dossier

XIX Legislatura

13 gennaio 2025

Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario

Atto del Governo n. 242

Ai sensi degli articoli 1 e 16 della legge 21 febbraio 2024, n. 15

Senato della Repubblica

Camera dei deputati

Senato della Repubblica

SERVIZIO STUDI
TEL. 06 6706-2451 - ✉ studi1@senato.it – 𝕏 @SR_Studi

Ufficio per le ricerche nei settori economico e finanziario

Dossier n. 424

Camera dei deputati

SERVIZIO STUDI
Dipartimento Finanze
Tel. 06 6760-9496 - ✉ st_finanze@camera.it – 𝕏 @CD_finanze

Atti del Governo n. 242

FI0099.docx

I N D I C E

PREMESSA

L'**atto del Governo n 242** contenente lo 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 per il recepimento della direttiva (UE) 2022/2556 per quanto riguarda la resilienza operativa digitale per il settore finanziario, è **composto da 17 articoli** e **dà attuazione all'articolo 16** della legge 21 febbraio 2024, n. 15 (legge di delegazione europea 2022-2023).

Il **termine di esercizio della delega** con riferimento al regolamento (UE) 2022/2554 nonché per il recepimento della direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio, del 14 dicembre 2022.è previsto **entro diciotto mesi** dall'entrata in vigore della legge di delegazione europea 2022-2023 (entrata in vigore il 10 marzo 2024) e **scade pertanto il 10 settembre 2025.**

Si ricorda che il regolamento (UE) 2022/2554 **si applica dal 17 gennaio 2025**. Si ricorda inoltre che anche la direttiva (UE) 2022/2556 prevede (articolo 10) che gli Stati membri **adottino e pubblichino le misure necessarie per conformarsi alla stessa entro il 17 gennaio 2025**.

I principi di delega, il regolamento (UE) 2022/2554 e la direttiva (UE) 2022/2556

I principi di delega per l'attuazione del regolamento (UE) 2022/2554 e per il recepimento della direttiva (UE) 2022/2556 sono indicati, come anticipato, all'articolo 16 della legge n. 15 del 2024.

Si prevede che l'adeguamento alle disposizioni del regolamento e il recepimento della citata direttiva possa avvenire con uno o più decreti legislativi, con le procedure di cui all'articolo 31 della legge 24 dicembre 2012, n. 234, acquisito il parere dell'Agenzia per la cybersicurezza nazionale.

A tal fine il Governo è tenuto a seguire, oltre ai principi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 234, anche i seguenti **principi e criteri direttivi specifici,** come integrati successivamente all'approvazione della legge di delegazione europea 2022-2023, dalla legge n. 90 del 2024:

a) apportare alla normativa vigente le occorrenti modifiche e integrazioni, anche al sistema sanzionatorio, necessarie all'**adeguamento dell'ordinamento giuridico nazionale** al regolamento (UE)

2022/2554 e al recepimento della direttiva (UE) 2022/2556, incluso l'**eventuale esercizio delle opzioni**, anche mediante la normativa secondaria di cui alla lettera d), previste dal regolamento (UE) 2022/2554. Nell'adozione di tali modifiche e integrazioni il Governo tiene conto degli **orientamenti delle Autorità di vigilanza europee**, degli **atti delegati adottati dalla Commissione europea** e delle disposizioni legislative nazionali di **recepimento delle seguenti direttive** strettamente correlate al regolamento (UE) 2022/2554:

1) la 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**, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2);

2) la direttiva (UE) 2022/2557 del 14 dicembre 2022 del Parlamento europeo e del Consiglio relativa alla **resilienza dei soggetti critici** e che abroga la direttiva 2008/114/CE del Consiglio;

b) assicurare che alle **autorità competenti**, individuate ai sensi dell'articolo 19, comma 1, paragrafo 2, e dell'articolo 46 del regolamento (UE) 2022/2554, siano attribuiti tutti i **poteri di vigilanza, di indagine e sanzionatori** per l'attuazione del regolamento (UE) 2022/2554 e della direttiva (UE) 2022/2556, coerentemente con il riparto di competenze nel settore finanziario nazionale;

c) attribuire alle autorità di cui alla lettera b) il potere di imporre le **sanzioni e le altre misure amministrative** previste dagli articoli 42, paragrafo 6, e 50 del regolamento (UE) 2022/2554, nel rispetto dei limiti edittali e delle procedure previsti dalle disposizioni nazionali che disciplinano l'irrogazione delle sanzioni e l'applicazione delle altre misure amministrative da parte delle autorità anzidette, avuto riguardo al riparto di competenze nel settore finanziario nazionale;

c-bis) 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, **nonché alla società Poste italiane Spa per l'attività del Patrimonio Bancoposta, di cui al regolamento di cui al decreto del Presidente della Repubblica 14 marzo 2001, n. 144**, le occorrenti modifiche e integrazioni, anche mediante la normativa secondaria di cui alla lettera d) del presente comma, per conseguire un livello elevato di resilienza operativa digitale e assicurare la stabilità del settore finanziario nel suo complesso, in particolare:

1) definendo presidi in materia di resilienza operativa digitale equivalenti a quelli stabiliti nel regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022;

2) tenendo conto, nella definizione dei presidi di cui al numero 1), del principio di proporzionalità e delle attività svolte dagli intermediari finanziari e dal Patrimonio Bancoposta;

3) attribuendo alla Banca d'Italia l'esercizio dei poteri di vigilanza, di indagine e sanzionatori di cui alla lettera b) nei confronti dei soggetti di cui alla presente lettera

d) prevedere, ove opportuno, il ricorso alla **disciplina secondaria adottata dalle autorità** indicate alla lettera b) secondo le rispettive competenze.

- ***I contenuti del regolamento (UE) 2022/2054 e della direttiva (UE) 2022/2056***

Il regolamento (UE) 2022/2054

Il regolamento (UE) 2022/2554 (c.d. DORA, *Digital Operational Resilience Act*) - riconducibile al c.d. "Pacchetto finanza digitale" - è volto a **definire un quadro dettagliato sulla resilienza operativa digitale per le entità finanziarie dell'UE** al fine di:

- **approfondire la dimensione della gestione dei rischi digitali** e in particolare migliorare e razionalizzare la gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technologies – ICT) da parte delle entità finanziarie;
- **istituire test accurati dei sistemi di ICT** e accrescere la consapevolezza da parte delle autorità di vigilanza dei rischi informatici e degli incidenti cui sono esposte le entità finanziarie;
- **conferire alle autorità di vigilanza finanziaria poteri di sorveglianza** sui rischi dovuti alla dipendenza delle entità finanziarie da fornitori terzi di servizi;
- **istituire un meccanismo coerente di segnalazione degli incidenti**.

Il regolamento in esame **si applica ad un novero ampio di entità finanziarie** regolamentate, tra cui **enti creditizi, istituti di pagamento, istituti di moneta elettronica,** imprese di investimento, fornitori di servizi per le cripto-attività, depositari centrali di titoli, controparti centrali, sedi di negoziazione, gestori di fondi di investimento alternativi e società di gestione, fornitori di servizi di comunicazione dati, imprese di assicurazione e di riassicurazione, agenzie di *rating* del credito, revisori legali e società di revisione, fornitori di servizi di *crowdfunding* (art. 2).

Il **Capo II del regolamento** si compone degli articoli da 5 a 16 ed **è dedicato alla gestione dei rischi informatici**.

L’art. 5 stabilisce che le entità finanziarie devono predisporre un quadro per la gestione dei rischi relativi alle ICT efficace e prudente.

Le entità finanziarie devono **predisporre un quadro per la gestione dei rischi** informatici (art. 6) “solido, esaustivo ed adeguatamente documentato”, che consenta di affrontare i rischi in maniera “rapida, efficiente ed esaustiva”, assicurando un elevato livello di resilienza operativa digitale corrispondente alle esigenze, alle dimensioni e alla complessità delle loro attività commerciali.

Esso deve comprendere anche una strategia di resilienza digitale, che definisca le modalità di attuazione del quadro medesimo.

In particolare, **le entità finanziarie devono**:

- **utilizzare strumenti e sistemi di ICT idonei, affidabili, di sufficiente capacità** e resilienti, tali da fare fronte alle esigenze di informazioni supplementari richieste da condizioni di stress del mercato o da altre situazioni avverse (art. 7);
- **identificare costantemente tutte le fonti di rischi** relativi alle ICT (art. 8);
- **introdurre misure di protezione e prevenzione** (art. 9);
- **individuare tempestivamente le attività anomale**, compresi i problemi di prestazione della rete delle ICT **e gli incidenti** a esse connessi, nonché per individuare i potenziali singoli punti di vulnerabilità rilevanti, c.d. points of failure (art. 10);
- mettere in atto politiche di continuità operativa e sistemi e piani di risposta e ripristino in caso di disastro relativo alle ICT (artt. 11 e 12).

Ulteriori disposizioni del **Capo II dispongono in ordine agli strumenti di riesame delle situazioni critiche, alle capacità evolutive di resilienza dei sistemi e alla comunicazione tra le entità finanziarie**.

L’art. 16 chiude il Capo II in parola e reca una disciplina concernente talune entità che non sono destinatarie delle disposizioni sopra ricordate.

Il **Capo III (artt. da 17 a 23) disciplina le misure per la gestione, classificazione e segnalazione degli incidenti informatici**.

Le entità finanziarie devono approntare un **processo di gestione per individuare, gestire e notificare gli incidenti** (art. 17), per **classificarli e determinarne l'impatto**, sulla base dei criteri ivi specificati (art. 18) e **segnalarli alle autorità competenti** secondo determinate modalità (art. 19).

Ulteriori disposizioni riguardano l’armonizzazione dei modelli e dei contenuti per le segnalazioni e la centralizzazione delle segnalazioni. Si prevede, infatti, la possibilità di istituire **un polo unico dell'UE per la segnalazione degli incidenti gravi** connessi alle ICT da parte delle entità finanziarie (art. 21).

Il **Capo IV (composto dagli articoli da 24 a 27) dispone in ordine ai test di resilienza**, ordinari ed avanzati, al fine di identificare punti deboli, carenze o lacune, nonché verificare la capacità di attuare tempestivamente misure correttive. Si prevede un'applicazione proporzionata di tali prescrizioni: solo talune entità hanno l'obbligo di svolgere prove avanzate mediante test di penetrazione guidati dalla minaccia (TLPT). Tali test sono eseguiti da soggetti che rispettano specifici requisiti.

Il **Capo V (articoli da 28 a 44) reca disposizioni concernenti i rischi informatici derivanti da terzi**, in considerazione del fatto che le società finanziarie dipendono sempre più da società tecnologiche non finanziarie per i loro servizi ICT.

A tale riguardo, l'art. 30 precisa le principali **disposizioni contrattuali inerenti a diritti e obblighi dell'entità finanziaria e del fornitore terzo di servizi ITC**. Tali diritti e obblighi dovranno essere attribuiti chiaramente e definiti per iscritto. In particolare, i contratti che disciplinano il rapporto dovranno contenere: una descrizione chiara e completa dei servizi, l'indicazione delle località in cui i dati devono essere trattati, descrizioni complete del livello dei servizi accompagnate da obiettivi di prestazione quantitativi e qualitativi, disposizioni pertinenti in materia di accessibilità, disponibilità, integrità, sicurezza e protezione dei dati personali, nonché garanzie per l'accesso, il ripristino e la restituzione in caso di inadempienze dei fornitori terzi di servizi di ICT, i termini di preavviso e gli obblighi di segnalazione dei fornitori terzi di servizi di ICT, i diritti di accesso, ispezione e *audit* da parte dell'entità finanziaria o di un terzo designato a tale scopo nonché le strategie di uscita dedicate. Inoltre, il medesimo Capo V reca disposizioni finalizzate a sottoporre i fornitori terzi di servizi di ICT critici a un quadro di sorveglianza dell'Unione per garantire la convergenza in materia di vigilanza.

Il **Capo VI** si compone del solo art. 45, il quale mira a consentire alle entità finanziarie di istituire accordi per lo scambio di informazioni e dati sulle minacce informatiche.

Il regolamento, inoltre, **individua le autorità competenti** ad assicurare il rispetto degli obblighi disposti dalla nuova disciplina **in relazione alle varie categorie di entità finanziarie (Capo VII, artt. 46-56)**. Il **Capo VIII** dispone in ordine **agli atti delegati** mentre **il Capo IX reca le disposizioni transitorie e finali** e le modifiche ai regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e regolamento (UE) 2016/1011, oltre all'entrata in vigore.

La direttiva (UE) 2022/2056

La direttiva (UE) 2022/2556 interviene su diverse direttive dell'Unione europea(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) al fine di adeguarne i contenuti alle previsioni del regolamento (UE) 2022/2554.

Ciò, come riportato nei considerando della direttiva medesima, risulta necessario in quanto **i requisiti connessi alla gestione dei rischi informatici** nel settore finanziario contenuti nelle sopra ricordate direttive sono diversi e talvolta incompleti. In alcuni casi, i rischi informatici sono stati affrontati solo implicitamente come parte del rischio operativo e in altri casi non sono stati affrontati affatto.

La direttiva attua quindi una serie di modifiche necessarie per **apportare chiarezza giuridica e coerenza in relazione all'applicazione**, da parte delle entità finanziarie autorizzate e sottoposte a vigilanza conformemente a tali direttive, **dei vari requisiti di resilienza operativa digitale necessari per lo svolgimento delle**

loro attività e per la prestazione di servizi, garantendo in tal modo il corretto funzionamento del mercato interno.

