dossier

XIX Legislatura

26 ottobre 2026

Schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale al regolamento (UE), relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali

Atto del Governo n. 447

Ai sensi degli articoli 1 e 15 della legge 17 marzo 2026, n. 36

Senato della Repubblica

Camera dei deputati

Senato della Repubblica

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

Dossier n. 785

Camera dei deputati

SERVIZIO STUDI
Dipartimento Istituzioni
Tel. 06 6760-3855 - ✉ st_istituzioni@camera.it @CD_istituzioni

Dipartimento Trasporti
Tel. 06 6760-2614 - ✉ st_trasporti@camera.it @CD_trasporti

SERVIZIO PER I RAPPORTI CON L'UNIONE EUROPEA
Tel. 066760-2145-✉ rue_segreteria@camera.it-@CD_europa–europa.camera.it

Atti del Governo n. 447

La documentazione dei Servizi e degli Uffici del Senato della Repubblica e della Camera dei deputati è destinata alle esigenze di documentazione interna per l'attività degli organi parlamentari e dei parlamentari. Si declina ogni responsabilità per la loro eventuale utilizzazione o riproduzione per fini non consentiti dalla legge. I contenuti originali possono essere riprodotti, nel rispetto della legge, a condizione che sia citata la fonte.

I N D I C E

SCHEDE DI LETTURA

CAPO I – DISPOSIZIONI GENERALI.....5

- Articolo 1 *(Oggetto)* 5
- Articolo 2 *(Definizioni)* 9
- Articolo 3 *(Atti di indirizzo)* 12
- Articolo 4 *(Autorità di notifica)* 14
- Articolo 5 *(Domanda e procedura di designazione e notifica degli organismi di valutazione di conformità)* 16
- Articolo 6 *(Modifiche delle notifiche)* 18
- Articolo 7 *(Ricorso contro le decisioni degli organismi notificati)* 20
- Articolo 8 *(Raccordo informativo con l'autorità di notifica ai sensi del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024)* 21
- Articolo 9 *(Autorità di vigilanza del mercato)*.....23
- Articolo 10 *(Poteri e misure di vigilanza del mercato dell'Agenzia)* 27
- Articolo 11 *(Poteri di vigilanza delle Autorità del settore finanziario e del Garante per la protezione dei dati personali)* 31
- Articolo 12 *(Collaborazione tra Autorità)* 34
- Articolo 13 *(Collaborazione dell'Agenzia e delle autorità del settore finanziario con il Garante per la protezione dei dati personali)*.....36
- Articolo 14 *(Reclami alle autorità di vigilanza del mercato e segnalazioni al CSIRT Italia)* 38

CAPO IV – DISPOSIZIONI SANZIONATORIE 40

- Articolo 15 *(Poteri sanzionatori delle autorità di vigilanza del mercato e procedimento di irrogazione delle sanzioni)*.....40
- Articolo 16 *(Devoluzione dei proventi)*.....46

CAPO V – MISURE PER LE MICROIMPRESE E LE PICCOLE IMPRESE E DI SEMPLIFICAZIONE.....48

- Articolo 17 *(Terminale per le segnalazioni al CSIRT Italia)*.....48
- Articolo 18 *(Misure per le microimprese e le piccole e medie*

imprese, comprese le start-up*)*.....50

CAPO VI – SPAZI DI SPERIMENTAZIONE NORMATIVA 52

- Articolo 19 *(Istituzione e gestione dello spazio di sperimentazione normativa per la ciberresilienza)*.....52
- Articolo 20 *(Promozione dell'innovazione e coordinamento con gli altri spazi di sperimentazione)* 55

CAPO VII – ULTERIORI MODIFICAZIONI E INTEGRAZIONI DELLA NORMATIVA DI SETTORE E DISPOSIZIONI DI COORDINAMENTO 58

- Articolo 21 *(Modifiche al decreto legislativo 12 ottobre 2022, n. 157)*.....58
- Articolo 22 *(Funzioni dell'Agenzia per la cybersicurezza nazionale)* 62
- Articolo 23 *(Modifiche al codice del consumo, di cui al decreto legislativo 6 settembre 2005, n. 206)* 64

