dossier

XIX Legislatura

Gennaio 2025

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

Atto del Governo n. 242

Senato della Repubblica

Camera dei deputati

SERVIZIO DEL BILANCIO
Tel. 06 6706 5790 – ✉ SBilancioCU@senato.it – 𝕏 @SR_Bilancio
Nota di lettura n. 220

SERVIZIO BILANCIO DELLO STATO
Tel. 06 6760 2174 / 9455 – ✉ bs_segreteria@camera.it
Verifica delle quantificazioni n. 296

La redazione del presente dossier è stata curata dal Servizio del bilancio del Senato della Repubblica.

I N D I C E

INFORMAZIONI SUL PROVVEDIMENTO

Natura dell'atto:	Schema di decreto legislativo	
Atto del Governo n.	242	
Titolo breve:	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	
Riferimento normativo:	Articoli 1 e 16 della legge 21 febbraio 2024, n. 15	
Relazione tecnica (RT):	Presente	
	Senato	**Camera**
Commissione competente:	**6ª** Commissione permanente (Finanze e tesoro) in sede *consultiva*. **4ª** Commissione permanente (Politiche dell'Unione europea) e **5ª** Commissione permanente (Bilancio) in sede *osservazioni*.	Assegnazione primaria: VI Finanze Deliberazione di rilievi: V Bilancio e Tesoro Esame per i profili di compatibilità normativa UE: XIV Politiche dell'Unione Europea

PREMESSA

L’atto del Governo n 242 contiene lo schema di decreto legislativo recante disposizioni per l’adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/2554 (c.d. DORA, *Digital Operational Resilience Act*), relativo alla resilienza operativa digitale per il settore finanziario e per il recepimento della direttiva (UE) 2022/2556 sempre per quanto riguarda la resilienza operativa digitale per il settore finanziario.

I principi di delega per l’attuazione del regolamento (UE) 2022/2554 e per il recepimento della direttiva (UE) 2022/2556 sono indicati all’articolo 16 della legge n. 15 del 2024 (legge di delegazione europea 2022-2023). Il comma 3 dell’articolo prevede che dal recepimento della normativa UE non debbano derivare nuovi o maggiori oneri a carico della finanza pubblica e che le amministrazioni competenti provvedono all'adempimento dei compiti derivanti dall'esercizio delle deleghe previste con le risorse umane, strumentali e finanziarie già disponibili a legislazione vigente.

L’articolo 1, comma 3, della legge di delegazione europea 2022-2023 prevede che eventuali spese non contemplate da leggi vigenti e che non riguardano l'attività ordinaria delle amministrazioni statali o regionali possono essere previste nei decreti legislativi nei soli limiti occorrenti per l'adempimento degli obblighi derivanti dall'esercizio delle deleghe. Alla relativa copertura, nonché alla copertura delle minori entrate eventualmente derivanti dall'attuazione delle deleghe, laddove non sia possibile farvi fronte con i fondi già assegnati alle competenti amministrazioni, si provvede mediante riduzione dell’apposito fondo per il recepimento della normativa europea di cui all'articolo 41-*bis* della legge n. 234 del 2012; qualora la dotazione del fondo si rivelasse insufficiente, i decreti legislativi dai quali derivino nuovi o maggiori oneri possono

essere emanati solo successivamente all'entrata in vigore dei provvedimenti legislativi che stanziano le occorrenti risorse finanziarie, in conformità all'articolo 17, comma 2, della legge 31 dicembre 2009, n. 196.

CAPO I
DISPOSIZIONI GENERALI

Articoli 1 e 2
(*Definizioni (Art.1); Oggetto e ambito di applicazione (Art. 2)*)

L'articolo 1 reca le definizioni di alcuni termini utilizzati nello schema di decreto in esame.

Si stabilisce che, ai fini dell'interpretazione del decreto in esame, valgono le definizioni contenute nell'articolo 2, paragrafo 2, e 3 del Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022 (cosiddetto regolamento DORA).

Inoltre, vengono definite come Autorità nazionale competente NIS l'Agenzia per la cybersicurezza nazionale, quale autorità nazionale unica competente in materia di sicurezza delle reti e dei sistemi informativi, e come CSIRT Italia il Gruppo nazionale di risposta agli incidenti di sicurezza informatica operante presso l'Agenzia di cybersicurezza nazionale.