Per ulteriori elementi informativi si veda la scheda di lettura dell'articolo 14.

CAPO I
(Disposizioni generali)

Articolo 1
(Definizioni)

L'**articolo 1** reca le **definizioni** di alcuni termini utilizzati nel decreto in esame.

In particolare la disposizione 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).

Si ricorda che il suddetto paragrafo 2 indica le entità che rientrano nella definizione di entità finanziarie, mentre il comma 3 individua i soggetti a cui non si applicano le norme del regolamento Dora.

Inoltre si rinvia ad alcune definizioni contenute:

- nel decreto legislativo n. 138 del 2024 di recepimento della direttiva (UE) 2022/2555 (c.d. NIS 2), 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;

In particolare, 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.

- nel richiamato regolamento DORA;
- nella direttiva DORA ovvero alla direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio del 14 dicembre 2022;
- 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);
- nel decreto del Presidente della Repubblica 14 marzo 2001, n. 144, recante norme sui servizi di bancoposta.

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.

Articolo 2
(Oggetto e ambito di applicazione)

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.

Il **comma 1** chiarisce che il decreto in esame detta le **disposizioni necessarie all'adeguamento del quadro normativo nazionale** al regolamento DORA (ossia il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022) e al recepimento della direttiva DORA (ossia la direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio del 14 dicembre 2022), nonché a garantire il coordinamento con le vigenti disposizioni di settore.

Per una descrizione del suddetto regolamento e della direttiva si rinvia alla premessa del presente dossier.

Il **comma 2** prevede, inoltre, che il presente decreto legislativo individua, anche **le disposizioni applicabili agli intermediari finanziari e a Bancoposta** in materia di resilienza operativa digitale.

Il **comma 3** precisa, infine, che **resta fermo** quanto stabilito dal decreto-legge 21 settembre 2019, n. 105 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 **ovvero di quelli individuati in un atto amministrativo, adottato dal Presidente del Consiglio dei ministri**, su proposta del Comitato interministeriale per la cybersicurezza-CIC, **non soggetto a pubblicazione**. Tale previsione appare coerente con quanto previsto dall'articolo 1, paragrafo 3, del regolamento DORA ovvero che il regolamento medesimo lascia impregiudicata la responsabilità degli Stati membri per quanto riguarda le funzioni essenziali dello Stato concernenti la sicurezza pubblica, la difesa e la sicurezza nazionale conformemente al diritto dell'Unione.

CAPO II
(Autorità competenti e cooperazione)

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

L'**articolo 3** indica nella **Banca d'Italia, nella Consob, nell'IVASS e nella COVIP**, le 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**.

Il **comma 1** stabilisce che, ai sensi dell'articolo 46 del regolamento DORA, in materia di Autorità competenti, **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**.

L'articolo 46 del Regolamento DORA (regolamento (UE) 2022/2554) contiene i riferimenti normativi da prendere in considerazione al fine di individuare l'autorità competente per i diversi settori di attività.

In particolare si fa riferimento ai seguenti soggetti: enti creditizi, istituti di pagamento, istituti di moneta elettronica, prestatori di servizi di informazione sui conti di cui all'articolo 33, paragrafo 1, della direttiva (UE) 2015/2366, imprese di investimento, fornitori di servizi per le cripto-attività, depositari centrali di titoli, controparti centrali, sedi di negoziazione e fornitori di servizi di comunicazione dati, repertori di dati sulle negoziazioni, gestori di fondi di investimento alternativi (cosiddetti GEFIA), società di gestione, imprese di assicurazione e di riassicurazione, intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio, enti pensionistici aziendali o professionali, agenzie di *rating* del credito, amministratori di indici di riferimento critici, fornitori di servizi di *crowdfunding* e repertori di dati sulle cartolarizzazioni.

I **commi 2** e **3** dispongono che la **Banca d'Italia** sia l'Autorità competente per:

- il rispetto degli obblighi posti dal Regolamento DORA a carico di **Cassa depositi e prestiti S.p.A**. (comma 2);
- il rispetto degli obblighi posti dal presente decreto legislativo a carico degli **intermediari finanziari e di Bancoposta** (comma 3).

Il **comma 4** individua **nella Banca d'Italia l'Autorità competente** interessata il cui membro del personale è il rappresentante di alto livello del forum di sorveglianza di cui all'articolo 32 del regolamento DORA, nella **Consob l'Autorità competente che partecipa in qualità di osservatore** su **base permanente** con un proprio rappresentante e, a seconda della tematica trattata, anche **l'IVASS e la COVIP in qualità di osservatori con un proprio rappresentante**.

Si ricorda che il citato articolo 32 stabilisce che il comitato congiunto istituisce il forum di sorveglianza come sottocomitato incaricato di coadiuvare il lavoro del comitato congiunto e dell'Autorità di sorveglianza capofila, per quanto concerne i rischi informatici derivanti da terzi in tutti i settori finanziari.

Il forum di sorveglianza prepara i progetti di posizioni comuni e atti comuni del comitato congiunto in tale ambito e discute periodicamente gli sviluppi rilevanti in materia di vulnerabilità e rischi relativi alle tecnologie dell'informazione e della comunicazione (*Information and Communication Technologies*–TIC), promuovendo un approccio coerente al monitoraggio dei rischi informatici derivanti da terzi a livello dell'Unione.

Si ricorda, altresì, che il comitato congiunto delle autorità europee di vigilanza, istituito dall'articolo 54 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010, funge da *forum* in cui l'Autorità coopera regolarmente e strettamente con l'Autorità europea di vigilanza (Autorità europea delle assicurazioni e delle pensioni aziendali e professionali) e l'Autorità europea di vigilanza (Autorità europea degli strumenti finanziari e dei mercati) per assicurare l'uniformità intersettoriale tenendo conto delle specificità settoriali, in particolare per quanto concerne:

- i conglomerati finanziari e, ove richiesto dal diritto dell'Unione, il consolidamento prudenziale;
- la contabilità e la revisione dei conti;
- le analisi microprudenziali degli sviluppi intersettoriali, dei rischi e delle vulnerabilità in termini di stabilità finanziaria;
- i prodotti di investimento al dettaglio;
- la cibersicurezza;
- lo scambio di informazioni e di migliori prassi con il Comitato europeo per il rischio sistemico-CERS e le altre Autorità europee di vigilanza-AEV;
- i servizi finanziari al dettaglio e le tematiche inerenti alla protezione dei depositanti, dei consumatori e degli investitori;
- la consulenza del comitato all'Autorità europea di vigilanza.

In particolare si prevede che, ai fini della partecipazione al **forum di sorveglianza**, di cui all'articolo 32 del regolamento DORA:

- la **Banca d'Italia** è l'**Autorità competente** interessata di cui al paragrafo 4, lettera *b*), del citato articolo 32;
- la Consob partecipa in qualità di **osservatore con un proprio rappresentante** ai sensi del paragrafo 4, lettera *d*), del medesimo articolo 32;

- a seconda della tematica trattata, possono partecipare in qualità di osservatori con un proprio rappresentante ai sensi del paragrafo 4, lettera *d*), del medesimo articolo 32 **anche l'IVASS e la COVIP**.

Si ricorda che, in base alle suddette lettere *b*) e *d*) il forum di sorveglianza è composto, tra l'altro, da: un rappresentante di alto livello del personale in servizio dell'Autorità competente interessata di ciascuno Stato membro e, se del caso, un rappresentante supplementare di un'Autorità competente di ciascuno Stato membro in qualità di osservatore.

Il **comma 5** dispone, infine, che **i protocolli** di cui all'articolo 5, comma 1, del decreto in commento possono disciplinare **le modalità di partecipazione e lo scambio di informazioni** relative al forum di sorveglianza.

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

L'**articolo 4** reca disposizioni concernenti le **segnalazioni dei gravi incidenti TIC** 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 DORA** destinataria di tali segnalazioni e notifiche.

Il **comma 1** individua, in continuità con quanto disposto dall'articolo 19 del regolamento DORA, le Autorità competenti alla ricezione delle **segnalazioni dei gravi incidenti TIC** (tecnologie dell'informazione e della comunicazione - *Information and Communication Technologies* – ICT) e delle **notifiche volontarie relative alle minacce informatiche significative**. Segnatamente:

- **Banca d'Italia**, per quanto riguarda:
  - enti creditizi;
  - istituti di pagamento;
  - prestatori di servizi di informazione sui conti;
  - istituti di moneta elettronica;
  - fornitori di servizi per le cripto-attività ed emittenti di *token* collegati ad attività;
  - controparti centrali;
  - gestori di fondi di investimento alternativi;
  - società di gestione;
  - fornitori di servizi di *crowdfunding*;
  - sedi di negoziazione all'ingrosso di titoli di Stato;
  - Cassa depositi e prestiti S.p.A.;
  - intermediari finanziari;
  - Bancoposta;
- **Consob**, con riferimento ai depositari centrali di titoli e alle sedi di negoziazione, escluse le sedi di negoziazione all'ingrosso di titoli di Stato;
- **IVASS**, per quanto concerne le imprese di assicurazione e di riassicurazione e gli intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio;
- **COVIP**, con riguardo agli enti pensionistici aziendali o professionali.

Sul punto, si evidenzia che, ai sensi del menzionato articolo 19 del regolamento DORA, le entità finanziarie sono tenute alla segnalazione dei gravi incidenti TIC all'autorità competente interessata di cui all'articolo 46. Peraltro, qualora un'entità finanziaria sia soggetta alla vigilanza di più di un'autorità nazionale competente DORA, **gli Stati membri devono designare un'unica autorità competente quale responsabile** dell'espletamento delle funzioni e dei compiti previsti dal medesimo articolo 19.

A tal riguardo, si specifica che le entità finanziarie tenute a siffatti obblighi informativi sono indicate dall'articolo 2, paragrafo 1, del regolamento DORA.

Il **comma 2** prevede che, in caso di entità finanziarie **vigilate da più Autorità competenti DORA**, l'Autorità ricevente, di cui al precedente comma 1, **trasmetta tempestivamente** alle altre Autorità competenti 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**, in base alle modalità definite nei protocolli di intesa.

In merito, si segnala che, oltre alla notifica iniziale, le relazioni richiamate dal sopra citato articolo 19, paragrafo 4, sono le seguenti:

- una relazione intermedia dopo la notifica iniziale, non appena lo stato originario dell'incidente muta in maniera significativa o il trattamento del grave incidente TIC cambia alla luce delle nuove informazioni disponibili, seguita, a seconda dei casi, da notifiche aggiornate, ogni qualvolta sia disponibile un aggiornamento della situazione, nonché su specifica richiesta dell'autorità competente;
- una relazione finale, quando l'analisi delle cause che hanno dato origine all'incidente sia stata completata, indipendentemente dal fatto che le misure di attenuazione siano già state attuate, e quando al posto delle stime siano disponibili i dati dell'impatto effettivo.

Il **comma 3**, facendo salvo quanto disposto dai commi 1, 2 e 4, 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 (c.d. CER), 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 medesimo regolamento. Si specifica, altresì, che tali informazioni trasmesse a CSIRT Italia sono **coperte dal segreto d'ufficio**.

A tal proposito, si evidenzia che l'obbligo informativo al Gruppo nazionale di risposta agli incidenti di sicurezza informatica (CSIRT) è previsto dall'articolo 19, paragrafo 1, comma 6, del regolamento DORA.

In particolare, si dispone che, fatta salva la segnalazione dei gravi incidenti TIC da parte dell'entità finanziaria all'autorità competente interessata, gli Stati membri possono stabilire, in aggiunta, che alcune o tutte le entità finanziarie forniscano, altresì, la notifica iniziale e ciascuna relazione di cui al paragrafo 4 del medesimo articolo, utilizzando i modelli di cui all'articolo 20 del regolamento DORA, 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 (c.d. NIS 2).

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. Peraltro, si prevede che tali informazioni trasmesse a CSIRT Italia siano **coperte dal segreto d'ufficio**.

In linea con quanto suesposto, l'articolo 19, paragrafo 2, comma 3, del regolamento DORA prevede che gli Stati membri possano stabilire che le entità finanziarie che procedono alla notifica su base volontaria, nonché alla notifica delle minacce informatiche significative qualora ritengano che la minaccia sia rilevante per il sistema finanziario, gli utenti dei servizi o i clienti, possano, altresì, trasmettere tale notifica ai CSIRT nazionali designati o istituiti a norma della direttiva (UE) 2022/2555 (NIS 2).

Infine, il **comma 4** 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 ai sensi del comma 2, la notifica iniziale, le relazioni sui gravi incidenti TIC, nonché le notifiche volontarie relative alle minacce informatiche significative.

Si ricorda che, ai sensi del paragrafo 6 dell'articolo 19 del regolamento, dopo aver ricevuto la notifica iniziale e ciascuna delle relazioni di cui al paragrafo 4, sopra ricordate l'autorità competente trasmette tempestivamente i dettagli del grave incidente TIC ai seguenti destinatari sulla base, delle rispettive competenze:

a) all'Autorità bancaria europea (ABE), all'autorità di regolamentazione e di vigilanza dei mercati finanziari dell'Unione europea (ESMA) o all'Autorità europea delle assicurazioni e delle pensioni aziendali o professionali (EIOPA);
b) alla BCE, qualora siano coinvolti enti creditizi, istituti di pagamento e istituti di moneta elettronica;
c) alle autorità competenti, ai punti di contatto unici o ai CSIRT;
d) alle autorità di risoluzione e al Comitato di risoluzione unico (SRB) per quanto riguarda gli enti creditizi e le imprese di investimento rientranti

nell'ambito applicativo regolamento (UE) 2014/806, qualora tali dettagli riguardino incidenti che comportano un rischio per le funzioni essenziali;

e) ad altre pertinenti autorità pubbliche ai sensi del diritto nazionale.