CAPO VIII – DISPOSIZIONI TRANSITORIE, FINANZIARIE E FINALI 66

- Articolo 24 *(Attuazione da parte dell'Agenzia per la cybersicurezza nazionale degli obblighi di cui al decreto legislativo 12 ottobre 2022, n. 157)* 66
- Articolo 25 *(Abrogazioni)* 67
- Articolo 26, commi 1-3 *(Disposizioni finanziarie)* 71
- Articolo 26, comma 4 *(Personale dell'Agenzia per la cybersicurezza nazionale)* 73
- Articolo 27 *(Protezione dei dati e riservatezza)* 77

Schede di lettura

CAPO I – DISPOSIZIONI GENERALI

Articolo 1
(Oggetto)

L'**articolo 1** specifica l'**oggetto** del presente schema di decreto legislativo.

Preliminarmente, si ricorda che lo schema di decreto in esame attua la delega conferita al Governo dall'articolo 15 della **legge n. 36 del 2026** (legge di delegazione europea 2025) ai fini dell'adeguamento della normativa nazionale al **regolamento (UE) 2024/2847** (c.d. *Cyber Resilience Act*), relativo ai **requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali**. Il termine di delega è di sei mesi a partire dal 9 aprile 2026, data di entrata in vigore della predetta legge.

Il citato articolo 15 della legge n. 36 del 2026 individua, al comma 2, in aggiunta ai princìpi e criteri direttivi generali previsti all'articolo 32 della legge n. 234 del 2012, anche i seguenti princìpi e criteri direttivi specifici:

- apportare alla normativa vigente tutte le modifiche e le integrazioni necessarie ad assicurare la corretta e integrale applicazione del regolamento (UE) 2024/2847 e delle pertinenti norme tecniche di regolamentazione e di attuazione, garantendo il coordinamento, con le disposizioni del decreto-legge n. 105 del 2019 e col decreto legislativo n. 138 del 2024, nonché con le disposizioni settoriali in vigore;
- individuare l'Agenzia per la cybersicurezza nazionale quale autorità di notifica ai sensi dell'articolo 36 del regolamento (UE) 2024/2847;
- individuare l'Agenzia per la cybersicurezza nazionale quale autorità di vigilanza del mercato ai sensi dell'articolo 52 del regolamento (UE) 2024/2847, in relazione ai requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali;
- prevedere forme di coordinamento tra l'Agenzia per la cybersicurezza nazionale, nel ruolo di autorità di notifica e di autorità di vigilanza del mercato, e le altre autorità nazionali competenti individuate dal decreto legislativo n. 157 del 2022, nonché tra le altre pubbliche amministrazioni e le autorità indipendenti, ai fini dello svolgimento dei compiti discendenti dal regolamento (UE) 2024/2487;
- adeguare e raccordare alle disposizioni del regolamento (UE) 2024/2847 le disposizioni nazionali vigenti e, in particolare, le modalità e le procedure di vigilanza, sorveglianza del mercato e controllo della

sicurezza cibernetica dei prodotti con elementi digitali, con abrogazione espressa delle norme nazionali incompatibili;

- definire il sistema sanzionatorio prevedendo sanzioni effettive, dissuasive e proporzionate alla gravità e alla durata ed all'eventuale reiterazione della violazione degli obblighi derivanti dal regolamento (UE) 2024/2847. Si prevede, in particolare, che ciò avvenga:
  - anche in deroga ai criteri e ai limiti previsti dall'articolo 32, comma 1, lettera *d*), della legge n. 234 del 2012;
  - in coordinamento con il sistema sanzionatorio previsto dal decreto-legge n. 105 del 2019 e dal decreto legislativo n. 138 del 2024, in coerenza, quanto al procedimento applicabile, con quanto previsto dall'articolo 17, comma 4-*quater*, del decreto-legge n. 82 del 2021;
  - apportando alla normativa vigente le necessarie modificazioni, anche al fine di introdurre misure deflattive del procedimento sanzionatorio o del contenzioso;
  - prevedendo che gli introiti derivanti dall'irrogazione delle sanzioni siano versati all'entrata del bilancio dello Stato per essere riassegnati all'apposito capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze, di cui all'articolo 18 del decreto-legge n. 82 del 2021 per incrementare la dotazione del bilancio dell'Agenzia per la cybersicurezza nazionale;
- garantire che l'Agenzia per la cybersicurezza nazionale disponga di adeguate risorse umane, strumentali e finanziarie per lo svolgimento dei compiti previsti dal regolamento (UE) 2024/2847.