In via generale, si stabilisce che per quanto non diversamente previsto dal presente articolo, si applicano le definizioni del TUB, del TUF, del CAP e del decreto legislativo 5 dicembre 2005, n. 252.

L'articolo 2 definisce l'oggetto e l'ambito di applicazione del decreto, disponendo che le norme del medesimo dettino le disposizioni necessarie all'adeguamento del quadro normativo nazionale al regolamento DORA, al recepimento della direttiva DORA, nonché al coordinamento con altre disposizioni settoriali.

La RT evidenzia che le norme del Capo I contengono «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.

Assicura che tutte le disposizioni del Capo I hanno carattere ordinamentale e, comunque, non comportano nuovi o maggiori oneri per la finanza pubblica.

Al riguardo, ritenuto il carattere ordinamentale delle disposizioni in esame, non ci sono osservazioni.

CAPO II
AUTORITÀ COMPETENTI E COOPERAZIONE

Articolo 3
(*Autorità competenti DORA e partecipazione al forum di sorveglianza*)

L'articolo indica la Banca d'Italia, la Consob, l'IVASS e la COVIP quali Autorità competenti per il rispetto degli obblighi posti dal regolamento DORA a carico dei soggetti vigilati e ne definisce il ruolo nella partecipazione al forum di sorveglianza.

La RT ricorda che l'articolo 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»).

Rileva che in linea con la vigente ripartizione di competenze in materia di vigilanza, l'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.

Con riferimento a tutte le disposizioni di cui al Capo II, 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, assicura che le Autorità sopra indicate provvedono all'attuazione dei compiti di cui al Capo II dello schema di decreto in esame con le sole risorse umane, strumentali e finanziarie disponibili a legislazione vigente, e comunque senza nuovi o maggiori oneri a carico della finanza pubblica.

Al riguardo, per i profili di quantificazione, posto che le Autorità di vigilanza richiamate dalle disposizioni, compresa la Banca d'Italia, non rientrano nell'elenco delle Pubbliche Amministrazioni ai fini del consolidamento del conto economico della PA, non ci sono osservazioni.

Articolo 4
(*Segnalazione dei gravi incidenti TIC e notifica volontaria delle minacce informatiche significative*)

L'articolo reca disposizioni concernenti le segnalazioni dei gravi incidenti TIC (tecnologie dell'informazione e della comunicazione) e le notifiche volontarie delle minacce informatiche significative. Nello specifico, per ogni tipologia di entità finanziaria soggetta al regolamento DORA,

nonché per Bancoposta e per gli intermediari finanziari, viene individuata l'Autorità competente destinataria di tali segnalazioni e notifiche (commi 1 e 2).

Il comma 3 stabilisce che le entità finanziarie del settore bancario e delle infrastrutture dei mercati finanziari di cui all'allegato I della direttiva (UE) 2022/2555 (c.d. NIS 2), nonché i soggetti appartenenti al settore bancario e delle infrastrutture dei mercati finanziari identificati come critici ai sensi della direttiva (UE) 2022/2557, forniscono la notifica iniziale dei gravi incidenti TIC e ciascuna delle suddette relazioni anche a CSIRT Italia, sulla base dei modelli e nel rispetto dei termini definiti dall'articolo 20 del regolamento DORA. Si specifica, altresì, che tali informazioni trasmesse a CSIRT Italia siano coperte dal segreto d'ufficio.

Il comma 4 dispone che le entità finanziarie che provvedono alla notifica su base volontaria delle minacce informatiche significative possono trasmettere la notifica anche a CSIRT Italia. Tali informazioni trasmesse a CSIRT Italia siano coperte dal segreto d'ufficio.

Il comma 5 prevede, con riferimento alle sedi di negoziazione all'ingrosso di titoli di Stato, che la Banca d'Italia invii anche al Ministero dell'economia e delle finanze, contestualmente alla trasmissione alla Consob, la notifica iniziale, le relazioni sui gravi incidenti TIC, nonché le notifiche volontarie relative alle minacce informatiche significative.

La RT conferma che l'articolo 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 trasmetta 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 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, mentre 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.