Una volta ricevute le informazioni sopra descritte, l'ABE, l'ESMA o l'EIOPA e la BCE, in consultazione con l'ENISA e in collaborazione con l'autorità competente interessata, valutano la pertinenza dell'grave incidente TIC rispetto alle autorità competenti in altri Stati membri. A seguito di tale valutazione, l'ABE, l'ESMA o l'EIOPA inviano una notifica al riguardo il prima possibile alle autorità competenti interessate in altri Stati membri. La BCE notifica i membri del Sistema europeo di banche centrali in merito a questioni afferenti il sistema di pagamenti. Sulla base di tale notifica, le autorità competenti adottano, se del caso, tutte le misure necessarie per proteggere l'immediata stabilità del sistema finanziario.

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

L'**articolo 5** 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**.

Il **comma 1** prevede che le **Autorità competenti DORA** individuino **forme di coordinamento operativo e informativo** tramite uno o più **protocolli d'intesa** al fine di assicurare la **tempestiva e completa condivisione dei dati e delle informazioni** utili all'esercizio delle proprie funzioni di vigilanza, ivi incluse le informazioni sui gravi incidenti TIC, anche in relazione alle entità finanziarie soggette, ai sensi della normativa di settore, alla vigilanza di più autorità. Le medesime Autorità stabiliscono, altresì, le modalità di pubblicazione dei suddetti protocolli.

Il **comma 2** dispone, in attuazione di quanto disposto dal regolamento DORA, la **stipulazione di protocolli di intesa** tra le Autorità competenti DORA e l'Agenzia per la cybersicurezza nazionale (ACN), volti alla realizzazione delle seguenti attività:

- regolazione dello scambio di informazioni pertinenti;
- istituzione di forme di consulenza e assistenza tecnica reciproca, nonché di meccanismi di coordinamento efficaci e di risposta rapida nel caso di incidenti;
- specificazione, se del caso, delle modalità di coordinamento delle attività relative a soggetti essenziali o importanti, ai sensi della direttiva (UE) 2022/2555 (c.d. NIS 2), che siano stati designati come fornitori terzi critici di servizi TIC, a norma dell'articolo 31 del regolamento DORA.

Si prevede, altresì, la stipula di un **protocollo d'intesa tra le Autorità competenti DORA con il Corpo della Guardia di finanza**, ai sensi dell'articolo 19, paragrafo 6, lettera *e*), del regolamento DORA, 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.

Al riguardo, si evidenzia che l'articolo 47 del regolamento DORA stabilisce che le Autorità europee di vigilanza (AEV) e le autorità competenti ai sensi del regolamento medesimo possono partecipare alle attività del gruppo di cooperazione per le questioni che riguardano le loro attività di vigilanza in relazione alle entità finanziarie, al fine di promuovere la cooperazione e di consentire lo scambio di pratiche di vigilanza tra le predette autorità competenti e il gruppo di cooperazione istituito dall'articolo 14 della direttiva (UE) 2022/2555 (c.d. NIS 2). Le AEV e le autorità competenti possono chiedere di essere invitate a partecipare alle attività del gruppo di cooperazione per questioni relative alle entità essenziali o importanti ai sensi della menzionata direttiva che sono anch'esse state designate come fornitori terzi critici di servizi TIC.

Inoltre, l'articolo 19, paragrafo 6, lettera *e*) sopra richiamato prevede, in particolare, la trasmissione di informazioni di interesse in materia di incidenti informatici, oltre che alle autorità specificamente indicate, ad altre pertinenti autorità pubbliche ai sensi del diritto nazionale.

A tal riguardo, la relazione illustrativa del Governo evidenzia che la disposizione in esame muove dall'esigenza di favorire forme di raccordo informativo tra le autorità competenti DORA e la Guardia di finanza. In particolare, 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, 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.

Nella medesima relazione illustrativa il Governo osserva che la disposizione non amplia il novero dei settori in cui si troverebbe a operare la Guardia di finanza, bensì si propone di fornire alla medesima dei preziosi *input* informativi idonei a rendere più efficace ed efficiente il proprio dispositivo di contrasto al crimine economico-finanziario.

Il **comma 3** prevede che le **informazioni** (su minacce, vulnerabilità e incidenti informatici) acquisite dall'Agenzia per la cybersicurezza nazionale, anche in forza dei sopra citati protocolli di intesa, **siano trasmesse agli organismi di informazione per la sicurezza** istituiti con legge n. 124 del 2007, affinché questi 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.

Sul punto, si segnala che gli organismi di informazione per la sicurezza sopra citati sono i seguenti:

- Dipartimento delle informazioni per la sicurezza (DIS) (articolo 4 della legge n. 124 del 2007);
- Agenzia informazioni e sicurezza esterna (AISE) (articolo 6 della legge n. 124 del 2007);
- Agenzia informazioni e sicurezza interna (AISI) (articolo 7 della legge n. 124 del 2007).

La relazione illustrativa del Governo evidenzia che la disposizione in commento si pone in continuità 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 NIS 2 (articolo 17, comma 5)) volte a prevedere l'acquisizione da parte degli organismi di *intelligence* di informazioni ricevute dall'Agenzia per la cybersicurezza nazionale da parte dei soggetti tenuti agli obblighi informativi CER e NIS 2.

Peraltro, nella medesima relazione, il Governo osserva che la trasmissione delle informazioni agli organismi di informazione per la sicurezza risulta anche coerente con il sistema del regolamento DORA, sulla base di quanto disposto dallo stesso al già menzionato articolo 19, paragrafo 6, lettera *e*).

Il **comma 4** stabilisce che l'**Autorità nazionale competente NIS** 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 (si veda la relativa scheda) da parte di un'entità finanziaria.

CAPO III
(Disposizioni applicabili a intermediari finanziari e Bancoposta)

Articolo 6
(Disposizioni applicabili agli intermediari finanziari)

L'**articolo 6** individua le disposizioni del regolamento (UE) 2022/2554 (cd. "**regolamento DORA**") applicabili agli **intermediari finanziari** iscritti all'albo di cui all'articolo **106 del TUB**. In ossequio al principio di proporzionalità richiamato nei criteri di delega, si richiede a tali soggetti l'adozione del **quadro semplificato per la gestione dei rischi informatici** (cd. "**ICT *risk management framework* semplificato**") in conformità alle relative disposizioni contenute nel regolamento DORA. Per gli **intermediari finanziari** che si qualificano come "**microimprese**" (che occupino meno di 10 dipendenti e realizzino un fatturato annuo e/o totale di bilancio annuo non superiore a 2 milioni di euro) si applica una **disciplina *ad hoc*** per lo svolgimento dei **test di resilienza operativa digitale**. La **Banca d'Italia** può individuare, in via regolamentare, una **categoria di intermediari finanziari** da considerarsi "**significativi**" cui applicare il **quadro completo per la gestione dei rischi informatici** (cd. "***ICT risk management framework* completo**").

L'**articolo 6** individua le **disposizioni** del regolamento (UE) 2022/2554 (cd. "**regolamento DORA**") applicabili agli **intermediari finanziari**, in attuazione a quanto previsto dall'articolo 16, comma 2, lettera *c-bis*), della legge di delegazione europea 2022-2023 (inserita dall'articolo 15 della legge 28 giugno 2024, n. 90).

Al fine di conseguire un livello di resilienza operativa digitale e di assicurare la stabilità del settore finanziario nel suo complesso, le disposizioni applicabili agli **intermediari finanziari** iscritti all'albo di cui all'**articolo 106** del decreto legislativo 1° settembre 1993, n. 385 (cd. "Testo unico delle leggi in materia bancaria e creditizia – **TUB**") sono individuate secondo il **principio di proporzionalità** richiamato nei criteri di delega, nonché tenuto conto delle **attività svolte** dagli intermediari finanziari.

Gli intermediari finanziari iscritti all'albo di cui all'articolo 106 del TUB (tenuto dalla Banca d'Italia) sono soggetti, diversi dalle banche, che esercitano in via professionale, nei confronti del pubblico, le seguenti attività:

1) concessione di finanziamenti sotto qualsiasi forma;
2) riscossione dei crediti ceduti e servizi di cassa e pagamento ai sensi della legge n. 130 del 1999 in materia di cartolarizzazione dei crediti (c.d. *servicing*).

Per espressa previsione dell'articolo 106, comma 2, del TUB, gli intermediari possono esercitare anche le seguenti attività:

a) emettere moneta elettronica e prestare servizi di pagamento, se autorizzati e iscritti nel relativo albo;
b) prestare solo servizi di pagamento, se autorizzati e iscritti nel relativo albo;
c) prestare servizi di investimento, nei casi e alle condizioni previste dalla Banca d'Italia ai sensi del TUF;
d) effettuare le altre attività previste da norme di legge, a condizione che siano svolte in via subordinata rispetto alle attività di concessione di finanziamenti, come per esempio: la promozione e conclusione di contratti relativi alla concessione di finanziamenti sotto qualsiasi forma e alla prestazione di servizi di pagamento; l'erogazione di finanziamenti agevolati e la gestione di fondi pubblici; l'intermediazione assicurativa e riassicurativa previa iscrizione negli appositi registri.

Secondo quanto illustrato nella relazione tecnica, a commento della sezione III dello schema di decreto legislativo, 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).

Nello specifico, il **comma 1**, dispone che agli **intermediari finanziari** sia applicabile, in via generale, il **quadro semplificato per la gestione dei rischi informatici** (cd. "***Information and Communication Technologies*** – **ICT** – ***risk management framework*** **semplificato**") previsto per le entità finanziarie di minori dimensioni o complessità.

Più precisamente, si rendono applicabili le seguenti disposizioni del regolamento DORA e, in quanto compatibili, le relative norme tecniche di regolamentazione e attuazione.

Disposizioni del regolamento DORA applicabili agli intermediari finanziari	
Articolo	**Descrizione**
4	Applicazione del **principio di proporzionalità**, tenuto conto: (*i*) delle loro **dimensioni**; (*ii*) del profilo di **rischio complessivo**; (*iii*) della **natura**, **portata** e **complessità** dei loro **servizi**, della loro **attività** e della loro **operatività**.
16, paragrafi 1 e 2	Adozione di un **quadro semplificato per la gestione dei rischi informatici** che consenta, in particolare, di garantire: (*a*) un **costante monitoraggio** di tutti i **sistemi di Tecnologie dell'Informazione e della Comunicazione** (**TIC** o **ICT**); (*b*) la **tempestiva individuazione e rilevazione** delle fonti di rischi informatici e delle anomalie dei sistemi informatici; (*c*) l'implementazione di **misure di *backup* e ripristino** delle funzioni essenziali e relativi ***testing* periodici**; (*d*) **programmi di formazione e sensibilizzazione sulla sicurezza delle TIC per il personale e la dirigenza**. Inoltre, il quadro di gestione dei rischi deve essere **documentato e riesaminato periodicamente** e al verificarsi di incidenti gravi connessi alle TIC conformemente alle istruzioni delle autorità di vigilanza.
17	Definizione ed attuazione di un **processo di gestione, classificazione e segnalazione degli incidenti connessi alle TIC**.
18, paragrafi 1 e 2	**Classificazione degli incidenti connessi alle TIC e delle minacce informatiche** significative.
19, paragrafi 1, 2, 3, 4 e 5	**Segnalazione dei gravi incidenti TIC all'autorità di vigilanza competente e notifica** alla medesima autorità, **su base volontaria**, **delle minacce informatiche significative** per il sistema finanziario, gli utenti dei servizi o i clienti. Si applica il modello previsto dell'articolo 20 del regolamento che prevede la trasmissione di una notifica iniziale, seguita da una relazione intermedia e da una relazione finale al termine dell'analisi delle cause che hanno originato l'incidente e della quantificazione dell'impatto effettivo.
22, paragrafo 1	**Riscontri tempestivi**, **pertinenti e proporzionali**, nonché orientamenti di alto livello dell'**autorità di vigilanza competente**, a seguito della notifica iniziale e delle successive relazioni.
24	**Requisiti generali per lo svolgimento dei test di resilienza operativa digitale** per le entità diverse dalle microimprese. Il **programma di test** di resilienza operativa digitale deve essere solido ed esaustivo, nonché parte integrante del quadro per la gestione dei rischi informatici e comprendere una serie di valutazioni, test, metodologie, pratiche e strumenti da applicare. I test devono essere svolti da soggetti indipendenti, interni o esterni, con **cadenza almeno annuale**, su tutti i sistemi e le applicazioni di TIC a supporto di funzioni essenziali o importanti.
25, paragrafo 1	**Test di strumenti e sistemi di TIC**: valutazione e scansione delle vulnerabilità, analisi *open source*, valutazioni della sicurezza delle reti, analisi delle carenze, esami della sicurezza fisica, questionari e soluzioni di scansione del *software*, esami del codice sorgente, ove fattibile, test basati su scenari, test di compatibilità, test di prestazione, test *end-to-end* e *test* di penetrazione.
28, paragrafi 1,3,4,5,6,7 e 8	**Principi generali di una solida gestione dei rischi informatici derivanti da terzi**.
29	**Valutazione preliminare del rischio di concentrazione delle TIC a livello di entità**.
30, paragrafi 1,2,3 e 4	**Principali disposizioni contrattuali** concernenti l'individuazione dei diritti e degli obblighi dell'entità finanziaria e del fornitore terzo di servizi TIC.
31, paragrafo 12	**Designazione di un fornitore terzo critico di servizi TIC stabilito in un paese terzo**, nel caso in cui detto fornitore abbia istituito un'impresa figlia nell'Unione entro 12 mesi dalla designazione.
45	**Meccanismi di condivisione delle informazioni** tra entità finanziarie.
51	Esercizio del **potere di imporre sanzioni amministrative e misure di riparazione** di cui all'articolo 50 del regolamento da parte dell'autorità di vigilanza competente.
54	**Pubblicazione delle sanzioni amministrative** senza indebito ritardo sul sito web ufficiale dell'autorità di vigilanza competente.
55	Obbligo del **segreto professionale** a tutte le persone che prestano o hanno prestato la loro attività per le autorità competenti sulle informazioni riservate ricevute, scambiate o trasmesse a norma del regolamento.
56	**Protezione dei dati**: le autorità competenti sono autorizzate a trattare i dati personali solo se necessario ai fini dell'adempimento dei rispettivi obblighi e doveri ai sensi del regolamento.

