanza finanziaria di accedere alle informazioni relative agli incidenti connessi alle TIC; garantisse la valutazione da parte delle entità finanziarie dell'efficacia delle proprie misure di prevenzione e resilienza e l'identificazione delle vulnerabilità delle TIC; rafforzasse le norme per la sorveglianza indiretta dei fornitori terzi di servizi TIC; consentisse una sorveglianza diretta delle attività di fornitori terzi critici di servizi TIC; incoraggiasse lo scambio di dati sulle minacce nel settore finanziario.

Una ulteriore opzione, l'opzione 3, prevedeva che all'adozione di un atto sulla resilienza si accompagnasse quello di un atto dedicato alla vigilanza centralizzata dei fornitori terzi di servizi di TIC, con istituzione di una nuova autorità incaricata di vigilare sui fornitori terzi che erogano servizi di TIC alle imprese finanziarie.

L'opzione 2 è stata, come anticipato, quella perseguita, in quanto si è rivelata, rispetto alle altre opzioni, quella che si è meglio prestata a realizzare la maggior parte degli obiettivi dell'iniziativa, tenendo conto dei criteri di efficienza e coerenza, nonché quella che ha goduto del maggior sostegno

da parte degli *stakeholder*, in quanto passibile di ridurre al minimo i costi di transizione rispetto alla vigente legislazione dell'UE in materia di servizi finanziari e di bilanciare adeguatamente l'interazione con l'attuale quadro «orizzontale», in particolare, quello risultante dalla disciplina contenuta nella direttiva (UE) 2022/2555.

Venendo alla disciplina nazionale e ai contenuti del provvedimento in commento, la valutazione delle opzioni di intervento lasciate aperte da DORA è stata condotta prendendo in considerazione, innanzitutto, l'attuale contesto normativo.

Al livello di strumento normativo, si è optato per una soluzione organica, ossia quella di disciplinare il *framework* nazionale della resilienza digitale delle entità finanziarie in un decreto autonomo, intervenendo sulle singole discipline settoriali solo al fine di attuare le modifiche richieste dal recepimento della direttiva DORA, che viene a incidere, modificandole, su una serie di direttive che sono state fatte oggetto di recepimento in diversi *corpus* normativi settoriali, sia a livello primario che a livello secondario.

Si prevede, in particolare, all'articolo 9 (Poteri regolamentari) una delega alle Autorità competenti al fine di consentire loro di emanare, nell'ambito delle rispettive competenze, disposizioni attuative dello schema di decreto, nonché del regolamento DORA, anche per tener conto degli orientamenti delle Autorità europee di vigilanza, nonché delle disposizioni riguardanti le modalità di esercizio dei poteri di vigilanza.

Per quanto, invece, concerne le opzioni in relazione alle quali DORA lascia agli Stati membri una scelta discrezionale basata su valutazioni che concernono unicamente le politiche interne del singolo Stato membro, la delega di cui all'articolo 16 della legge di delegazione europea 2022-2023 prevede la possibilità di un eventuale esercizio delle medesime.

All'interno della cornice di regolamentazione unitaria rappresentata dal provvedimento in commento sono state, pertanto, valutate le seguenti opzioni:

- **Articolo 2, paragrafo 4** – possibilità di escludere dall'ambito di applicazione del regolamento le entità di cui all'articolo 2, paragrafo 5, punti da 4) a 23), della direttiva 2013/36/UE che sono situate nei rispettivi territori.

  Tale opzione non è stata esercitata. Cassa Depositi e Prestiti è espressamente annoverata tra i soggetti destinatari della disciplina (articolo 3, comma 2);

- **Articolo 19, paragrafo 1, sesto comma** – possibilità di stabilire che alcune o tutte le entità finanziarie forniscano la notifica iniziale e ciascuna relazione di cui all'articolo 19, paragrafo 4, del regolamento DORA utilizzando i modelli di cui all'articolo 20 alle autorità competenti o ai gruppi di intervento per la sicurezza informatica in caso di incidente (*computer security incident response teams* — CSIRT) designati o istituiti a norma della direttiva (UE) 2022/2555 (NIS 2).

  Tale opzione è stata esercitata per alcune entità finanziarie (cfr. articolo 4, comma 3) e, nello specifico, per le banche e le infrastrutture dei mercati finanziari che ricadranno anche nell'ambito di applicazione della disciplina di recepimento della direttiva NIS2.

- **Articolo 19, paragrafo 2, terzo comma** – possibilità di stabilire che le entità finanziarie che procedono alla notifica su base volontaria e a norma del primo comma possano, altresì, trasmettere tale notifica ai CSIRT nazionali designati o istituiti a norma della direttiva (UE) 2022/2555.

  Tale opzione è stata esercitata (cfr. articolo 4, comma 4).