Al riguardo, per quanto riguarda l'eventuale coinvolgimento nelle segnalazioni degli incidenti TIC anche del CSIRT Italia, istituito presso l'Agenzia per la cybersicurezza nazionale[1], poiché tale soggetto rientra nell'ambito delle pubbliche amministrazioni a fini di contabilità nazionale andrebbe assicurato che questi possa svolgere gli adempimenti amministrativi connessi alla trattazione e alla custodia delle informazioni

[1] I compiti del CSIRT sono definiti dal decreto legislativo 18 maggio 2018, n. 65, e dal decreto del Presidente del Consiglio dei ministri 8 agosto 2019, articolo 4.

ricevute previsti dalla norma avvalendosi delle sole risorse umane, finanziarie e strumentali già previste ai sensi della legislazione vigente[2].

Articolo 5
(*Protocolli d'intesa e scambio di informazioni*)

L'articolo reca disposizioni in materia di cooperazione e scambio di informazioni. In particolare, viene disciplina la cooperazione tra Autorità competenti DORA e le strutture e le autorità competenti istituite a norma della direttiva (UE) 2022/2555 (c.d. NIS 2), e, in particolare, con l'Agenzia per la cybersicurezza nazionale (ACN) e il Corpo della Guardia di finanza, attraverso forme di coordinamento operativo e informativo regolate da uno o più protocolli d'intesa. Tali protocolli hanno il fine di regolare lo scambio di informazioni, istituire forme di consulenza e assistenza tecnica reciproca e meccanismi di coordinamento e risposta rapida nel caso di incidenti e, per quanto riguarda la Guardia di finanza, di prevenzione, accertamento e repressione degli illeciti.

Le informazioni (su minacce, vulnerabilità e incidenti informatici) acquisite dall'Agenzia per la cybersicurezza nazionale, anche in forza dei sopra citati protocolli di intesa, sono trasmesse agli organismi di informazione per la sicurezza istituiti con legge n. 124 del 2007 affinché questi ultimi possano adempiere alle loro finalità istituzionali. Siffatta trasmissione avviene sulla base di apposita intesa conclusa tra gli stessi organismi e l'Agenzia per la cybersicurezza nazionale.

L'Agenzia per la cybersicurezza nazionale è tenuta a informare, senza indebito ritardo, le Autorità competenti DORA, nell'eventualità in cui, in sede di vigilanza o di esecuzione, venga a conoscenza di una violazione degli obblighi di segnalazione di cui all'articolo 4 del decreto in esame da parte di un'entità finanziaria.

La RT evidenzia che l'articolo 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.

Dalla prevista 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, atteso il carattere ordinamentale della disposizione, non derivano nuovi o maggiori oneri a carico della finanza pubblica.

---

[2] Sul punto, in sede di prima applicazione del decreto-legge n. 82/2021 è stato previsto che la dotazione organica dell'Agenzia fosse contenuta nel limite di trecento unità, di cui n. 12 di livello dirigenziale generale e n. 40 di livello dirigenziale. Lo stanziamento annuale per l'Agenzia, previsto a legislazione vigente è il seguente: euro 102.637.500 per l'anno 2025; euro 112.637.500 per l'anno 2026; euro 124.637.500 a decorrere dall'anno 2027.

Quanto alle disposizioni che prevedono mirate forme di raccordo informativo tra le autorità competenti DORA e la Guardia di finanza, evidenzia che 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, 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».

Pertanto, alla luce di tali considerazioni, la RT assicura che 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.

Quindi, conclude riferendo che 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.

Al riguardo, circa la prevista condivisione delle informazioni utili all'esercizio delle funzioni di vigilanza delle Autorità competenti DORA, ivi incluse le informazioni sui gravi incidenti TIC, e l'Agenzia di cybersicurezza nazionale (quest'ultima rientrante nel novero delle Amministrazioni pubbliche ai fini della contabilità nazionale), andrebbe confermato che tale Agenzia potrà stipulare i previsti protocolli con le Autorità competenti DORA avvalendosi delle sole risorse umane, finanziarie e strumentali previste in bilancio ai sensi della legislazione vigente o eventualmente concordando con le stesse Autorità specifiche forme di rimborso per le eventuali spese aggiuntive da sostenersi per le istruttorie inerenti allo scambio di informazioni[3].