Il **comma 2** dispone per gli intermediari finanziari che si qualificano come **microimprese** ai sensi dell'articolo 3, paragrafo 1, punto 60), del regolamento DORA, quanto segue:

1) **non trova applicazione** l'**articolo 24** del regolamento DORA concernente i requisiti generali per lo svolgimento dei test di resilienza operativa digitale;
2) trova applicazione la **disciplina *ad hoc*** contenuta nell'**articolo 25**, paragrafi 1 e 3 del regolamento DORA:

- il programma di test di resilienza operativa, ad essi applicabile, prevede l'esecuzione di test adeguati, tra cui valutazione e scansione delle vulnerabilità, analisi *open source*, valutazioni della sicurezza delle reti, analisi delle carenze, esami della sicurezza fisica, questionari e soluzioni di scansione del *software*, esami del codice sorgente, ove fattibile, test basati su scenari, test di compatibilità, test di prestazione, test *end-to-end* e test di penetrazione;
- relativamente alle modalità di svolgimento dei test, combinando un approccio basato sul rischio con una pianificazione strategica dei test relativi alle TIC, tenendo debitamente conto della necessità di mantenere un approccio equilibrato tra l'entità delle risorse e il tempo da assegnare ai test relativi alle TIC, da un lato, e l'urgenza, il tipo di rischio, la criticità dei patrimoni informativi e dei servizi forniti nonché qualsiasi altro fattore rilevante, compresa la capacità dell'entità finanziaria di assumere rischi calcolati, dall'altro.

Ai sensi dell'articolo 3, paragrafo 1, punto 60), del regolamento DORA, si definisce "microimpresa" un'entità finanziaria, diversa da una sede di negoziazione, una controparte centrale, un repertorio di dati sulle negoziazioni o un depositario centrale di titoli, che: (*i*) **occupa meno di 10 persone** e (*ii*) realizza un **fatturato annuo e/o un totale di bilancio annuo non superiore a 2 milioni di euro**.

Il **comma 3** attribuisce alla potestà regolamentare della **Banca d'Italia** l'eventuale individuazione di una **categoria di intermediari finanziari** da considerarsi "**significativi**" cui applicare l'***ICT risk management framework* completo**, anziché quello semplificato di cui all'articolo 16, paragrafi 1 e 2. In tal senso, viene richiamato l'articolo 9 dello schema di decreto legislativo che conferisce alla Banca d'Italia il potere di emanare le disposizioni attuative del medesimo decreto e del regolamento DORA (si veda la relativa scheda).

In tal caso, in luogo all'articolo 16, paragrafi 1 e 2 del regolamento DORA, si rendono applicabili le seguenti disposizioni del medesimo regolamento e, in quanto compatibili, le relative norme tecniche di regolamentazione e attuazione.

Disposizioni del regolamento DORA applicabili alla categoria di intermediari finanziari individuati dalla Banca d'Italia	
Articolo	**Descrizione**
5	**Governance e organizzazione** nell'adozione di un **quadro di gestione e di controllo interno** in grado di garantire una gestione efficace e prudente **di tutti i rischi informatici**. Si definiscono le responsabilità dell'organo di gestione dell'entità finanziaria rispetto ai sistemi di Tecnologie dell'Informazione e della Comunicazione (TIC o ICT).
6	Adozione di un **quadro completo per la gestione dei rischi informatici** solido, esaustivo e adeguatamente documentato, che consenta di affrontare i rischi informatici in maniera rapida, efficiente ed esaustiva, assicurando un elevato livello di resilienza operativa digitale. In particolare, (*i*) comprende strategie, politiche, procedure, protocolli e strumenti in materia di TIC necessari per proteggere adeguatamente tutti i patrimoni informativi e i risorse TIC; (*ii*) la responsabilità della gestione e della sorveglianza dei rischi informatici è affidata ad una funzione di controllo; (*iii*) è documentato e riesaminato almeno una volta all'anno, nonché in occasione di gravi incidenti TIC e in seguito a indicazioni o conclusioni delle autorità di vigilanza formulate a seguito di pertinenti test di resilienza operativa digitale o di processi di audit.
7	Utilizzo e aggiornamento di **sistemi, protocolli e strumenti di TIC** che, in conformità al principio di proporzionalità, siano **idonei alle dimentisioni** delle operazioni a supporto dell'attività dell'entità, **affidabili**, **dotati di capacità sufficiente per eleborare i dati** in maniera accurata e **tecnologicamente resilienti**.
8	**Identificazione delle fonti di rischio relative alle TIC**, con particolare riguardo all'esposizione al rischio da e verso altre entità finanziarie, valutazione circa le minacce informatiche per i patrimoni informativi e per le risorse TIC. Riesame periodio, e almeno una volta all'anno, degli scenari di rischio che esercitano un impatto.
9	**Protezione dei sistemi TIC e prevenzione** di indisponibilità, deterioramento dell'autenticità o dell'integrità, o di violazioni della riservatezza e la perdita di dati. A tale scopo, le entità finanziarie monitorano e controllano costantemente la sicurezza e il funzionamento dei sistemi e degli strumenti di TIC e riducono al minimo l'impatto dei rischi informatici sui sistemi di TIC adottando politiche, procedure e strumenti adeguati per la sicurezza delle TIC.
10	Adozione di **meccanismi di individuazione tempestiva delle attività anomale**, compresi i problemi di prestazione della rete delle TIC e gli incidenti a esse connessi, nonché **dei pontenziali singoli punti di vulnerabilità importanti**.
11, paragrafi 1,2,3,4,5,6,7,8 e 10	Attuazione di **piani di risposta e ripristino** relativi alle TIC associati soggetti a un *audit* interno indipendente. In particolare, predispongono, mantengono e testano periodicamente opportuni piani di continuità operativa delle TIC, con riguardo alle funzioni essenziali o importanti esternalizzate o appaltate tramite accordi con fornitori terzi di servizi TIC.
12, paragrafi 1,2,3,4,6 e 7	Elaborazione e documentazone di **Politiche e procedure di *backup*** (si identifica il perimetro dei dati e la frequenza minima di *backup*) e **Procedure e metodi di ripristino e recupero** da effettuarsi periodicamente.
13	**Apprendimento ed evoluzione** mediante la raccolta delle informazioni concernenti le vulnerabilità e le minacce informatiche, gli incidenti connessi alle TIC (attacchi informatici) e l'analisi dei probabili effetti sulla resilienza operativa digitale. A seguito di un grave incidente connesso alle TIC, deve essere garantito un **riesame** (tempestivo, di qualità, di efficacia della procedura di attivazione dei livelli successivi e della comunicazione interna) volto ad analizzare le cause di pertubazione e ad identificare i **miglioramenti** da apportare alle operazioni riguardanti le TIC, nonché ad attuare le modifiche richieste dall'autorità competente.
14	**Piani di comunicazione dei gravi incidenti connessi alle TIC** per il personale interno e per i portatori di interessi esterni (clienti, controparti e pubblico). Con riguardo al personale interno, le politiche di comunicazione tengono conto della distinzione tra personale coinvolto nella gestione dei rischi infomatici (come il responsabile della risposta e del ripristino) e personale da informare. Viene individuata una persona cui affidare l'attuazione della strategia di comunicazione per gli incidenti connessi alle TIC e la funzione di informazione al pubblico e ai media.

Articolo 7
(Disposizioni applicabili a Bancoposta)

L'**articolo 7** individua le disposizioni del regolamento (UE) 2022/2554 (cd. "**regolamento DORA**") applicabili a **Bancoposta**. In ossequio al principio di proporzionalità richiamato nei criteri di delega, si rende applicabile la medesima disciplina applicata per le banche. In particolare, si fa riferimento all'adozione del **quadro completo per la gestione dei rischi informatici** (cd. "**ICT *risk management framework* completo**"), alla **disciplina sulla segnalazione degli incidenti TIC** e a quella afferente ai **test di resilienza operativa digitale**, in conformità alle relative disposizioni contenute nel regolamento DORA.

L'**articolo 7** individua le **disposizioni** del regolamento (UE) 2022/2554 (cd. "**regolamento DORA**") applicabili a **Bancoposta**, in attuazione a quanto previsto dall'articolo 16, comma 2, lettera *c-bis*), della legge di delegazione europea 2022-2023 (inserita dall'articolo 15 della legge 28 giugno 2024, n. 90).

Al fine di conseguire un livello di resilienza operativa digitale e di assicurare la stabilità del settore finanziario nel suo complesso, le disposizioni applicabili a **Bancoposta** sono individuate secondo il **principio di proporzionalità** richiamato nei criteri di delega, nonché tenuto conto delle **attività da questa svolte**.

Nello specifico, l'articolo 7, **comma 1**, dispone che a **Bancoposta** siano applicabili le disposizioni del regolamento DORA descritte nella seguente tabella e, in quanto compatibili, le relative norme tecniche di regolamentazione e attuazione.

A tale riguardo, nella relazione illustrativa si chiarisce che 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**).

Rispetto alle disposizioni applicabili agli intermediari finanziari:

- si applicano **sia le disposizioni previste per gli intermediari finanziari previste al comma 1** dell'articolo 6 (ad eccezione dell'articolo 16, comma 1 e 2, vedi la scheda relativa all'articolo 6)) **sia quelle previste al comma 3** (ad eccezione dell'articolo 11);

- si applicano inoltre gli articoli: 23, 26 paragrafi 1,2, 3, 4, 5, 6, 7, 8, 9, e 10, 27.

Disposizioni del regolamento DORA applicabili a Bancoposta	
Articolo	**Descrizione**
4	Applicazione del **principio di proporzionalità**, tenuto conto: (*i*) delle loro **dimensioni**; (*ii*) del profilo di **rischio complessivo**; (*iii*) della **natura**, **portata** e **complessità** dei loro **servizi**, della loro **attività** e della loro **operatività**.
5	**Governance e organizzazione** nell'adozione di un **quadro di gestione e di controllo interno** in grado di garantire una gestione efficace e prudente **di tutti i rischi informatici**. Si definiscono le responsabilità dell'organo di gestione dell'entità finanziaria rispetto ai sistemi di Tecnologie dell'Informazione e della Comunicazione (TIC o ICT).
6	Adozione di un **quadro completo per la gestione dei rischi informatici** solido, esaustivo e adeguatamente documentato, che consenta di affrontare i rischi informatici in maniera rapida, efficiente ed esaustiva, assicurando un elevato livello di resilienza operativa digitale. In particolare, (*i*) comprende strategie, politiche, procedure, protocolli e strumenti in materia di TIC necessari per proteggere adeguatamente tutti i patrimoni informativi e i risorse TIC; (*ii*) la responsabilità della gestione e della sorveglianza dei rischi informatici è affidata ad una funzione di controllo; (*iii*) è documentato e riesaminato almeno una volta all'anno, nonché in occasione di gravi incidenti TIC e in seguito a indicazioni o conclusioni delle autorità di vigilanza formulate a seguito di pertinenti test di resilienza operativa digitale o di processi di audit.
7	Utilizzo e aggiornamento di **sistemi, protocolli e strumenti di TIC** che, in conformità al principio di proporzionalità, siano **idonei alle dimentisioni** delle operazioni a supporto dell'attività dell'entità, **affidabili**, **dotati di capacità sufficiente per eleborare i dati** in maniera accurata e **tecnologicamente resilienti**.
8	**Identificazione delle fonti di rischio relative alle TIC**, con particolare riguardo all'esposizione al rischio da e verso altre entità finanziarie, valutazione circa le minacce informatiche per i patrimoni informativi e per le risorse TIC. Riesame periodio, e almeno una volta all'anno, degli scenari di rischio che esercitano un impatto.
9	**Protezione dei sistemi TIC e prevenzione** di indisponibilità, deterioramento dell'autenticità o dell'integrità, o di violazioni della riservatezza e la perdita di dati. A tale scopo, le entità finanziarie monitorano e controllano costantemente la sicurezza e il funzionamento dei sistemi e degli strumenti di TIC e riducono al minimo l'impatto dei rischi informatici sui sistemi di TIC adottando politiche, procedure e strumenti adeguati per la sicurezza delle TIC.
10	Adozione di **meccanismi di individuazione tempestiva delle attività anomale**, compresi i problemi di prestazione della rete delle TIC e gli incidenti a esse connessi, nonché **dei pontenziali singoli punti di vulnerabilità importanti**.
11, paragrafi 1,2,3,4,5,6,7,8 e 10	Attuazione di **piani di risposta e ripristino** relativi alle TIC associati soggetti a un *audit* interno indipendente. In particolare, predispongono, mantengono e testano periodicamente opportuni piani di continuità operativa delle TIC, con riguardo alle funzioni essenziali o importanti esternalizzate o appaltate tramite accordi con fornitori terzi di servizi TIC.
12, paragrafi 1,2,3,4,6 e 7	Elaborazione e documentazone di **Politiche e procedure di *backup*** (si identifica il perimetro dei dati e la frequenza minima di *backup*) e **Procedure e metodi di ripristino e recupero** da effettuarsi periodicamente.
13	**Apprendimento ed evoluzione** mediante la raccolta delle informazioni concernenti le vulnerabilità e le minacce informatiche, gli incidenti connessi alle TIC (attacchi informatici) e l'analisi dei probabili effetti sulla resilienza operativa digitale. A seguito di un grave incidente connesso alle TIC, deve essere garantito un **riesame** (tempestivo, di qualità, di efficacia della procedura di attivazione dei livelli successivi e della comunicazione interna) volto ad analizzare le cause di pertubazione e ad identificare i **miglioramenti** da apportare alle operazioni riguardanti le TIC, nonché ad attuare le modifiche richieste dall'autorità competente.
14	**Piani di comunicazione dei gravi incidenti connessi alle TIC** per il personale interno e per i portatori di interessi esterni (clienti, controparti e pubblico). Con riguardo al personale interno, le politiche di comunicazione tengono conto della distinzione tra personale coinvolto nella gestione dei rischi infomatici (come il responsabile della risposta e del ripristino) e personale da informare. Viene individuata una persona cui affidare l'attuazione della strategia di comunicazione per gli incidenti connessi alle TIC e la funzione di informazione al pubblico e ai media.