- **Articolo 26, paragrafo 9** – possibilità di designare un'autorità pubblica unica nel settore finanziario responsabile delle questioni relative ai TLPT nel settore finanziario a livello nazionale e a cui sono affidati tutte le competenze e tutti i compiti a tal fine.

Tale opzione non è stata esercitata.

- **Articolo 52** – possibilità 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.

  Si è optato per l'introduzione di un regime sanzionatorio di natura esclusivamente amministrativa.

A tali opzioni si affiancano le discrezionalità relative alla designazione di singole autorità per specifiche finalità del regolamento DORA, in particolare:

- **Articolo 19, paragrafo 1, secondo comma** – designazione di un'unica autorità competente quale autorità competente interessata responsabile dell'espletamento delle funzioni e dei compiti di cui al relativo articolo, se un'entità finanziaria è soggetta alla vigilanza di più di un'autorità nazionale competente di cui all'articolo 46 del regolamento DORA.

  La scelta è stata effettuata nell'articolo 4, comma 1.

- **Articolo 32, paragrafo 5** – designazione dell'autorità competente interessata il cui membro del personale è il rappresentante di alto livello di cui all'articolo 32, paragrafo 4, primo comma, lettera *b*).

  La scelta è stata effettuata nell'articolo 3, comma 4, dello schema di decreto.

Per quanto, invece, concerne l'introduzione di un regime di resilienza operativa digitale per gli intermediari finanziari e Bancoposta, la relativa disciplina è stata modulata estendendo quella dettata dal regolamento DORA, in stretta aderenza a quanto imposto dal criterio di delega recato dall'articolo 16, comma 2, lettera c-*bis*) della legge di delegazione 2022-2023, che richiede l'applicazione a intermediari finanziari e Bancoposta di presidi equivalenti a quelli definiti dal regolamento DORA per le altre entità finanziarie. La necessità di tener conto del principio di proporzionalità, contemplata espressamente dal richiamato criterio direttivo, è alla base della previsione di cui all'articolo 6, ove si dispone al comma 1 che gli intermediari finanziari siano soggetti all'ICT *risk management framework* «semplificato» previsto dall'articolo 16 del regolamento DORA per le entità finanziarie di minori dimensioni o complessità. per gli intermediari finanziari che si qualificano come «microimprese» ai sensi dell'articolo 3, paragrafo 1, punto 60), del regolamento DORA (in quanto occupino meno di 10 dipendenti e realizzino un fatturato annuo e/o totale di bilancio annuo non superiore a 2 milioni di euro) non si applica l'articolo 24 in materia di requisiti generali per lo svolgimento dei test di resilienza operativa digitale, in quanto a tali soggetti si applica la disciplina *ad hoc* prevista dal successivo articolo 25, paragrafo 3, del regolamento DORA (cfr. *infra sub* §4.2.A). Infine, il comma 3 dell'articolo 6 rimette alla potestà regolamentare della Banca d'Italia l'eventuale individuazione di una categoria di intermediari finanziari da considerarsi «significativi» (anche per tipologia di attività svolte), a cui applicare l'ICT *risk management framework* completo, in luogo di quello semplificato.

4. COMPARAZIONE DELLE OPZIONI E MOTIVAZIONE DELL'OPZIONE PREFERITA

4.1 Impatti economici, sociali ed ambientali per categoria di destinatari

L'iniziativa unionale su cui si fonda lo schema di decreto in esame prevede la creazione di un quadro per la resilienza operativa delle entità finanziarie, con introduzione di una disciplina dedicata che attualmente non rientra nell'*acquis*.

Ciò implicherà l'assoggettamento a nuovi specifici obblighi per i soggetti individuati nel regolamento DORA come destinatari della nuova disciplina, anche in relazione ai rapporti instaurati con i soggetti definiti quali «fornitori terzi di servizi TIC».

I principali soggetti interessati dalle nuove disposizioni sono, pertanto:

a) enti creditizi (nonché le entità di cui all'articolo 2, paragrafo 5, punti da 4) a 23), della direttiva 2013/36/UE per cui non sia stata esercitata l'opzione di esclusione dall'ambito di applicazione del regolamento);

b) istituti di pagamento, compresi gli istituti di pagamento esentati a norma della direttiva (UE) 2015/2366;

c) prestatori di servizi di informazione sui conti;

d) istituti di moneta elettronica, compresi gli istituti di moneta elettronica esentati a norma della direttiva 2009/110/CE;

e) imprese di investimento;

f) fornitori di servizi per le cripto-attività autorizzati a norma del regolamento del Parlamento europeo e del Consiglio concernente i mercati delle cripto-attività (MiCAR) ed emittenti di token collegati ad attività;

g) depositari centrali di titoli;

h) controparti centrali;

i) sedi di negoziazione;

j) repertori di dati sulle negoziazioni;

k) gestori di fondi di investimento alternativi, ad eccezione dei gestori di cui all'articolo 3, paragrafo 2, della direttiva 2011/61/UE;

l) società di gestione di OICVM;

m) fornitori di servizi di comunicazione dati;

n) imprese di assicurazione e di riassicurazione;

o) intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio;

p) enti pensionistici aziendali o professionali;

q) agenzie di *rating* del credito;

r) amministratori di indici di riferimento critici;

s) fornitori di servizi di *crowdfunding*;

t) repertori di dati sulle cartolarizzazioni.