Ciò premesso, l'**articolo 1** in esame chiarisce che il presente schema di decreto contiene le **disposizioni necessarie all'adeguamento** della normativa nazionale alla disciplina recata dal **regolamento (UE) 2024/2847** (c.d. *Cyber Resilience Act*) e alle pertinenti **norme tecniche di regolamentazione e di attuazione**, nonché al **coordinamento** con la legislazione di settore attualmente vigente.

- ***Regolamento (UE) 2024/2847***

Il regolamento (UE) 2024/2847 (c.d. *Cyber Resilience Act*) stabilisce **requisiti orizzontali di cibersicurezza** per i prodotti con elementi digitali, stabilendo:

- norme per la messa a disposizione sul mercato di prodotti con elementi digitali per garantire la cybersicurezza di tali prodotti;
- requisiti essenziali di cybersicurezza per la **progettazione, lo sviluppo e la produzione** di prodotti con elementi digitali e obblighi per gli operatori economici in relazione a tali prodotti per quanto riguarda la cybersicurezza;

- requisiti essenziali di cybersicurezza per i **processi di gestione delle vulnerabilità messi in atto dai fabbricanti** per garantire la cybersicurezza dei prodotti con elementi digitali durante il periodo in cui si prevede che i prodotti siano in uso e obblighi per gli operatori economici in relazione a tali processi;
- norme sulla **vigilanza del mercato**, compreso il monitoraggio, e sull'applicazione delle norme e dei requisiti anzidetti.

Il regolamento persegue le seguenti finalità:

- migliorare la sicurezza informatica in tutta l'Unione europea, stabilendo **requisiti obbligatori di sicurezza informatica** per i prodotti con elementi digitali;
- promuovere **pratiche sicure** incoraggiando i produttori a integrare la sicurezza informatica nelle fasi di progettazione e sviluppo dei prodotti;
- garantire **trasparenza e responsabilità** richiedendo ai produttori di fornire informazioni chiare sulle caratteristiche di sicurezza informatica dei loro prodotti e di assumersi la responsabilità di risolvere le vulnerabilità;
- promuovere un **mercato unico per la cibersicurezza** armonizzando le norme in tutti gli Stati membri per ridurre la frammentazione e garantire condizioni di parità.

Il regolamento si applica ai **prodotti *software* o *hardware***, comprese le relative soluzioni di elaborazione dati da remoto, la cui finalità prevista o il cui uso ragionevolmente prevedibile include una **connessione dati logica o fisica, diretta o indiretta, a un dispositivo o a una rete**. Sono esclusi dal campo di applicazione, tra gli altri, i prodotti disciplinati dai regolamenti (UE) 2017/745, 2017/746 e 2019/2144, quelli certificati ai sensi del regolamento (UE) 2018/1139, i pezzi di ricambio identici e i prodotti sviluppati esclusivamente per sicurezza nazionale o difesa.

Il regolamento prescrive degli **obblighi in capo ai fabbricanti**. In partcolare, essi devono integrare la cibersicurezza nella progettazione e nello sviluppo dei prodotti, prevedendo, tra l'altro, configurazioni sicure per impostazione predefinita, livelli adeguati di crittografia e meccanismi di controllo degli accessi. Sono tenuti, altresì, a condurre e mantenere aggiornata una valutazione del rischio e ad attuare misure volte ad affrontare le vulnerabilità individuate durante il ciclo di vita del prodotto; se si affidano a componenti o servizi di terzi, devono esercitare la dovuta diligenza al momento della loro integrazione. Devono, inoltre, fornire una documentazione chiara e completa, che comprenda la descrizione delle caratteristiche di cibersicurezza del prodotto, le istruzioni per un'installazione, una configurazione e un utilizzo sicuri, le informazioni su come segnalare le vulnerabilità e una dichiarazione di conformità al regolamento. Durante il periodo di supporto, che deve riflettere il periodo di utilizzo previsto del prodotto, forniscono aggiornamenti di sicurezza volti ad affrontare le vulnerabilità e a mantenere la sicurezza del prodotto.