Disposizioni del regolamento DORA applicabili a Bancoposta	
Articolo	**Descrizione**
17	Definizione ed attuazione di un **processo di gestione, classificazione e segnalazione degli incidenti connessi alle TIC**.
18, paragrafi 1 e 2	**Classificazione degli incidenti connessi alle TIC e delle minacce informatiche** significative.
19, paragrafi 1,2,3,4 e 5	**Segnalazione dei gravi incidenti TIC all'autorità di vigilanza competente e notifica** alla medesima autorità, **su base volontaria**, **delle minacce informatiche significative** per il sistema finanziario, gli utenti dei servizi o i clienti. Si applica il modello previsto dell'articolo 20 del regolamento che prevede la trasmissione di una notifica iniziale, seguita da una relazione intermedia e da una relazione finale al termine dell'analisi delle cause che hanno originato l'incidente e della quantificazione dell'impatto effettivo.
22, paragrafo 1	**Riscontri tempestivi**, **pertinenti e proporzionali**, nonché orientamenti di alto livello dell'**autorità di vigilanza competente**, a seguito della notifica iniziale e delle successive relazioni.
23	**Incidenti operativi o relativi alla sicurezza dei pagamenti riguardanti enti creditizi, istituti di pagamento, prestatori di servizi di informazione sui conti e istituti di moneta elettronica**.
24	**Requisiti generali per lo svolgimento dei test di resilienza operativa digitale** per le entità diverse dalle microimprese. Il **programma di test** di resilienza operativa digitale deve essere solido ed esaustivo, nonché parte integrante del quadro per la gestione dei rischi informatici e comprendere una serie di valutazioni, test, metodologie, pratiche e strumenti da applicare. I test devono essere svolti da soggetti indipendenti, interni o esterni, con **cadenza almeno annuale**, su tutti i sistemi e le applicazioni di TIC a supporto di funzioni essenziali o importanti.
25, paragrafo 1	**Test di strumenti e sistemi di TIC**: valutazione e scansione delle vulnerabilità, analisi *open source* , valutazioni della sicurezza delle reti, analisi delle carenze, esami della sicurezza fisica, questionari e soluzioni di scansione del *software* , esami del codice sorgente, ove fattibile, test basati su scenari, test di compatibilità, test di prestazione, test *end-to-end* e *test* di penetrazione.
26, paragrafi 1,2,3,4,5,6,7,8,9 e 10	**Test avanzati di strumenti, sistemi e processi di TIC basati su test di penetrazione guidati dalla minaccia (TLPT)**: effettuati con cadenza almeno triennale (frequenza che può essere ridotta o aumentata, ove necessario, dall'autorità competente). Ciascun test di penetrazione guidato dalla minaccia riguarda alcune o tutte le funzioni essenziali o importanti dell'entità finanziaria ed è effettuato sui sistemi attivi di produzione a supporto di tali funzioni. Alla fine dei test, dopo che le relazioni e i piani correttivi siano stati concordati, l'entità finanziaria e, ove applicabile, i soggetti incaricato dello svolgimento dei test esterni trasmettono all'autorità designata una sintesi delle pertinenti risultanze, i piani correttivi e la documentazione attestante che i TLPT sono stati svolti conformemente ai requisiti.
27	**Requisiti per i soggetti incaricati dello svolgimento dei test di penetrazione basati su minacce** (alto grado di idoneità e reputazione; capacità tecniche e organizzative e con dimostrata esperienza specifica nel campo delle analisi delle minacce, dei test di penetrazione; siano certificati da un ente di accreditamento in uno Stato membro o rispettino codici formali di condotta; forniscano una garanzia indipendente o una relazione di *audit* concernente la solida gestione dei rischi e siano debitamente e pienamente coperti da un'assicurazione di responsabilità professionale, anche contro i rischi di colpa e negligenza) e necessità che il ricorso a tali soggetti sia stato approvato da parte dell'autorità competente.
28, paragrafi 1,2,3,4,5,6,7 e 8	**Principi generali di una solida gestione dei rischi informatici derivanti da terzi**. Adottano e riesaminano periodicamente una strategia per i rischi informatici derivanti da terzi, tenendo conto della strategia basata su una varietà di fornitori. Tale strategia comprende una politica per l'utilizzo dei servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi e si applica su base individuale e, se del caso, su base subconsolidata e consolidata.
29	**Valutazione preliminare del rischio di concentrazione delle TIC a livello di entità**.
30, paragrafi 1,2,3 e 4	**Principali disposizioni contrattuali** concernenti l'individuazione dei diritti e degli obblighi dell'entità finanziaria e del fornitore terzo di servizi TIC.
31, paragrafo 12	**Designazione di un fornitore terzo critico di servizi TIC stabilito in un paese terzo**, nel caso in cui detto fornitore abbia istituito un'impresa figlia nell'Unione entro 12 mesi dalla designazione.
45	**Meccanismi di condivisione delle informazioni** tra entità finanziarie.
51	Esercizio del **potere di imporre sanzioni amministrative e misure di riparazione** di cui all'articolo 50 del regolamento da parte dell'autorità di vigilanza competente.
54	**Pubblicazione delle sanzioni amministrative** senza indebito ritardo sul sito web ufficiale dell'autorità di vigilanza competente.
55	Obbligo del **segreto professionale** a tutte le persone che prestano o hanno prestato la loro attività per le autorità competenti sulle informazioni riservate ricevute, scambiate o trasmesse a norma del regolamento.
56	**Protezione dei dati**: le autorità competenti sono autorizzate a trattare i dati personali solo se necessario ai fini dell'adempimento dei rispettivi obblighi e doveri ai sensi del regolamento.

CAPO IV
(Poteri di vigilanza e sanzioni)

Articolo 8
(Poteri di vigilanza)

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.

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, nonché di quelli previsti dalla normativa di settore e dall'articolo in esame, nei confronti delle entità finanziarie, Cassa depositi e prestiti S.p.A., degli intermediari finanziari, di Bancoposta e dei fornitori terzi di servizi TIC a supporto di funzioni essenziali o importanti. Tali poteri vengono conferiti ai fini dello svolgimento dei compiti previsti dal regolamento DORA, dagli atti delegati e dalle norme tecniche di regolamentazione e di attuazione del medesimo regolamento, nonché dal presente decreto e dalle relative disposizioni attuative.

Sul punto, si segnala che tra i poteri di vigilanza previsti dal sopra citato articolo 50, paragrafo 2, si annoverano:

- l'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;
- lo svolgimento di 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;
- la richiesta dell'applicazione di misure correttive e di riparazione per le violazioni dei requisiti del regolamento DORA.

Inoltre, il menzionato articolo 42, paragrafo 6, prescrive che, a norma dell'articolo 50, le autorità competenti possono adottare, come misura di ultima istanza, a seguito della notifica e, se del caso, della consultazione di cui ai paragrafi 4 e 5 del medesimo articolo 42, 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.

Viene, altresì, specificato che **restano fermi i poteri** di cui le predette Autorità sono già titolari in forza degli articoli 51, 53-*bis*, 54 e 108 del decreto legislativo n. 385 del 1993 (TUB); dell'articolo 4, comma 4, del decreto legislativo n. 129 del 2024; degli articoli 6, comma 1, lettera *c*), 30-*septies*, 188, 189, 190, 205-*bis* del decreto legislativo n. 209 del 2005 (CAP); degli articoli 5-*septies* e 19 del decreto legislativo n. 252 del 2005, nei confronti dei soggetti ai quali siano state esternalizzate funzioni aziendali e del relativo personale. Restano, altresì, fermi i poteri di cui agli articoli 114-*quinquies*.2 e 114-*quaterdecies* del TUB e agli articoli 6-*bis*, 6-*ter*, 7 e 62-*novies* del decreto legislativo n. 58 del 1998 (TUF) e dell'articolo 22 della legge n. 262 del 2005.

Si riporta, di seguito, una tabella riepilogativa dei poteri previsti dalle disposizioni sopra menzionate.

Norma di riferimento	Tipologia di potere
Articolo 51 TUB	Vigilanza informativa da parte della Banca d'Italia sulle banche
Articolo 53-*bis* TUB	Poteri di intervento della Banca d'Italia
Articolo 54 TUB	Vigilanza ispettiva della Banca d'Italia
Articolo 108 TUB	Vigilanza della Banca d'Italia
Articolo 4, comma 4, d.lgs. n. 129 del 2024	Poteri generali di vigilanza e di indagine della Banca d'Italia e della Consob in materia di cripto-attività
Articolo 6, comma 1, lettera *c*), CAP	Vigilanza dell'IVASS nei confronti dei soggetti, enti e organizzazioni che in qualunque forma svolgono funzioni parzialmente comprese nel ciclo operativo delle imprese di assicurazione o di riassicurazione limitatamente ai profili assicurativi e riassicurativi, fermi restando i poteri nei confronti delle imprese di assicurazione o di riassicurazione per le attività esternalizzate
Articolo 30-*septies* CAP	Potere di vigilanza dell'IVASS in materia di esternalizzazione

Articolo 188 CAP	Poteri di intervento dell'IVASS
Articolo 189 CAP	Poteri di indagine dell'IVASS
Articolo 190 CAP	Vigilanza informativa da parte dell'IVASS nei confronti dei soggetti vigilati
Articolo 205-*bis* CAP	Vigilanza dell'IVASS sulle funzioni e le attività esternalizzate dalle imprese aventi sede in Italia
Articolo 5-*septies*, d.lgs. n. 252 del 2005	Potere di vigilanza della COVIP in materia di esternalizzazione
Articolo 19, d.lgs. n. 252 del 2005	Poteri di intervento, vigilanza e controllo della COVIP
Articolo 114-*quinquies*.2 TUB	Poteri di vigilanza della Banca d'Italia sugli istituti di moneta elettronica
Articolo 114-*quaterdecies* TUB	Poteri di vigilanza della Banca d'Italia sugli istituti di pagamento
Articolo 6-*bis* TUF	Poteri informativi e di indagine della Banca d'Italia in materia di intermediazione finanziaria
Articolo 6-*ter* TUF	Poteri ispettivi della Banca d'Italia e della Consob in materia di intermediazione finanziaria
Articolo 7 TUF	Poteri di intervento della Banca d'Italia e della Consob in materia di intermediazione finanziaria
Articolo 62-*novies* TUF	Poteri ispettivi della Banca d'Italia e della Consob nei confronti dei gestori delle sedi di negoziazione e di coloro ai quali i gestori medesimi abbiano esternalizzato funzioni operative essenziali o importanti e al loro personale
Articolo 22, legge n. 262 del 2005	Potere della Banca d'Italia, della CONSOB, dell'ISVAP, della COVIP e dell'Antitrust di avvalersi, nell'ambito delle attività di vigilanza informativa e ispettiva, a fini di accertamento, del Corpo della guardia di finanza, che agisce con i poteri ad esso attribuiti per l'accertamento dell'IVA e delle imposte sui redditi.

Articolo 9
(Poteri regolamentari)

L'**articolo 9** attribuisce alle Autorità competenti DORA il **potere di emanazione** di disposizioni attuative del presente decreto e del regolamento DORA.

La presente disposizione 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.

Articolo 10
(Sanzioni amministrative a altre misure)

L'**articolo 10** modifica il testo unico delle leggi in materia bancaria e creditizia (**comma 1**), il testo unico delle disposizioni in materia di intermediazione finanziaria (**comma 2**), il codice delle assicurazioni private (**comma 3**), il decreto legislativo n. 252 del 2005 recante le disciplina delle forme pensionistiche complementari (**comma 4**) e il 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.