Una disciplina nazionale modulata su quella dettata dal regolamento DORA si applica, come si è detto, anche a intermediari finanziari e Bancoposta.

Con riferimento ai dati quantitativi circa i potenziali destinatari della nuova disciplina che hanno sede nel territorio della Repubblica, si riporta di seguito una tabella esplicativa[5].

[5] Le fonti utilizzate per i dati gli albi ed elenchi tenuti da Banca d'Italia, Consob/ESMA, IVASS e Covip. Il dato è relativo al 5 agosto 2024 (https://www.consob.it/web/area-pubblica/albo-sim1; https://www.consob.it/web/area-pubblica/mercati-italiani; https://www.esma.europa.eu/document/csd-register; https://www.esma.europa.eu/document/list-registered-trade-repositories; https://www.bancaditalia.it/compiti/vigilanza/albi-elenchi/; https://infostat-ivass.bancaditalia.it/RIGAInquiry-public/ng/#/home; https://www.esma.europa.eu/credit-rating-agencies/cra-authorisation; https://www.esma.europa.eu/esmas-activities/investors-and-issuers/benchmark-administrators; https://www.esma.europa.eu/esmas-activities/markets-and-infrastructure/securitisation).

Categorie di soggetti destinatari	N° di soggetti
Enti creditizi (e entità di cui all'articolo 2, paragrafo 5, punti da 4) a 23), della direttiva 2013/36/UE	347
Intermediari finanziari iscritti nell'albo ex art. 106 TUB	181
Istituti di pagamento, compresi gli istituti di pagamento esentati a norma della direttiva (UE) 2015/2366	41
Prestatori di servizi di informazione sui conti	3
Istituti di moneta elettronica, compresi gli istituti di moneta elettronica esentati a norma della direttiva 2009/110/CE	11
Imprese di investimento	60
Fornitori di servizi per le cripto-attività autorizzati ai sensi di MiCAR ed emittenti di *token* collegati ad attività;	-
Depositari centrali di titoli	1
Controparti centrali	1
Sedi di negoziazione	20[6]
Repertori di dati sulle negoziazioni	-
Gestori di fondi di investimento alternativi	75
Società di gestione di OICVM	44
Fornitori di servizi di comunicazione dati	-
Imprese di assicurazione e di riassicurazione	86
Intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio	5
Enti pensionistici aziendali o professionali	189
Agenzie di *rating* del credito	4
Amministratori di indici di riferimento critici	-
Fornitori di servizi di *crowdfunding*	36[7]

[6] Il dato si riferisce alle singole sedi di negoziazione italiane (6 mercati regolamentati e 14 sistemi multilaterali di negoziazione) autorizzati dalla Consob alla data del 5 agosto 2024; tali sedi sono gestite ed organizzate da due gestori di mercato e da una SIM.

[7] Il dato include una SIM conteggiata anche sotto la voce "Imprese di investimento".

Repertori di dati sulle cartolarizzazioni	-

Oltre all'impatto specifico sugli operatori come sopra rappresentato, il decreto in esame presenta effetti anche sulle amministrazioni nazionali.

In particolare, la normativa in commento attribuisce le dovute funzioni di vigilanza alla Banca d'Italia, alla Consob, all'IVASS e alla COVIP, quali autorità competenti ai sensi dell'articolo 46 di DORA (e alla Banca d'Italia quale autorità competente per gli intermediari finanziari e Bancoposta). Il provvedimento in esame attribuisce, inoltre, alle stesse Autorità poteri di accertamento e sanzionatori, nonché una potestà regolamentare dedicata. Prevede che le medesime autorità individuino forme di coordinamento operativo e informativo tramite protocolli d'intesa, e stipulino protocolli di intesa anche con l'Agenzia per la cybersicurezza nazionale, in particolare, relativamente allo scambio di informazioni pertinenti, all'istituzione di forme di consulenza e assistenza tecnica reciproca e di risposta rapida nel caso di incidenti, nonché specifichino, se del caso, le modalità di coordinamento delle attività relative a soggetti essenziali o importanti per la NIS2 che siano stati designati come fornitori terzi critici di servizi TIC.