Riguardo agli elementi informativi forniti secondo cui il coinvolgimento della Guardia di finanza non amplierebbe i settori di competenza di tale soggetto, si conviene con la RT in merito all'assenza di nuovi o maggiori oneri finanziari; sarebbero comunque utili maggiori ragguagli idonei a confermare l'adeguatezza delle risorse umane, finanziarie e strumentali attualmente a disposizione del citato Corpo[4].

Sul comma 3, che prevede che le informazioni (su minacce, vulnerabilità e incidenti informatici) acquisite dall'Agenzia per la cybersicurezza nazionale, anche in forza di protocolli di intesa, debbano comunque essere trasmesse agli organismi di informazione per la sicurezza istituiti con la legge n. 124 del 2007 (DIS, AISE e AISI), affinché questi ultimi possano adempiere alle loro finalità istituzionali sulla base di apposita intesa conclusa tra gli stessi organismi e l'Agenzia per la cybersicurezza nazionale, andrebbero fornite rassicurazioni sulla capacità di detti soggetti di svolgere tali attività avvalendosi delle sole risorse già previste dalla legislazione vigente[5].

---

[3] Si segnala che esiste già un protocollo d'intesa per lo scambio informativo e la cooperazione per la protezione delle minacce *cyber* tra ACN e Banca d'Italia, siglato il 22 dicembre 2022.

[4] La Guardia di finanza, a marzo 2024, disponeva di una forza organica di 63.885 militari delle varie categorie e ruoli (ufficiali, marescialli, brigadieri, appuntati e finanzieri). Le dotazioni organiche risultavano così suddivise: 3.325 ufficiali; 27.747 marescialli; 10.000 brigadieri; 22.813 appuntati e finanzieri.

[5] Gli organi del sistema di informazione e sicurezza nazionale non sono contemplati nell'elenco delle PA consolidate nel comparto S13 ai fini del consolidamento del conto economico della PA. La relativa dotazione finanziaria annuale relativa alla copertura dei loro fabbisogni di funzionamento è iscritta nello stato di previsione del Ministero dell'economia e delle finanze del bilancio 2025-2027 (cap.1670, per cui sono stanziati 1,2 miliardi di euro annui per il triennio 2025-2027).

CAPO III
DISPOSIZIONI APPLICABILI A INTERMEDIARI FINANZIARI E BANCOPOSTA

Articoli 6 e 7
(*Disposizioni applicabili agli intermediari finanziari (Art. 6); Disposizioni applicabili a Bancoposta (Art. 7)*)

L'articolo 6 individua le disposizioni del regolamento (UE) 2022/2554 applicabili agli intermediari finanziari iscritti all'albo di cui all'articolo 106 del TUB.

L'articolo 7 individua le disposizioni dello stesso regolamento applicabili a Bancoposta. In ossequio al principio di proporzionalità richiamato nei criteri di delega, si rende applicabile la medesima disciplina applicata per le banche.

La RT rileva che 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 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, la 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.

Al riguardo, non ci sono osservazioni.

CAPO IV
POTERI DI VIGILANZA E SANZIONI

Articoli 8 e 9
(*Poteri di vigilanza (art.8)*)
(*Poteri regolamentari (art. 9)*)

L'articolo 8 disciplina i poteri di vigilanza e di indagine che le Autorità competenti DORA possono espletare nei confronti delle entità finanziarie e dei fornitori terzi di servizi TIC a supporto di funzioni essenziali o importanti, nonché le attività di accesso e ispezione che tali Autorità possono porre in essere nei confronti dei medesimi soggetti, ai fini dell'esercizio dei poteri suddetti.

In particolare, il comma 1 attribuisce alle Autorità competenti DORA, secondo le rispettive competenze, i poteri di vigilanza di cui agli articoli 50, paragrafo 2, e 42, paragrafo 6, del regolamento DORA.

I poteri di cui al comma 1 includono almeno i poteri seguenti: a) l'avere accesso a qualsiasi documento o dato, detenuto in qualsiasi forma, che l'autorità competente consideri pertinente per lo

svolgimento dei propri compiti e la possibilità di riceverne o farne una copia; b) lo svolgere ispezioni o indagini *in loco* comprendenti tra l'altro: la convocazione di rappresentanti delle entità finanziarie per ottenere spiegazioni scritte od orali su fatti o documenti relativi all'oggetto e alle finalità dell'indagine e registrarne le risposte; l'audizione di persone fisiche o giuridiche consenzienti allo scopo di raccogliere informazioni pertinenti all'oggetto dell'indagine; c) il richiedere l'applicazione di misure correttive e di riparazione per le violazioni dei requisiti del regolamento.