I **commi 6-9** recano disposizioni concernenti i poteri di vigilanza, indagine e sanzionatori per l'adempimento - da parte delle Autorità competenti - dei compiti loro assegnati ai sensi del regolamento DORA e dettano le disposizioni relative a sanzioni amministrative o misure di riparazione per violazioni che sono passibili di sanzioni penali.

Si rammenta che l'art. 16, comma 2, lettere *b)* e *c)*, della legge n. 15 del 2024 (legge di delegazione europea 2022-2023) prevede che il Governo, nell'attuazione della delega: assicuri che alle autorità competenti siano attribuiti tutti i poteri di vigilanza, di indagine e sanzionatori per l'attuazione del regolamento (UE) 2022/2554 e della direttiva (UE) 2022/2556, coerentemente con il riparto di competenze nel settore finanziario nazionale; attribuisca alle suddette autorità il potere di imporre le sanzioni e le altre misure amministrative previste dagli articoli 42, paragrafo 6, e 50 del regolamento (UE) 2022/2554, nel rispetto dei limiti edittali e delle procedure previsti dalle disposizioni nazionali che disciplinano l'irrogazione delle sanzioni e l'applicazione delle altre misure amministrative da parte delle autorità anzidette, avuto riguardo al riparto di competenze nel settore finanziario nazionale.

Modifiche al testo unico delle leggi in materia bancaria e creditizia - TUB di cui al decreto legislativo n. 385 del 1993 (comma 1)

L'**articolo 10, comma 1, lettera *a)***, modifica l'articolo 144 TUB, concernente le sanzioni amministrative alle società o enti disciplinati dal medesimo testo unico, introducendo i commi 8-*bis* e 8-*ter*.

Il nuovo comma 8-*bis* riguarda le sanzioni applicabili per l'inosservanza dei seguenti articoli del regolamento (UE) 2022/2554 e delle relative norme tecniche di regolamentazione e attuazione:

i. art. 5, che pone in capo alle entità finanziarie l'obbligo di predisporre un quadro di gestione e di controllo interno che garantisca una gestione efficace e prudente di tutti i rischi informatici;
ii. art. 6, paragrafi 1, 2, 3, 4, 5, 6, 7 e 8, relativo alla predisposizione di un quadro per la gestione dei rischi informatici solido, esaustivo e adeguatamente documentato, che consenta di affrontare i rischi informatici in maniera rapida, efficiente ed esaustiva, assicurando un elevato livello di resilienza operativa digitale;
iii. art. 10, concernente i meccanismi di individuazione delle attività anomale, e dei potenziali singoli punti di vulnerabilità (*points of failure*) rilevanti;
iv. art. 12, concernente le politiche e le procedure e i metodi di ripristino e recupero (*backup*);
v. art. 16, paragrafi 1 e 2, inerente alle caratteristiche dei quadri semplificati per la gestione dei rischi informatici che devono essere approntati dai "soggetti esentati", ossia i soggetti ai quali non si applicano gli articoli da 5 a 15 del regolamento n. 2554;
vi. art. 17, sulla gestione degli incidenti connessi alle tecnologie dell'informazione e della comunicazione (TIC);
vii. art. 19, paragrafi 1, 3 e 4, sulle segnalazioni di gravi incidenti TIC e sulla notifica volontaria delle minacce informatiche significative;
viii. art. 24, inerente ai requisiti generali per lo svolgimento di *test* di resilienza operativa digitale che mirino a valutare la preparazione alla gestione degli incidenti connessi alle TIC, a identificare punti deboli, carenze e lacune della resilienza operativa digitale e ad attuare tempestivamente misure correttive (tali obblighi si applicano alle entità finanziarie diverse dalle microimprese).

In caso di inosservanza delle disposizioni del regolamento n. 2554 di cui ai suddetti punti i-viii si applica la sanzione amministrativa pecuniaria:

- **da euro 30.000 fino al 10 per cento del fatturato** nei confronti delle **banche**, degli **intermediari finanziari** e dei relativi **fornitori terzi di servizi TIC** (lettera *a)* del nuovo comma 8-*bis* dell'art. 144 TUB);
- **da euro 30.000 fino a euro 5 milioni ovvero fino al 10 per cento del fatturato**, quando tale importo è superiore a 5 milioni e il fatturato è disponibile e determinabile, nei confronti **degli istituti di pagamento**, degli **istituti di moneta elettronica** e dei relativi **fornitori terzi di servizi TIC** (lettera *b)* del nuovo comma 8-*bis* dell'art. 144 TUB).

Il nuovo comma 8-*ter* riguarda le sanzioni applicabili per l'inosservanza dei seguenti articoli del regolamento (UE) 2022/2554 e delle relative norme tecniche di regolamentazione e attuazione:

ix. art. 7, sulle caratteristiche (quali l'idoneità in relazione alle dimensioni delle operazioni, l'affidabilità, la capacità e la resilienza) dei sistemi, protocolli e strumenti di TIC che le entità finanziarie sono tenuti ad adottare;

x. art. 8, in materia di identificazione e di valutazione dei rischi alle operazioni delle TIC da parte delle entità finanziarie diverse dalle microimprese;

xi. art. 9, concernente la protezione e la prevenzione;

xii. art. 11, paragrafi 1, 2, 3, 4, 5, 6, 7, 8, 9 e 10, relativo alla predisposizione di una politica esaustiva di continuità operativa delle TIC, quale parte integrante della politica generale di continuità operativa dell'entità finanziaria;

xiii. art. 13, in materia di apprendimento ed evoluzione, con riferimento, tra l'altro, al riesame successivo agli incidenti, finalizzato all'analisi delle cause e all'identificazione dei miglioramenti che è necessario apportare alle operazioni riguardanti le TIC o nell'ambito della politica di continuità operativa delle TIC;

xiv. art. 14, in materia di piani di comunicazione delle crisi e di politiche di comunicazione per il personale interno e per i portatori di interessi esterni;

xv. art. 18, paragrafi 1 e 2, inerente alla classificazione degli incidenti connessi alle TIC e alle minacce informatiche, in relazione al numero e alla rilevanza di clienti o controparti finanziarie interessati, alla durata ed estensione geografica dell'incidente, nonché a perdite di dati, criticità dei servizi colpiti, impatto economico dell'incidente;

xvi. art. 25, sui *test* di strumenti e sistemi di TIC;

xvii. art. 26, paragrafi 1, 2, 3, 4, 5, 6, 7 e 8, sui *test* avanzati di strumenti, sistemi e processi di TIC basati su *test* di penetrazione guidati dalla minaccia (TLPT);

xviii. art. 27, sui requisiti per i soggetti incaricati dello svolgimento dei *test*;

xix. art. 28, paragrafi 2, 3, 4, 5, 6, 7 e 8, in materia di principi generali di una solida gestione dei rischi informatici derivanti da terzi;

xx. art. 29, sulla valutazione preliminare del rischio di concentrazione delle TIC che tenga conto delle conseguenze di eventuali conclusioni di accordi contrattuali relativi ai suddetti servizi TIC a supporto di funzioni essenziali o importanti;

xxi. art. 30, paragrafi 1, 2, 3 e 4, sugli elementi necessari degli accordi contrattuali per l'utilizzo di servizi TIC;

xxii. art. 31, paragrafo 12, il quale prevede che le entità finanziarie possano ricorrere ai servizi di un fornitore terzo di servizi TIC stabilito in un paese terzo e che è stato designato come critico (conformemente al paragrafo 1, lettera *a*), del medesimo art. 31) soltanto se detto fornitore ha istituito un'impresa figlia nell'Unione europea entro 12 mesi dalla designazione.

In caso di inosservanza delle disposizioni del regolamento n. 2554 di cui ai punti ix-xxii si applica la sanzione amministrativa pecuniaria:

- **da euro 30.000 fino al 7 per cento del fatturato** nei confronti delle **banche**, degli **intermediari finanziari** e dei relativi **fornitori terzi di servizi TIC** (lettera *a)* del nuovo comma 8-*ter* dell'art. 144 TUB);
- **da euro 30.000 fino a euro 3,5 milioni ovvero fino al 7 per cento del fatturato**, quando tale importo è superiore a euro 5 milioni e il fatturato è disponibile e determinabile, nei confronti **degli istituti di pagamento**, degli **istituti di moneta elettronica** e dei relativi **fornitori terzi di servizi TIC** (lettera *b)* del nuovo comma 8-*ter* dell'art. 144 TUB).

Le sanzioni disciplinate dal presente **comma 1, lettera *a)***, si applicano in caso di **omessa collaborazione o mancato seguito dato nell'ambito di un'indagine, ispezione o richiesta**.

L'**articolo 10, comma 1, lettera *b)***, modifica l'articolo 144-ter TUB concernente le sanzioni amministrative nei confronti di **soggetti che svolgono funzioni di amministrazione, di direzione o di controllo, nonché del personale**.

La disposizione in esame introduce, in primo luogo, i nuovi commi da 2-*bis* a 2-*quater* nel citato art. 144-*ter* TUB.

Il comma 2-*bis* prevede che alle **persone fisiche** si applichino le seguenti sanzioni amministrative pecuniarie, salvo che il fatto costituisca reato:

- **da euro 5.000 fino a euro 5 milioni**, nei casi di inosservanza delle disposizioni di cui ai punti i-viii del regolamento (lettere *a)* e *b)* del nuovo comma 8-*bis* dell'articolo 144 TUB);
- **da euro 5.000 fino a euro 3,5 milioni**, nei casi di inosservanza delle disposizioni di cui ai punti ix-xxii del regolamento (lettere *a)* e *b)* del nuovo comma 8-*ter* dell'articolo 144).

Il comma 2-*ter* specifica che le suddette sanzioni si applichino nei confronti dei soggetti 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 stabilisce che la sanzione è applicabile quando l'inosservanza è conseguenza della violazione di doveri propri o dell'organo di appartenenza e la condotta ha inciso in modo rilevante sulla complessiva organizzazione o sui profili di rischio aziendali. Inoltre, le sanzioni si applicano quando la condotta abbia determinato la non ottemperanza a provvedimenti ispettivi o di vigilanza adottati dalla Banca d'Italia oppure quando essa abbia contribuito a determinare l'inosservanza dell'ordine di porre termine al comportamento in violazione e di astenersi dal ripeterlo (di cui all'articolo 50, paragrafo 4, lettera *a)*, del regolamento n. 2554).

Il comma 2-*quater* stabilisce che se il vantaggio ottenuto dall'autore della violazione, se determinabile, è superiore all'ammontare delle sanzioni fissato dal comma 2-*bis*, la **sanzione pecuniaria è elevata fino al doppio del vantaggio ottenuto**.

Viene quindi prevista una modifica di mero coordinamento al comma 3 dell'art. 144-*ter* in questione.

Un nuovo comma 3-*bis* - di cui si propone l'introduzione - prevede la possibilità di applicare la sanzione amministrativa accessoria dell'**interdizione** dallo svolgimento di funzioni di amministrazione, direzione e controllo presso intermediari e imprese autorizzati ai sensi della normativa applicabile. L'interdizione è disposta per un periodo **non inferiore a sei mesi e non superiore a tre anni**.

Modifiche al testo unico delle disposizioni in materia di intermediazione finanziaria - TUF, di cui al decreto legislativo 24 febbraio 1998, n. 58 (comma 2)

Il **comma 2** introduce nel decreto legislativo n. 58 del 1998 un nuovo articolo 190-*bis*.3. Esso prevede, al comma 1, che in caso di inosservanza

delle disposizioni del regolamento n. 2554 di cui ai punti i-viii (v. sopra) si applichi la sanzione amministrativa pecuniaria:

- **da euro 30.000 fino a euro 5 milioni, ovvero fino al 10 per cento del fatturato**, quando tale importo è superiore a euro 5 milioni e il fatturato è determinabile, nei confronti delle **SIM** (società di intermediazione mobiliare), delle **SGR** (società di gestione del risparmio), delle **SICAV** (società di investimento a capitale variabile), delle **SICAF** (società di investimento a capitale fisso), delle **controparti centrali**, dei **gestori di mercati regolamentati** e dei relativi **fornitori terzi di servizi TIC** (art. 190-*bis*.3, co. 1, lettera *a)*);
- **da euro 30.000 fino a euro 20 milioni, ovvero fino al 10 per cento del fatturato**, quando tale importo è superiore a 20 milioni ed è determinabile, nei confronti dei **depositari centrali di titoli e dei relativi fornitori terzi di servizi TIC** (art. 190-*bis*.3, co. 1, lettera *b)*);
- **da euro 500 fino a euro 500.000, ovvero fino al 5 per cento del fatturato**, quando tale importo è superiore a euro 500.000 e il fatturato è determinabile, nei confronti dei **fornitori di servizi di *crowdfunding* e dei relativi fornitori terzi di servizi TIC** (art. 190-*bis*.3, co. 1, lettera *c)*);
- **da euro 10.000 fino a un milione, ovvero fino al 10 per cento del fatturato totale annuo**, quando tale importo è superiore a un milione e il fatturato è determinabile, nei confronti degli **amministratori di indici di riferimento critici e dei relativi fornitori terzi di servizi TIC** (art. 190-*bis*.3, co. 1, lettera *d)*).