Per quanto concerne gli effetti delle previsioni così riassunte sulle amministrazioni nazionali, si evidenzia come dalle nuove attribuzioni non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Le Autorità provvedono all'attuazione delle disposizioni di cui al presente decreto con le risorse umane, strumentali e finanziarie previste a legislazione vigente. In particolare, la Banca d'Italia ha, ai sensi degli articoli 131 e 282 del TFUE, un bilancio autonomo e gode della più ampia indipendenza finanziaria e la Consob, l'IVASS e la COVIP provvedono autonomamente alla copertura dei costi derivanti dalle attività svolte, con forme di autofinanziamento basate sulle contribuzioni dovute dai soggetti vigilati. Con riferimento all'Agenzia per la cybersicurezza nazionale, le attività disciplinate dallo schema di decreto sono svolte nell'ambito delle funzioni istituzionali dell'Agenzia con risorse umane, strumentali e finanziarie disponibili a legislazione vigente e non determinano nuovi oneri per la finanza pubblica.

4.2 Impatti specifici

A. Effetti sulle PMI (Test PMI)

Per quanto concerne, in particolare, i dati e, quindi, i termini numerici degli impatti sulle PMI derivanti dal presente intervento normativo, si rileva che sarà possibile dar conto di tali elementi solo *ex post*, una volta che le misure di attuazione saranno entrate in vigore ed avranno esplicato i loro effetti.

Si segnala, a tale riguardo, che il regolamento DORA prevede un regime semplificato per talune entità finanziarie che si qualifichino come microimprese (in quanto occupino meno di 10 dipendenti e realizzino un fatturato annuo e/o totale di bilancio annuo non superiore a 2 milioni di euro) e non si applica a intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio che sono microimprese o piccole o medie imprese, dovendosi considerare «piccola impresa» ogni entità finanziaria che occupi 10 o più persone ma meno di 50 persone e realizzi un fatturato annuo e/o un totale di bilancio annuo che supera 2 milioni di euro, ma non superiore a 10 milioni di euro e «media impresa» ogni entità finanziaria che non è una piccola impresa, occupa meno di 250 persone e realizza un fatturato annuo non superiore a 50 milioni di euro e/o un bilancio annuo non superiore a 43 milioni di euro.

B. Effetti sulla concorrenza

Con il presente intervento normativo non sono previsti obblighi ulteriori atti a creare svantaggi concorrenziali per le imprese italiane. Di converso, il rafforzamento della resilienza operativa digitale delle entità finanziarie, in linea con le previsioni stabilite a livello europeo, potrà generare un positivo effetto pro-concorrenziale.

C. Oneri informativi

Il provvedimento normativo in esame allinea l'ordinamento nazionale a quanto previsto dal regolamento DORA, il quale, per consentire alle autorità competenti di assolvere alle funzioni di vigilanza, acquisendo un panorama completo di natura, frequenza, rilevanza e impatto degli incidenti connessi alle TIC, introduce un regime di segnalazione dei medesimi incidenti. In base a tale regime, è richiesto a tutte le entità finanziarie di riferire alle rispettive autorità competenti, con un meccanismo funzionale a eliminare o ridurre le sovrapposizioni e le duplicazioni esistenti in modo da diminuire gli oneri informativi a carico dei soggetti vigilati e ridurre i costi di *compliance*.

In tale ottica di razionalizzazione e di semplificazione degli oneri informativi applicabili, coerentemente con quanto previsto dal nuovo quadro europeo, il provvedimento in esame identifica le autorità competenti a ricevere le segnalazioni degli incidenti e le notifiche volontarie delle minacce significative, istituendo dei meccanismi di scambio informativo tra le Autorità in caso di intermediari co-vigilati, ed estende le disposizioni del regolamento DORA in materia di incidenti TIC anche agli intermediari finanziari e Bancoposta.

D. Rispetto dei livelli minimi di regolazione europea

Il provvedimento normativo in esame non prevede l'introduzione o il mantenimento di livelli di regolazione superiori a quelli richiesti dal regolamento DORA e dalla direttiva DORA.

L'introduzione di una disciplina sulla resilienza operativa digitale per soggetti non ricompresi nell'ambito di applicazione della disciplina DORA (intermediari finanziari e a Bancoposta) discende dalla legge di delegazione europea 2022-2023, che ha delegato il Governo ad apportare alla disciplina applicabile agli intermediari finanziari e a Bancoposta le occorrenti modifiche e integrazioni, per conseguire un livello elevato di resilienza operativa digitale e assicurare la stabilità del settore finanziario nel suo complesso, in particolare, assicurando presidi equivalenti a quelli previsti dal regolamento DORA per gli altri soggetti vigilati.

4.3 Motivazione dell'opzione preferita

Le scelte regolatorie contenute nel provvedimento normativo in esame derivano dalla necessità di adeguare l'ordinamento nazionale a quanto previsto dal regolamento DORA e di recepire la direttiva DORA, nonché di prevedere una disciplina equivalente a quella dettata da DORA per intermediari finanziari e Bancoposta, secondo i principi e criteri direttivi declinati nella delega di cui all'articolo 16 della legge di delegazione europea 2022-2023.