Inoltre le autorità competenti possono adottare, come misura di ultima istanza, a seguito della notifica e, se del caso, della consultazione con le autorità competenti designate o istituite in conformità della direttiva (UE) 2022/2555 responsabili della vigilanza, una decisione che impone alle entità finanziarie di sospendere temporaneamente, in tutto o in parte, l'utilizzo o l'introduzione di un servizio prestato dal fornitore terzo critico di servizi TIC, fino a quando non siano stati affrontati i rischi identificati nelle raccomandazioni trasmesse ai fornitori terzi critici di servizi TIC. Laddove si renda necessario, le autorità competenti possono chiedere alle entità finanziarie di risolvere, in tutto o in parte, gli accordi contrattuali pertinenti stipulati con i fornitori terzi critici di servizi TIC.

Il comma 2 prevede che le Autorità competenti DORA, ai fini dell'esercizio dei poteri di cui sopra, possano effettuare accessi e ispezioni presso i fornitori terzi di servizi TIC a supporto di funzioni essenziali o importanti delle entità finanziarie, di Cassa depositi e prestiti S.p.A., degli intermediari finanziari e di Bancoposta, 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 prevede che le Autorità competenti DORA possano emanare, nell'ambito delle rispettive competenze, disposizioni attuative del decreto in esame e del regolamento DORA, anche al fine di considerare gli orientamenti delle Autorità europee di vigilanza, nonché le disposizioni riguardanti le modalità di esercizio dei poteri di vigilanza.

La RT evidenzia all'articolo 8 che il comma 1 definisce 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.

Sul 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.

Conferma che 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.

Al riguardo, nulla da osservare, posto che le Autorità competenti Dora non rientrano tra le pubbliche amministrazioni.

Articolo 10
(*Sanzioni amministrative e altre misure*)

L'articolo 10 reca modifiche al testo unico delle leggi in materia bancaria e creditizia (comma 1), al testo unico delle disposizioni in materia di intermediazione finanziaria (comma 2), al codice delle assicurazioni private (comma 3), al decreto legislativo n. 252 del 2005 recante le disciplina delle forme

pensionistiche complementari (comma 4) e al decreto legislativo n. 129 del 2024 in materia di cripto-attività (comma 5), al fine di stabilire le sanzioni amministrative pecuniarie applicabili per l'inosservanza di disposizioni del regolamento DORA e delle relative norme tecniche di regolamentazione e attuazione. Le disposizioni in esame fissano i limiti edittali delle sanzioni applicabili nei confronti delle persone giuridiche, nonché delle persone fisiche che svolgono funzioni di amministrazione, direzione o controllo e del personale delle società e degli enti nei confronti dei quali sono accertate le violazioni. Si prevede, altresì, la possibilità di applicare la sanzione amministrativa accessoria dell'interdizione, per un periodo non inferiore a sei mesi e non superiore a tre anni, in considerazione della gravità della violazione.

Il comma 6 prevede che, laddove le violazioni di cui al presente articolo siano connotate da scarsa offensività o pericolosità, possa essere disposta l'applicazione di misure previste dall'articolo 50, paragrafo 4, lettere a) ed e), del regolamento DORA in luogo dell'irrogazione delle sanzioni amministrative pecuniarie. Si tratta dell'emanazione di un ordine che imponga alla persona fisica o giuridica di porre termine al comportamento in violazione del presente regolamento e di astenersi dal ripeterlo; nonché della pubblicazione di comunicazioni pubbliche, comprese dichiarazioni pubbliche, indicanti l'identità della persona fisica o giuridica e la natura della violazione.

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.

La RT evidenzia che 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, 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.

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*, secondo cui «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.

Al riguardo, per i profili di quantificazione, posto che le disposizioni in esame prevedono sanzioni pecuniarie di nuova istituzione e che i proventi da esse derivanti, trattandosi di eventuali entrate extratributarie, sono versati al bilancio dello Stato, non ci sono osservazioni.