Quanto alla segnalazione, i fabbricanti devono notificare senza indebito ritardo al CSIRT (*Computer Security Incident Response Team*), ossia il gruppo di intervento per la sicurezza informatica in caso di incidente, designato come coordinatore e all'ENISA (*European Union Agency for Cybersecurity*) gli incidenti gravi e le vulnerabilità attivamente sfruttate, e informare gli utenti sui

rischi potenziali, fornendo orientamenti sulla loro mitigazione. In circostanze eccezionali e per giustificati motivi connessi alla cibersicurezza, il CSIRT che riceve per primo la notifica può ritardare la condivisione delle notifiche relative a incidenti e vulnerabilità con gli altri CSIRT pertinenti tramite la piattaforma unica di segnalazione, per un periodo non più lungo di quanto strettamente necessario, alle condizioni specificate dal regolamento delegato (UE) 2026/881.

Il regolamento attribuisce **responsabilità anche a importatori e distributori**.

I primi devono verificare che i fabbricanti abbiano ottemperato al regolamento e assicurarsi che i prodotti siano correttamente etichettati e documentati; i secondi devono garantire, prima di metterli a disposizione sul mercato, che i prodotti rechino la marcatura CE e siano accompagnati dalle informazioni e dalle istruzioni per l'utente. La marcatura CE indica la conformità dei prodotti ai requisiti del regolamento. I fabbricanti di paesi terzi devono rispettare il regolamento per accedere al mercato dell'Unione, con possibili effetti sulle norme globali sulla cibersicurezza.

Il regolamento, già in vigore, si applica a partire dall'11 dicembre 2027, con l'eccezione delle disposizioni riguardanti gli obblighi di notifica delle vulnerabilità sfruttate attivamente e degli incidenti gravi – che trovano applicazione dall'11 settembre 2026 – e delle disposizioni in materia di notifica degli organismi di valutazione della conformità, le quali si applicano a decorrere dall'11 giugno 2026.

- ***Le recenti iniziative dell'Unione in materia di cibersicurezza***

Nel contesto degli sforzi volti al rafforzamento della resilienza digitale dell'Unione, la Commissione europea ha presentato un pacchetto di norme sulla **cibersicurezza** (sul quale, cfr. il *dossier* del Servizio RUE). Le proposte determinano un'**evoluzione** dell'**approccio europeo** che mira a trasformare progressivamente la cibersicurezza da ambito prevalentemente tecnico-regolatorio a **leva strategica** per la tutela delle infrastrutture critiche, la protezione delle catene di approvvigionamento e il rafforzamento dell'autonomia tecnologica dell'Unione. Il pacchetto comprende una proposta che riforma integralmente il c.d. ***Cybersecurity Act*** (regolamento (UE) 2019/881) e una proposta che modifica la c.d. **direttiva NIS 2** (direttiva (UE) 2022/2555). Su entrambe le proposte della Commissione europea, né il Consiglio né il Parlamento europeo hanno ancora adottato il rispettivo mandato negoziale in vista dell'avvio dei negoziati interistituzionali.

Presso la **Camera**, la **XIV Commissione** (Politiche dell'UE) ha esaminato le proposte ai fini della verifica di conformità al principio di sussidiarietà, adottando, il 6 maggio 2026, un documento recante una **valutazione conforme**.

Articolo 2
(Definizioni)

L'**articolo 2** reca le **definizioni** applicate ai fini dello schema di decreto in esame.

In particolare, il **comma 1**, prevede che trovino applicazione, con riferimento al presente provvedimento, le definizioni riportate nell'articolo 3 del regolamento (UE) 2024/2847, nell'articolo 3 del regolamento (UE) 2019/1020 e nell'articolo 4 del regolamento (UE) 2016/679.