Per realizzare quanto sopra, è necessario effettuare un intervento sull'ordinamento nazionale di adeguamento e di riforma al fine di introdurre norme tese a 1) recepire le previsioni della direttiva DORA che necessitano di una trasposizione a livello di normativa primaria; 2) attribuire alle autorità competenti i necessari poteri di vigilanza, di indagine e sanzionatori, secondo quanto previsto dal regolamento DORA; 3) definire un quadro per la cooperazione tra le autorità DORA e tra queste ultime e l'Agenzia per la cybersicurezza nazionale per il coordinamento con la disciplina attuativa della NIS2 per i settori del credito e delle infrastrutture del mercato finanziario (rispetto alla quale il regolamento DORA costituisce *lex specialis*); 4) prevedere una disciplina nazionale di resilienza operativa digitale per gli intermediari finanziari e Bancoposta equivalente a quella dettata da DORA.

L'intervento sub 1) è realizzato al Capo V apportando le necessarie modifiche ai decreti legislativi 24 febbraio 1998, n. 58, 9 settembre 2005, n. 209, 5 dicembre 2005, n. 252, 16 novembre 2015, n. 180. Ulteriori interventi funzionali all'attuazione delle modifiche apportate dalla direttiva DORA alla normativa di settore saranno effettuati dalla Autorità di vigilanza competenti (Banca d'Italia, Consob, IVASS e Covip) in sede di normativa secondaria, esercitando potestà regolamentari a esse già attribuite in virtù dell'ordinamento di settore.

Gli interventi sub 2) e 3) sono realizzati introducendo *ex novo* delle disposizioni normative (Capi II e IV), ferma la possibilità di effettuare ulteriori interventi a livello secondario anche per tener conto degli orientamenti delle Autorità europee di vigilanza, nonché per dettare le disposizioni riguardanti le modalità di esercizio dei poteri di vigilanza, in virtù della potestà regolamentare di cui all'articolo 9 del decreto in esame, che attribuisce alle autorità competenti DORA il potere, nell'ambito delle rispettive competenze, di emanare disposizioni attuative del decreto nonché del regolamento DORA.

Per quanto concerne gli intermediari finanziari e Bancoposta, le scelte regolatorie contenute nel Capo III del decreto in esame sono state adottate in stretta aderenza a quanto previsto dal criterio di cui all'articolo 16, comma 2, lettera *c-bis*), della legge di delegazione europea 2022-2023, che ha delegato specificamente il Governo a definire presidi in materia di resilienza operativa digitale equivalenti a quelli stabiliti nel regolamento DORA. È stato, altresì, richiesto al Governo di tener conto, nella definizione dei presidi, del principio di proporzionalità: tale principio è stato valorizzato prevedendo una disciplina modulare per gli intermediari finanziari (cfr. *sub* §3) e prevedendo un'applicazione differita delle medesime disposizioni.

5. MODALITÀ DI ATTUAZIONE E MONITORAGGIO

5.1 Attuazione

Si segnala che non sussistono indicazioni tali da indurre a ritenere che taluni fattori, legati al contesto giuridico o economico, possano comportare un ostacolo all'assolvimento di quanto previsto e allo svolgimento delle attività di cui alle norme in commento. Non si ravvisano, inoltre, fattori prevedibili che potrebbero condizionare o impedire l'attuazione delle nuove norme. L'attuazione delle disposizioni in commento è, in particolare, rimessa alle autorità di vigilanza competenti: Banca d'Italia, Consob, IVASS e COVIP.

5.2 Monitoraggio

L'applicazione delle previsioni del regolamento DORA, ai sensi dell'articolo 58 di tale regolamento, sarà monitorata dalla Commissione europea, che riesaminerà il regolamento entro il 17 gennaio 2028, e presenterà al Parlamento europeo e al Consiglio una relazione accompagnata, se del caso, da una proposta legislativa.

Al livello nazionale, il monitoraggio sull'applicazione del decreto in commento verrà realizzato, secondo le rispettive attribuzioni e riparto di compiti, dalle autorità competenti DORA: Banca d'Italia, Consob, IVASS e COVIP.

6. Consultazioni svolte nel corso dell'AIR

Il presente decreto legislativo è stato elaborato dal Dipartimento del Tesoro previo confronto tecnico con i competenti uffici della Banca d'Italia, della Consob, dell'IVASS e della COVIP, nonché dell'Agenzia per la Cybersicurezza Nazionale.

Lo schema di decreto legislativo non è stato sottoposto a pubblica consultazione, in quanto primariamente strumento per l'adeguamento dell'ordinamento al regolamento DORA per il recepimento della direttiva DORA, atti adottati ad esito di una pubblica consultazione che si è svolta tra il 19 dicembre 2019 e il 19 marzo 2020.

L’esercizio delle opzioni rimesse al legislatore nazionale non è produttivo di impatti significativi sui destinatari della disciplina.