CAPO V
ULTERIORI MODIFICAZIONI E INTEGRAZIONI DELLA NORMATIVA DI SETTORE E DISPOSIZIONI DI COORDINAMENTO

Articoli 11-15
(*Modifiche al testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58 (Art. 11);Modifica al codice delle assicurazioni private, di cui al decreto legislativo 7 settembre 2005, n. 209 (Art. 12); Modifica al decreto legislativo 5 dicembre 2005, n. 252 (Art. 13); Modifiche al decreto legislativo 16 novembre 2015, n. 180 (Art. 14); Disposizioni di coordinamento con il decreto legislativo 4 settembre 2024, n. 138 (Art. 15)*)

L'articolo 11 prevede l'adozione da parte dei mercati regolamentati di misure idonee a gestire i rischi cui sono esposti - in primo luogo di natura informatica - e a gestirli, eventualmente attenuando i loro effetti.

L'articolo 12 interessa le misure adottate dalle imprese assicurative private per garantire la continuità e la regolarità dell'attività esercitata, compresi i piani di emergenza.

L'articolo 13 riformula la disciplina sull'adozione di alcune misure di garanzia da parte dei fondi pensione, idonee a garantire la continuità e la regolarità dei medesimi; tale disciplina concerne i fondi pensione aventi soggettività giuridica, in quanto persone giuridiche o in quanto associazioni non riconosciute ma distinte dai soggetti promotori dell'iniziativa. La novella specifica che tra le suddette misure di garanzia rientrano l'istituzione e la gestione di sistemi informatici e di rete conformemente al regolamento (UE) 2022/2554, ove applicabile.

L'articolo 14 apporta modifiche al decreto legislativo 16 novembre 2015, n. 180, che istituisce un quadro di risanamento e risoluzione degli enti creditizi e delle imprese di investimento, necessarie a seguito dell'attuazione nell'ordinamento nazionale del regolamento (UE) 2022/2554, recante disposizioni relative alla resilienza operativa digitale per il settore finanziario. Si prevede che i piani di risoluzione debbano dimostrare 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 resilienza operativa digitale in caso di dissesto della banca e contengano una descrizione delle operazioni e dei sistemi essenziali per assicurare la continuità del funzionamento dei sistemi informatici di cui al regolamento 2022/2254. Inoltre, si inseriscono tra gli elementi da considerare nell'ambito della valutazione di risolvibilità di una banca o di un gruppo l'efficacia, anche in caso di risoluzione della banca/gruppo, dei contratti per l'utilizzo di servizi TIC.

L'articolo 15 chiarisce che Bancoposta 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 (settore bancario) o 4 (infrastrutture finanziarie) di cui all'allegato I del decreto di recepimento della direttiva NIS2 (decreto legislativo n. 138 del 2024).

La RT si limita a rilevare che il Capo V reca «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.

Assicura che tutte le modifiche ivi contenute sono di natura ordinamentale e, pertanto, non comportano nuovi o maggiori oneri per la finanza pubblica.

Al riguardo, sugli articoli 11-14, si conviene con la RT in merito al tenore ordinamentale delle disposizioni in esame. Pertanto, nulla da osservare.

Analogamente sull'articolo 15 non ci sono osservazioni.

CAPO VI
DISPOSIZIONI FINALI

Articoli 16 e 17
(*Clausola di invarianza finanziaria (Art.16); Entrata in vigore (Art. 17)*)

L'articolo 16 reca la clausola di invarianza finanziaria, disponendo 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.

L'articolo 17 disciplina l'entrata in vigore, disponendo 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).

La RT sull'articolo 16 rileva 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.

Sull'articolo 17 si limita a riferire del contenuto della norma.

Al riguardo, sull'articolo 16 - dopo aver ricordato che il comma 6-*bis* dell'articolo 17 della legge di contabilità prevede che, per le disposizioni corredate di clausole di neutralità finanziaria, la relazione tecnica deve comunque riportare la valutazione degli effetti derivanti dalle disposizioni medesime, nonché i dati e gli elementi idonei a suffragare l'ipotesi di invarianza degli effetti sui saldi di finanza pubblica, attraverso l'indicazione dell'entità delle risorse già esistenti nel bilancio e delle relative unità gestionali, utilizzabili per le finalità indicate dalle disposizioni - si segnala l'opportunità di fornire maggiori informazioni riguardo alle risorse disponibili presso l'Agenzia per la cybersicurezza nazionale.