Se le medesime violazioni sono compiute da **persona fisica**, salvo che il fatto costituisca reato si applicano le seguenti sanzioni (art. 190-*bis*.3, co. 2):

- **da euro 5.000 fino a euro 5 milioni**, nei casi di cui alle lettere *a)* e *b)*, del comma 1 (inerenti a SIM, SGE, SICAV, SICAF, controparti centrali, gestori mercati regolamentati, depositari centrali e relativi fornitori terzi di TIC);
- **da euro 500 fino a euro 500.000**, nei casi di cui alla lettera *c)* del comma 1 (inerente a fornitori di servizi di *crowdfunding* e relativi fornitori terzi di SIC);
- **da euro 5.000 fino a euro 500.000**, nei casi di cui alla lettera *d)* del comma 1 (inerente agli amministratori di indici di riferimento critici e dei relativi fornitori terzi di servizi TIC).

Il comma 3 del medesimo art. 190-*bis*.3 prevede che in caso di inosservanza delle disposizioni del regolamento n. 2554 di cui ai punti ix-xxii (v. sopra) si applica la sanzione amministrativa pecuniaria:

- **da euro 30.000 fino a euro 3,5 milioni, ovvero fino al 7 per cento del fatturato,** quando tale importo è superiore a euro 3,5 milioni ed è determinabile, nei confronti delle **SIM** (società di intermediazione mobiliare), delle **SGR** (società di gestione del risparmio), delle **SICAV** (società di investimento a capitale variabile), delle **SICAF** (società di investimento a capitale fisso), delle **controparti centrali**, dei **gestori di mercati regolamentati** e dei relativi **fornitori terzi di servizi TIC** (art. 190-*bis*.3, co. 3, lettera *a)*);
- **da euro 30.000 fino a euro 14 milioni, ovvero fino al 7 per cento del fatturato,** quando tale importo è superiore a euro 14 milioni ed è determinabile, nei confronti dei **depositari centrali di titoli e dei relativi fornitori terzi di servizi TIC** (art. 190-*bis*.3, co. 3, lettera *b)*);
- **da euro 500 fino a euro 350.000, ovvero fino al 3,5 per cento del fatturato**, quando tale importo è superiore e determinabile, nei confronti dei **fornitori di servizi di *crowdfunding* e dei relativi fornitori terzi di servizi TIC** (art. 190-*bis*.3, co. 3, lettera *c)*);
- **da euro 10.000 fino a euro 700.000, ovvero fino al 7 per cento del fatturato totale annuo**, quando tale importo è e determinabile, nei confronti degli **amministratori di indici di riferimento critici e dei relativi fornitori terzi di servizi TIC** (art. 190-*bis*.3, co. 3, lettera *d)*).

Se le medesime violazioni di cui ai punti ix-xxii (v. sopra) sono compiute da **persona fisica**, salvo che il fatto costituisca reato, si applicano le seguenti sanzioni (art. 190-*bis*.3, co. 4):

- **da euro 5.000 fino a euro 3,5 milioni**, nei casi di cui alle lettere *a)* e *b)*, del comma 3 (inerenti a SIM, SGE, SICAV, SICAF, controparti centrali, gestori mercati regolamentati, depositari centrali e relativi fornitori terzi di TIC);
- **da euro 500 fino a euro 350.000**, nei casi di cui alla lettera *c)* del comma 3 (inerente a fornitori di servizi di *crowdfunding* e relativi fornitori terzi di SIC);
- **da euro 5.000 fino a euro 350.000**, nei casi di cui alla lettera *d)* del comma 3 (inerente agli amministratori di indici di riferimento critici e dei relativi fornitori terzi di servizi TIC).

Il comma 5 dell'art. 190-*bis*.3 specifica che le sanzioni di cui ai commi 2 e 4 si applicano nei confronti dei soggetti 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 specifica che la sanzione è applicabile quando l'inosservanza è conseguenza della violazione di doveri propri o dell'organo di appartenenza e la condotta ha inciso in modo rilevante sulla complessiva organizzazione o sui profili di rischio aziendali. Si applica la sanzione, inoltre, quando la condotta abbia determinato la non ottemperanza a provvedimenti ispettivi o di vigilanza adottati dalla Banca d'Italia o dalla Consob (secondo le rispettive competenze) oppure quando essa abbia contribuito a determinare l'inosservanza dell'ordine di porre termine al comportamento in violazione e di astenersi dal ripeterlo (di cui all'articolo 50, paragrafo 4, lettera *a)*, del regolamento n. 2554).

Il comma 6 stabilisce che se il vantaggio ottenuto dall'autore della violazione, se determinabile, è superiore all'ammontare massimo delle sanzioni fissato dai commi da 1 a 4, la **sanzione pecuniaria è elevata fino al doppio del vantaggio ottenuto**.

Il comma 7 prevede la possibilità di applicare la sanzione amministrativa accessoria dell'**interdizione** dallo svolgimento di funzioni di amministrazione, direzione e controllo presso intermediari e imprese autorizzati ai sensi della normativa applicabile, in ragione della gravità della violazione. L'interdizione è disposta per un periodo **non inferiore a sei mesi e non superiore a tre anni**.

Il comma 8 dell'art. 190-*bis*.3 stabilisce che le sanzioni amministrative in oggetto sono applicate dalla Banca d'Italia o dalla Consob, secondo le rispettive competenze, applicando la procedura sanzionatoria disciplnata dal TUF medesimo.

Modifiche al codice delle assicurazioni private, di cui al decreto legislativo 7 settembre 2005, n. 209 (comma 3)

Il **comma 3, lettera *a)***, reca novelle all'articolo 310 del codice delle assicurazioni private rubricato "Sanzioni amministrative pecuniarie".

Inserendo una nuova lettera *c-bis)* al comma 1, la novella prevede l'applicazione della sanzione amministrativa pecuniaria **da 30.000 euro al 10 per cento del fatturato** in caso di violazione delle disposizioni del regolamento n. 2554 di cui ai punti i-viii (vedi sopra) da parte delle **imprese di assicurazione e di riassicurazione e i relativi fornitori terzi di TIC**.

La violazione delle disposizioni di cui ai punti xi-xxii comporta l'applicazione, nei confronti dei medesimi soggetti, di una sanzione **da 30.000 euro al 7 per cento del fatturato** (nuovo comma 1-*bis* di cui si propone l'inserimento nel medesimo art. 310 del codice)**.**

Le medesime sanzioni si applicano in caso di omessa collaborazione o mancato seguito alle indagini, ispezioni o richieste.

Ulteriore modifica riguarda il comma 2 dell'art. 310 citato. Se il vantaggio ottenuto dall'autore delle violazioni di cui al comma 1, lettera *c-bis*) è superiore al massimo edittale ivi indicato, la sanzione amministrativa pecuniaria è **elevata fino al doppio dell'ammontare del vantaggio ottenuto**, purché tale ammontare sia determinabile.

La **lettera *b)*** inserisce i nuovi commi 2-*bis*, 2-*ter* e 3-*bis* nell'art. 311-*sexies* del codice medesimo rubricato "sanzioni amministrative agli esponenti aziendali o al personale".

Il comma 2-*bis* prevede che se le violazioni sono compiute da **persona fisica**, si applica la sanzione amministrativa:

- **da euro 5.000 fino a euro 5 milioni**, nei casi previsti dal comma 1, lettera *c-bis*) dell'articolo 310;
- **da euro 5.000 fino a euro 3,5 milioni**, nei casi previsti dal comma 1-*bis* dell'articolo 310.

Il comma 2-*ter* specifica che le suddette sanzioni si applicano nei confronti dei soggetti 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 specifica che la sanzione è applicabile quando l'inosservanza è conseguenza della violazione di doveri propri o dell'organo di appartenenza e la condotta ha inciso in modo rilevante sulla complessiva organizzazione o sui profili di rischio aziendali. Si applica inoltre quando la condotta abbia determinato la non ottemperanza a provvedimenti ispettivi o di vigilanza adottati dall'IVASS oppure quando essa abbia contribuito a determinare l'inosservanza dell'ordine di porre termine al comportamento in violazione e di astenersi dal ripeterlo (di cui all'articolo 50, paragrafo 4, lettera *a)*, del regolamento n. 2554).

Viene quindi introdotto un nuovo comma 3-*bis*. Esso prevede la possibilità di applicare la sanzione amministrativa accessoria dell'**interdizione** dallo svolgimento di funzioni di amministrazione, direzione e controllo in ragione della gravità della violazione. L'interdizione è disposta per un periodo **non inferiore a sei mesi e non superiore a tre anni**.

La **lettera *c)*** inserisce i nuovi commi da 7-*ter* a 7-*octies* nell'art. 324 del codice delle assicurazioni recante "Sanzioni relative alle violazioni delle disposizioni in materia di realizzazione e di distribuzione dei prodotti assicurativi, inclusi i prodotti di investimento assicurativo, commesse dagli intermediari".

I commi 7-*ter* e 7-*quater* fissano le **sanzioni applicabili agli intermediari assicurativi, agli intermediari riassicurativi, agli intermediari assicurativi a titolo accessorio e dei relativi fornitori terzi di servizi TIC**.

A tali soggetti si applicano le sanzioni previste dal medesimo art. 324, comma 1, lettera *c)*, numero 1), del codice in caso di violazioni delle disposizioni del regolamento n. 2554 di cui ai punti i-viii. Si tratta pertanto delle sanzioni amministrative pecuniarie **da 5.000 euro a 5 milioni di euro oppure, se superiore, il cinque per cento del fatturato complessivo annuo** risultante dall'ultimo bilancio disponibile approvato dall'organo di amministrazione.

In caso di inosservanza delle sanzioni di cui ai punti ix-xxii, si applica, ai medesimi soggetti, la sanzione amministrativa pecuniaria **da 5.000 euro a 3,5 milioni di euro oppure, se superiore, pari al 3,5 per cento del fatturato complessivo annuo** risultante dall'ultimo bilancio disponibile approvato dall'organo di amministrazione.

Le medesime sanzioni si applicano anche in caso di mancata ottemperanza di provvedimenti ispettivi o di vigilanza.

Il comma 7-*quinquies* stabilisce che, salvo che il fatto costituisca reato, nei confronti della **persona fisica** si applica una sanzione amministrativa pecuniaria:

- da **1.000 euro a 700.000 euro** (comma 1, lettera c), numero 2) dell'art. 324 del codice) in caso di violazione delle disposizioni del regolamento di cui ai punti i-xiii (si tratta dei casi di cui al comma 7-*ter*);
- da **1.000 fino a 500.000 euro**, in caso di violazione delle disposizioni del regolamento di cui ai punti ix-xxii (si tratta dei casi di cui al comma 7-*quater*).

Il comma 7-*sexies* specifica che le suddette sanzioni si applicano nei confronti dei soggetti 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 specifica che la sanzione è applicabile quando l'inosservanza è conseguenza della violazione di doveri propri o dell'organo di appartenenza e la condotta ha inciso in modo rilevante sulla complessiva organizzazione o sui profili di rischio aziendali o ha contribuito a determinare la mancata ottemperanza della società. Si applica inoltre quando la condotta abbia determinato la non ottemperanza a provvedimenti ispettivi o di vigilanza adottati dall'IVASS oppure quando essa abbia contribuito a determinare l'inosservanza dell'ordine di porre termine al comportamento in violazione e di astenersi dal ripeterlo (di cui all'articolo 50, paragrafo 4, lettera *a)*, del regolamento n. 2554).

Il comma 7-*septies* stabilisce che se il vantaggio ottenuto dall'autore della violazione, se determinabile, è superiore all'ammontare massimo delle sanzioni fissato dai commi 7-*ter*, 7-*quater* e 7-*quinquies*, la **sanzione pecuniaria è elevata fino al doppio del vantaggio ottenuto**.

Il comma 7-*octies* prevede la possibilità di applicare la sanzione amministrativa accessoria dell'**interdizione** in ragione della gravità della violazione, per un periodo **non inferiore a sei mesi e non superiore a tre anni**, per lo svolgimento di funzioni di amministrazione, direzione e controllo presso intermediari e imprese autorizzati ai sensi della normativa applicabile.

Modifiche al decreto legislativo 5 dicembre 2005, n. 252 ("Disciplina delle forme pensionistiche complementari")

Il **comma 4** dell'articolo in esame inserisce nell'articolo 19-*quater* del decreto legislativo n. 252 del 2005 i nuovi commi 2-*bis* e 2-*ter*.

Il comma 2-*bis* assoggetta i componenti degli organi di amministrazione e di controllo, i direttori generali, i titolari delle funzioni fondamentali, i responsabili delle forme pensionistiche complementari, i liquidatori e i commissari dei fondi pensione (soggetti individuati dal comma 2 del medesimo art. 19-*quater*) alla sanzione amministrativa pecuniaria **da euro 500 a euro 25.000** (stabilita dal comma 2, lettera *b*), del medesimo art. 19-*quater*) in caso di inosservanza, in relazione alle rispettive competenze, delle disposizioni del regolamento n. 2554 menzionate in precedenza[1] e delle relative norme tecniche di regolamentazione e attuazione.

I medesimi soggetti, quando omettono di collaborare o dar seguito ad indagine, ispezione o richiesta, sono puniti con la sanzione amministrativa del pagamento di una somma **da euro 5.000 a euro 25.000** (sanzione di cui al comma 2, lettera *a)*, del medesimo articolo 19-*quater*).