Le scelte normative relative all’introduzione di un regime di resilienza operativa digitale per gli intermediari 106 e Bancoposta sono state effettuate in stretta aderenza al criterio di delega di cui all’articolo 16, comma 2, lett. c-bis della Legge di Delegazione europea 2022-2023.

PERCORSO DI VALUTAZIONE

L’AIR è stata redatta dal Ministero dell’economia e delle finanze – Dipartimento del Tesoro – Direzione V, Ufficio IX – sulla base degli elementi informativi disponibili al momento della redazione.

COMMISSIONE
EUROPEA

Bruxelles, 24.9.2020
SWD(2020) 199 final

DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE

SINTESI DELLA RELAZIONE SULLA VALUTAZIONE D'IMPATTO

che accompagna il documento

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

{COM(2020) 595 final} - {SEC(2020) 307 final} - {SWD(2020) 198 final}

Scheda di sintesi

Valutazione d'impatto sulla proposta di regolamento relativo alla resilienza operativa digitale nel settore finanziario

A. Necessità di intervento

Per quale motivo? Qual è il problema da affrontare?

Il settore finanziario dipende in larga misura dalle tecnologie dell'informazione e della comunicazione (TIC). È probabile che l'attuale pandemia di COVID-19 acceleri tale processo, dati i benefici derivanti dalla possibilità di accedere costantemente da remoto ai servizi finanziari. La dipendenza dalle tecnologie digitali desta tuttavia preoccupazione; le imprese devono essere in grado di resistere a potenziali perturbazioni delle TIC in modo da affrontare gli incidenti e le minacce digitali e continuare a erogare i servizi. In un settore finanziario altamente interconnesso che fornisce servizi transfrontalieri vitali da cui dipende l'economia reale, le vulnerabilità derivanti dalla dipendenza dalle TIC, che pure riguardano tutti i settori economici, sono particolarmente pronunciate a causa: 1) dell'uso ampio e radicato delle TIC e 2) della possibilità che gli effetti di un incidente operativo in un'impresa o in un sottosettore finanziario si propaghino rapidamente ad altre imprese o parti del settore finanziario e, infine, al resto dell'economia.

Sebbene il settore finanziario sia molto avanzato nell'integrazione normativa e di mercato e debba la sua prosperità a un unico insieme di norme armonizzate, il codice unico dell'UE, la risposta dell'UE alle crescenti esigenze di resilienza operativa a livello orizzontale e settoriale:

- si è basata su un'armonizzazione minima, lasciando così spazio alle interpretazioni nazionali e alla frammentazione nel mercato unico, oppure
- è stata troppo generica e ha avuto un'applicazione limitata, per cui ha affrontato il rischio operativo generale in misura variabile, regolamentando parzialmente alcune componenti della *resilienza* operativa digitale (ad esempio la gestione dei rischi relativi alle TIC, la segnalazione degli incidenti e i rischi relativi alle TIC derivanti da terzi) ma trascurandone altre (test).

Finora l'intervento dell'UE non ha affrontato il rischio operativo in misura corrispondente alle esigenze delle imprese finanziarie, che devono resistere e reagire alle vulnerabilità delle TIC e riprendersi dai loro effetti, e non fornisce alle autorità di vigilanza finanziaria gli strumenti per adempiere il loro mandato di contenere l'instabilità finanziaria derivante da tali vulnerabilità.

Le attuali lacune e incoerenze hanno provocato la proliferazione di iniziative nazionali (ad esempio in materia di test) e di approcci di vigilanza (ad esempio per quanto riguarda le dipendenze da terzi nel settore delle TIC) non coordinati, dando luogo a sovrapposizioni, duplicazione di requisiti ed elevati costi amministrativi e di conformità per le imprese finanziarie transfrontaliere o impedendo di individuare e affrontare i rischi relativi alle TIC. Nel complesso, la stabilità e l'integrità del settore finanziario non sono garantite e il mercato unico dei servizi finanziari rimane frammentato; di conseguenza la tutela dei consumatori e degli investitori ne risulta compromessa.

Qual è l'obiettivo dell'iniziativa?

L'obiettivo generale consiste nel rafforzare la resilienza operativa digitale del settore finanziario dell'UE, razionalizzando e aggiornando la vigente normativa finanziaria dell'Unione e introducendo nuovi requisiti laddove si riscontrino lacune, allo scopo di:

- migliorare la gestione dei rischi relativi alle TIC da parte delle imprese finanziarie;
- incrementare le conoscenze delle autorità di vigilanza in fatto di minacce e incidenti;
- migliorare i test che le imprese finanziarie effettuano sui propri sistemi di TIC; e
- migliorare la vigilanza sui rischi derivanti dalla dipendenza delle imprese finanziarie da fornitori terzi di TIC.

Più specificamente, la proposta introdurrebbe meccanismi di segnalazione degli incidenti più coerenti e uniformi, riducendo in tal modo gli oneri amministrativi a carico degli enti finanziari e rafforzando l'efficienza della vigilanza.

Qual è il valore aggiunto dell'intervento a livello dell'UE?

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. Le disposizioni vigenti in materia di rischio operativo sono di carattere puramente generale. 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.

B. Soluzioni

Quali opzioni strategiche legislative e di altro tipo sono state prese in considerazione? Ne è stata prescelta una? Per quale motivo?

Riguardo alla normativa dell'UE in materia di servizi finanziari, la valutazione d'impatto ha preso in considerazione tre opzioni, oltre a uno scenario di base che ipotizza l'assenza di interventi. Più specificatamente:

- **"nessun provvedimento"**. Le norme sulla resilienza operativa continuerebbero a fondarsi sull'attuale insieme di disposizioni dell'UE in materia di servizi finanziari (che registra varie divergenze), in parte sulla direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS) e sui regimi nazionali vigenti o futuri;
- **opzione 1 – rafforzamento delle riserve di capitale**. Si introdurrebbe una riserva di capitale aggiuntiva per rafforzare la capacità delle imprese finanziarie di assorbire le perdite che potrebbero verificarsi a causa della mancanza di resilienza operativa;
- **opzione 2 – un atto sulla resilienza operativa digitale dei servizi finanziari**. Si introdurrebbe in tal modo un quadro globale a livello dell'UE che stabilisca norme sulla resilienza operativa digitale per tutti gli enti finanziari regolamentati che
    - affronterebbe in modo più completo i rischi relativi alle TIC;
    - consentirebbe alle autorità di vigilanza finanziaria di accedere alle informazioni relative agli incidenti connessi alle TIC;
    - garantirebbe che le imprese finanziarie valutino l'efficacia delle proprie misure di prevenzione e resilienza e identifichino le vulnerabilità delle TIC;
    - rafforzerebbe le norme in materia di esternalizzazione che disciplinano la sorveglianza indiretta dei fornitori terzi di TIC;
    - consentirebbe una sorveglianza diretta delle attività dei fornitori terzi di TIC quando prestano i loro servizi a imprese finanziarie;
    - inoltre incoraggerebbe lo scambio di dati sulle minacce nel settore finanziario;
- **opzione 3 – atto sulla resilienza unito alla vigilanza centralizzata dei fornitori terzi di servizi di TIC critici**. oltre a introdurre un atto sulla resilienza operativa (opzione 2) verrebbe istituita una nuova autorità incaricata di vigilare sui fornitori terzi che erogano servizi di TIC critici alle imprese finanziarie. Ciò distinguerebbe anche più chiaramente il settore finanziario dall'ambito di applicazione della direttiva NIS.

È stata preferita l'opzione 2. Rispetto alle altre opzioni, questa realizza la maggioranza degli obiettivi dell'iniziativa, tenendo conto dei criteri di efficienza e coerenza. Quest'opzione riscuote inoltre il sostegno più vasto tra i portatori di interessi.

Chi sono i sostenitori delle varie opzioni?

La maggior parte dei portatori di interessi (privati, pubblici) concorda sulla necessità di un'azione dell'UE per salvaguardare più efficacemente la resilienza operativa delle imprese finanziarie. Inoltre molti ritengono necessaria l'azione dell'UE per affrontare gli oneri normativi derivanti dal fatto che le imprese finanziarie sono soggette a norme duplicate e incoerenti stabilite dalla direttiva NIS, dalla normativa dell'UE sui servizi finanziari e dai regimi nazionali (ad esempio per quanto riguarda la segnalazione degli incidenti). Di conseguenza pochi portatori di interessi sono favorevoli ad astenersi dall'intervenire. Pochi portatori di interessi ritengono opportuno salvaguardare la resilienza operativa tramite l'aumento delle riserve di capitale (opzione 1). Questo è tuttavia l'approccio tradizionale al rischio operativo, in particolare nel settore bancario, e pertanto è preso in considerazione, ad esempio, dagli organismi internazionali di normazione. Ampio sostegno tra i portatori di interesse che hanno risposto alla consultazione pubblica riscuote il tipo di misure qualitative previste dall'opzione 2, che razionalizzerebbero e aggiornerebbero la normativa finanziaria dell'UE e introdurrebbero nuovi requisiti laddove esistano lacune, mantenendo allo stesso tempo i collegamenti con la direttiva NIS a carattere orizzontale. Mentre alcuni portatori di interessi (in particolare quelli pubblici) ritengono opportuno rafforzare la vigilanza sui fornitori terzi di TIC, come prevede l'opzione 3, l'istituzione a tale scopo di una nuova autorità dell'UE incontra solo un limitato favore tra i portatori di interessi, al pari della discontinuità più netta rispetto al quadro della direttiva NIS.