Alle sanzioni in oggetto (comma 2-*ter*) si applica quanto previsto dall'art. 19-*quater*, commi:

- 3, il quale prevede che la COVIP, nei casi di maggiore gravità, può dichiarare decaduti dall'incarico i componenti degli organi collegiali, il direttore generale, il responsabile della forma pensionistica e i titolari delle funzioni fondamentali;
- 4 (ad eccezione del secondo periodo), stabilendo così l'applicazione alle sanzioni in oggetto di quanto previsto in materia di sanzioni amministrative dalla legge n. 689 del 1981, ad eccezione delle norme sul pagamento in misura ridotta (dettate dall'art. 16 della medesima legge n. 689); tale comma 4 prevede, altresì, che i fondi pensione e le società istitutrici di forme pensionistiche complementari

[1] Articoli 5, 6, paragrafi 1, 2, 3, 4, 5, 6, 7 e 8, 7, 8, 9, 10, 11, paragrafi 1, 2, 3, 4, 5, 6, 7, 8, 9 e 10, 12, 13, 14, 16, paragrafi 1 e 2, 17, 18, paragrafi 1 e 2, 19, paragrafi 1, 3 e 4, 24, 25, 26, paragrafi 1, 2, 3, 4, 5, 6, 7 e 8, 27, 28, paragrafi 2, 3, 4, 5, 6, 7 e 8, 29, 30, paragrafi 1, 2, 3 e 4, e 31, paragrafo 12, del suddetto regolamento (UE) 2022/2554.

rispondono in solido del pagamento della sanzione, salvo il diritto di regresso per l'intero nei confronti del responsabile della violazione; prevede inoltre che i fondi dotati di soggettività giuridica siano obbligati ad agire in regresso, salvo diversa deliberazione assembleare;

- 4-*bis*, prevedendo così che si applichi l'articolo 8, comma 2, della citata legge n. 689, concernente l'irrogazione della sanzione anche a chi, con più azioni od omissioni, esecutive di un medesimo disegno posto in essere in violazione di norme che stabiliscono sanzioni amministrative, commette, anche in tempi diversi, più violazioni della stessa o di diverse norme di legge in materia di previdenza ed assistenza obbligatorie.

Modifiche al decreto legislativo 5 dicembre 2024, n. 129 ("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")

Il **comma 5** introduce l'articolo 37-*bis* nel decreto legislativo n. 129 del 2024 in materia di **cripto-attività**.

Il comma 1 di tale art. 37-bis prevede l'applicazione delle seguenti sanzioni in caso di inosservanza delle disposizioni di cui ai punti i-viii e delle relative norme tecniche:

- **da euro 30.000 fino a euro 5 milioni,** ovvero, se superiore, fino **al 12,5 per cento del fatturato totale annuo** nei confronti degli **emittenti di *token*** collegati ad attività e dei **relativi fornitori terzi di servizi TIC**;
- **da euro 30.000 fino a euro 5 milioni,** ovvero, se superiore, fino al **5 per cento del fatturato totale annuo** nei confronti dei **prestatori di servizi in cripto-attività e dei relativi fornitori terzi di servizi TIC.**

Il comma 2 prevede che in caso di inosservanza delle disposizioni si cui ai punti ix-xxi e delle relative norme tecniche si applichi la sanzione amministrativa pecuniaria:

- **da euro 30.000 fino a euro 3,5 milioni,** ovvero, se superiore, fino al **9 per cento del fatturato totale annuo** nei confronti degli **emittenti di *token*** collegati ad attività e **dei relativi fornitori terzi di servizi TIC**;
- **da euro 30.000 fino a euro 3,5 milioni,** ovvero, se superiore, fino al **3,50 per cento del fatturato totale annuo** nei confronti dei

prestatori di servizi in cripto-attività e dei relativi fornitori terzi di servizi TIC.

Il comma 3 dispone circa le sanzioni nei confronti delle **persone fisiche**, nei confronti delle quali, salvo che il fatto non costituisca reato, si applica una sanzione amministrativa pecuniaria:

- **da euro 5.000 fino a euro 700.000**, nei casi al comma 1;
- **da euro 5.000 fino a euro 500.000**, nei casi al comma 2.

Il comma 4 specifica che le suddette sanzioni si applicano nei confronti dei soggetti 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 specifica che la sanzione è applicabile quando l'inosservanza è conseguenza della violazione di doveri propri o dell'organo di appartenenza e la condotta ha inciso in modo rilevante sulla complessiva organizzazione o sui profili di rischio aziendali. Si applica inoltre quando la condotta abbia determinato la non ottemperanza a provvedimenti ispettivi o di vigilanza adottati dalla Banca d'Italia o dalla Consob, secondo le rispettive cometenze, oppure quando essa abbia contribuito a determinare l'inosservanza dell'ordine di porre termine al comportamento in violazione e di astenersi dal ripeterlo (di cui all'articolo 50, paragrafo 4, lettera *a)*, del regolamento n. 2554).

Il comma 5 stabilisce che se il vantaggio ottenuto dall'autore della violazione, se determinabile, è superiore all'ammontare massimo delle sanzioni fissato dai commi 1, 2 e 3, la **sanzione pecuniaria è elevata fino al doppio dell'ammontare del vantaggio ottenuto**.

Il comma 6 prevede la possibilità di applicare la sanzione amministrativa accessoria dell'**interdizione** in ragione della gravità della violazione. L'interdizione è disposta per un periodo **non inferiore a sei mesi e non superiore a tre anni**, per lo svolgimento di funzioni di amministrazione, direzione e controllo presso intermediari e imprese.

Il comma 8 stabilisce che le sanzioni amministrative in oggetto sono applicate dalla Banca d'Italia o dalla Consob secondo le rispettive competenze e applicando la procedura sanzionatoria, come disciplinata dal testo unico in materia di intermediazione finanziaria, agli articoli 195 e 196-*ter*.

Altre misure (commi 6-9)

L'**articolo 10, comma 6**, dello schema di decreto in esame, stabilisce che, laddove le violazioni di cui 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.

CAPO V
(Ulteriori modificazioni e integrazioni della normativa di settore e disposizioni di coordinamento)

Articolo 11
(Modifiche al testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58)

L'**articolo 11** prescrive l'adozione di procedure, dispositivi e sistemi da parte dei mercati regolamentati, al fine di individuare rischi informatici e attutirne le conseguenze nei casi in cui essi si concretizzassero.

L'**articolo 11,** formato da un comma unico suddiviso in due lettere, 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. In funzione di tali obbiettivi, **l'articolo 11 novella gli articoli 65 e 65-*sexies* del testo unico delle disposizioni in materia di intermediazione finanziaria,** cioè il **decreto legislativo 24 febbraio 1998, n. 58.**

Pertanto, al **comma 1 dell'articolo 65 del decreto legislativo 58/1998, la lettera *b*)** viene sostituita e la **lettera *c*) è abrogata.** La **nuova versione** della **lettera *b*) del comma 1 dell'articolo 65 del decreto legislativo 58/1998** formulata **dall'articolo 11 dell'Atto del Governo in commento** si differenzia dalla precedente in quanto introduce un esplicito riferimento ai rischi informatici e al **Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022** relativo alla resilienza operativa digitale per il settore finanziario. La vigente **lettera *c*) del comma 1 dell'articolo 65 del decreto legislativo 58/1998** che si intende abrogare parla genericamente 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.

L'attuale articolo **65-*sexies* del testo unico delle disposizioni in materia di intermediazione finanziaria** è dedicato ai requisiti operativi delle sedi di negoziazione. Il **nuovo testo del comma 1 di tale articolo** fa del concetto di resilienza operativa nonché del **Regolamento (UE) 2022/2554** i riferimenti essenziali dei requisiti operativi di cui le sedi di negoziazione dei mercati regolamentati devono essere dotate. Rispetto alle disposizioni vigenti, la descrizione dei requisiti operativi necessari subisce qualche modifica nella forma, ma non nella sostanza.

Articolo 12
(Modifica al codice delle assicurazioni private, di cui al decreto legislativo 7 settembre 2005, n. 209)

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

L'**articolo 12 dell'Atto del Governo all'esame del Parlamento** riguarda le misure che le società assicurative private sono tenute a adottare al fine di garantire la continuità e la regolarità dell'attività che esse esercitano. Tra le suddette misure, sono compresi i piani di emergenza.

L'articolo 12 in commento interviene nella disciplina del settore in forma di novella, **sostituendo il vigente comma 4 dell'articolo 30 del decreto legislativo 7 settembre 2005, n. 209, Codice delle assicurazioni private, con un nuovo comma 4.**

Fermo restando che le imprese assicurative devono adottare misure ragionevoli idonee a garantire la continuità e la regolarità dell'attività esercitata, inclusa l'elaborazione di piani di emergenza, utilizzando a tali scopi adeguati e proporzionati sistemi, risorse e procedure interne, **la nuova versione proposta del comma 4 dell'articolo 30 del decreto legislativo 209/2005** afferma che in questo quadro occorrerà istituire e gestire sistemi informatici e di rete, conformemente al **Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022** relativo alla resilienza operativa digitale per il settore finanziario.

Articolo 13
(Adozione di misure di garanzia da parte dei fondi pensione)

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[2] dai soggetti promotori dell'iniziativa[3]. 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 (regolamento oggetto del presente schema di decreto).

La disciplina già vigente prevede che i fondi pensione appartenenti alle summenzionate categorie debbano adottare misure appropriate – quest'ultima qualificazione viene sostituita, nella presente novella, con il termine ragionevoli – atte a garantire la continuità e la regolarità dello svolgimento delle loro attività – tra cui l'elaborazione di piani di emergenza – mediante l'utilizzo di sistemi, risorse e procedure adeguati e proporzionati.

La novella, come detto, specifica che tra le misure di garanzia in oggetto rientrano l'istituzione e la gestione di sistemi informatici e di rete conformemente al regolamento (UE) 2022/2554, ove applicabile.

[2] Cfr. gli articoli da 36 a 42-*bis* del codice civile.

[3] La novella di cui al presente **articolo 13** concerne l'articolo 4-*bis*, comma 6, del D.Lgs. 5 dicembre 2005, n. 252; riguardo all'individuazione delle suddette categorie di fondi pensione, cfr. il comma 1 del medesimo articolo 4-*bis* e il comma 1 dell'articolo 4 dello stesso D.Lgs.

Articolo 14
(Modifiche al decreto legislativo 16 novembre 2015, n. 180)

L'**articolo 14** apporta le 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.

Nello specifico, l'**articolo 14** dispone le necessarie modifiche alla disciplina contenuta 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, a seguito dell'attuazione nell'ordinamento nazionale del regolamento (UE) 2022/2554.

Come chiarito dal Governo nella relazione illustrativa, per quanto riguarda gli interventi della direttiva DORA (direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio) 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.

La Direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio - 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 del settore finanziario

La Direttiva in titolo ha lo scopo di introdurre modifiche mirate alle direttive UE vigenti in materia di servizi finanziari per allinearle ai requisiti stabiliti dal regolamento sulla resilienza operativa digitale del settore finanziario (DORA).

In particolare, e sinteticamente, la direttiva di modifica fa parte del pacchetto sulla finanza digitale. Introduce modifiche mirate alle direttive UE esistenti in materia di servizi finanziari per allinearle ai requisiti in materia di reti e sistemi informativi e di gestione e rendicontazione del rischio legato alle tecnologie dell'informazione della comunicazione (TIC) stabiliti dal regolamento sulla resilienza operativa digitale del settore finanziario (regolamento DORA) e chiarisce alcune disposizioni per garantire che i rischi legati alle siano pienamente affrontati.

La direttiva prevede una serie di modifiche che appaiono necessarie per portare chiarezza e coerenza giuridica in relazione all'applicazione, da parte dei soggetti finanziari autorizzati e vigilati in conformità a tali direttive, di vari requisiti di resilienza operativa digitale necessari nell'esercizio delle loro attività, garantendo così il buon funzionamento del mercato interno.

La direttiva sottolinea la necessità di garantire l'adeguatezza di tali requisiti in relazione agli sviluppi del mercato, incoraggiando al contempo la proporzionalità, in particolare per quanto riguarda le dimensioni delle entità finanziarie e i regimi specifici a cui sono soggette, con l'obiettivo di ridurre i costi di conformità.

La direttiva modifica i vari requisiti in materia di rischio operativo o di gestione del rischio previsti dalle seguenti direttive:

- 2009/65/CE sul coordinamento delle disposizioni legislative, regolamentari e amministrative in materia di organismi di investimento collettivo in valori mobiliari,
- 2009/138/UE sull'accesso e l'esercizio delle attività di assicurazione e riassicurazione,
- 2011/61/UE sui gestori di fondi di investimento alternativi,
- 2013/36/UE sull'accesso all'attività degli enti creditizi e sulla regolamentazione prudenziale degli enti creditizi e delle imprese di investimento,
- 2014/65/UE sui mercati degli strumenti finanziari,
- 2015/2366/UE sui servizi di pagamento nel mercato interno,
- 2016/2341/UE sulle attività e la vigilanza degli enti aziendali o professionali

La direttiva è entrata in vigore il 16 gennaio 2023.

Articolo 15
(Disposizioni di coordinamento con il decreto legislativo 4 settembre 2024, n. 138)

L'**articolo 15** stabilisce che a Bancoposta non si applicano le disposizioni di cui all'articolo 17, in tema di cooperazione internazionale, e ai Capi IV, sulle misure di gestione del rischio di cibersicurezza, e V, in tema di giurisdizione e registrazione, del decreto n.138 del 2024 di recepimento della direttiva NIS2.

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

CAPO VI
(Disposizioni finali)

Articolo 16
(Clausola di invarianza finanziaria)

L'**articolo 16** contiene la clausola di invarianza finanziaria.

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.

Articolo 17
(Entrata in vigore)

L’**articolo 17** dispone l’entrata in vigore, fissandola al 17 gennaio 2025.

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.