C. Impatto dell'opzione prescelta

Quali sono i vantaggi dell'opzione prescelta (o in mancanza di quest'ultima, delle opzioni principali)?

L'opzione 2 affronterebbe i **rischi relativi alle TIC** in tutto il settore finanziario, rafforzando la capacità degli enti finanziari di resistere agli incidenti connessi alle TIC. Diminuirebbe così il rischio che un incidente informatico si propaghi rapidamente sui mercati finanziari. Sebbene sia difficile stimare i costi degli incidenti operativi nel settore finanziario (non tutti gli incidenti sono segnalati e l'entità dei costi è incerta), le valutazioni del settore indicano che i costi per il settore finanziario dell'UE potrebbero oscillare tra i 2 e i 27 miliardi di EUR all'anno. L'opzione prescelta ridurrebbe questi 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 gli oneri amministrativi. Per alcune delle maggiori banche, ad esempio, i relativi risparmi potrebbero oscillare tra i 40 e i 100 milioni di EUR all'anno. La segnalazione diretta amplierebbe anche le conoscenze delle autorità di vigilanza in merito agli incidenti connessi alle TIC. **L'armonizzazione delle pratiche in materia di test** renderebbe più facile individuare vulnerabilità e rischi sconosciuti. Diminuirebbe anche i costi, in particolare per le imprese transfrontaliere. Ad esempio, per le 44 maggiori banche transfrontaliere, i benefici complessivi attesi da un approccio comune ai test potrebbero oscillare tra gli 11 e gli 88 milioni di EUR. 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, aspetto apprezzabile per le autorità di vigilanza. Vi sarebbero inoltre benefici prudenziali derivanti dalla vigilanza sui fornitori terzi di TIC da parte delle autorità preposte. Nel complesso l'opzione prescelta si traduce in 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.

Quali sono i costi dell'opzione prescelta (o in mancanza di quest'ultima, delle opzioni principali)?

L'opzione prescelta comporterebbe costi sia una tantum che ricorrenti. I primi dipendono dagli investimenti in sistemi informatici e sono difficili da quantificare, data la diversa situazione dei sistemi preesistenti delle imprese. In assenza di intervento normativo, alcune imprese finanziarie hanno già effettuato cospicui investimenti nei sistemi di TIC. Di conseguenza, per le grandi imprese finanziarie il costo delle misure contenute nella presente 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 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. Anche le autorità di vigilanza dovrebbero sostenere alcuni costi a causa dei compiti supplementari che sarebbero chiamate a svolgere. Ad esempio, per le autorità di vigilanza che partecipano direttamente alla vigilanza sui fornitori terzi di TIC, l'incremento stimato in termini di dipendenti a tempo pieno potrebbe collocarsi tra 1 e 5 per l'autorità capofila e intorno a 0,25 per le autorità partecipanti.

Quale sarà l'incidenza su aziende, PMI e microimprese?

L'opzione prescelta 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. Tuttavia, nel definire i requisiti fondamentali nei principali settori di intervento, il principio di proporzionalità si applicherebbe sia all'insieme dei sottosettori che in seno a ciascun sottosettore, tenendo conto, tra l'altro, delle differenze a livello di modelli d'impresa, dimensioni, profili di rischio, importanza sistemica, ecc. Ad esempio, le misure in materia di segnalazione degli incidenti e i test sarebbero meno rigorose per le imprese finanziarie più piccole.

L'impatto sulle amministrazioni e sui bilanci nazionali sarà significativo?

No. Come illustrato in precedenza, la sorveglianza supplementare può comportare un certo incremento delle risorse di vigilanza, che tuttavia può andare a carico in tutto o in parte (nel caso di commissioni di vigilanza) dei bilanci pubblici.

Sono previsti altri impatti significativi?

Le conseguenze socioeconomiche della pandemia di COVID-19 sottolineano l'importanza cruciale dei mercati finanziari digitali e della loro resilienza operativa. L'opzione prescelta costituirebbe una solida base per cogliere i vantaggi della trasformazione digitale garantendo la resilienza operativa del mercato unico dei servizi finanziari, comprese le unioni bancarie e dei mercati dei capitali, sulla base di un insieme comune di norme e requisiti che mirano a garantire sicurezza, prestazioni, stabilità e parità di condizioni. Ne sarà rafforzata anche la leadership finanziaria e digitale dell'Europa, obiettivo indicato dalla Commissione nella comunicazione "Plasmare il futuro digitale dell'Europa".

D. Tappe successive
Quando saranno riesaminate le misure proposte?
Il primo riesame avverrebbe tre anni dopo l'entrata in vigore dello strumento giuridico. La Commissione presenterebbe al Parlamento europeo e al Consiglio una relazione sul riesame. Se del caso, il riesame potrebbe essere supportato da una consultazione pubblica, nonché da studi, discussioni tra esperti, indagini e seminari.