Il **comma 2** precisa che trovano, altresì, applicazione le seguenti definizioni:

- **regolamento**: il regolamento (UE) 2024/2847, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali;
- **Agenzia**: l'Agenzia per la cybersicurezza nazionale di cui all'articolo 5 del decreto-legge n. 82 del 2021, individuata quale autorità di notifica e autorità di vigilanza del mercato ai sensi degli articoli 36 e 52, paragrafo 2, del regolamento;

L'articolo 36 stabilisce che ogni Stato membro deve designare un'autorità di notifica responsabile dell'istituzione e dell'esecuzione delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e il loro controllo. Inoltre, l'articolo 52, paragrafo 2, prevede che ciascuno Stato membro debba designare una o più autorità di vigilanza del mercato al fine di garantire l'efficace attuazione del regolamento (UE) 2024/2847. In particolare, gli Stati membri possono designare un'autorità già esistente o una nuova autorità che agisca come autorità di vigilanza del mercato ai fini del regolamento medesimo.

- **CSIRT Italia**: il Gruppo nazionale di risposta agli incidenti di sicurezza informatica, di cui all'articolo 7, comma 1, lettera d-*ter*), del decreto-legge n. 82 del 2021, operante presso l'Agenzia e che, ai fini del presente decreto, è designato come coordinatore;

Il Gruppo nazionale di risposta agli incidenti di sicurezza informatica (CSIRT Italia) è, ai sensi dell'articolo 15 del decreto legislativo n. 138 del 2024 (decreto legislativo NIS), l'organismo nazionale preposto alla gestione degli incidenti di sicurezza informatica per i settori e i soggetti essenziali e importanti individuati dagli allegati al medesimo decreto, nel quadro delineato dal decreto-legge n. 82 del 2021. Il CSIRT dispone di un'infrastruttura di comunicazione sicura e

resiliente per lo scambio di informazioni con i soggetti vigilati e con gli altri portatori di interesse, è dotato di un alto livello di disponibilità dei propri canali di comunicazione, garantisce la riservatezza e l'affidabilità delle proprie attività ed è dotato di sistemi ridondanti e spazi di lavoro di *backup* al fine di garantire la continuità dei propri servizi. Tra i suoi compiti vi rientrano, in particolare: il monitoraggio e l'analisi delle minacce informatiche, delle vulnerabilità e degli incidenti a livello nazionale; l'emissione di preallarmi, allerte e bollettini in merito a minacce informatiche, vulnerabilità e incidenti, se possibile in tempo prossimo al reale; la risposta agli incidenti e l'assistenza ai soggetti interessati; l'analisi dei dati forensi, dei rischi e degli incidenti; l'esecuzione, su richiesta dei soggetti o, per quelli accessibili al pubblico, di propria iniziativa e senza impatto sul loro funzionamento, di una scansione proattiva dei sistemi informativi e di rete del soggetto interessato per rilevare le vulnerabilità con potenziale impatto significativo; il coordinamento della divulgazione coordinata delle vulnerabilità. Il CSIRT partecipa inoltre alla Rete di CSIRT nazionali e alla revisione tra pari, può cooperare con omologhi organismi di Paesi terzi, anche scambiando dati personali nel rispetto della normativa vigente, e coopera con le strutture pubbliche con funzione di CERT e con i soggetti privati, promuovendo pratiche e tassonomie comuni.

- **organismo nazionale di accreditamento**: Accredia, quale organismo autorizzato a svolgere l'attività di accreditamento nel territorio dello Stato, ai sensi dell'articolo 2, punto 11), del regolamento (CE) n. 765/2008, designato con decreto del Ministro dello sviluppo economico del 22 dicembre 2009;
- **organismo notificato**: l'organismo di valutazione della conformità a seguito della procedura di notifica e delle attività di cui agli articoli 43 e 44 del regolamento (che disciplinano rispettivamente l'attività di notifica degli organismi di valutazione della conformità e l'assegnazione dei numeri di identificazione agli organismi notificati);
- **ENISA**: l'Agenzia dell'Unione europea per la cybersicurezza;
- **sistema di IA ad alto rischio**: sistema di IA classificato come ad alto rischio ai sensi dell'articolo 6 del regolamento (UE) 2024/1689;

Il sopra citato articolo 6 individua le condizioni affinché un sistema di IA sia considerato ad alto rischio, indipendentemente dalla sua immissione sul mercato o dalla sua messa in servizio. Nello specifico, è necessario che il sistema di IA sia destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA sia esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione europea elencata nell'allegato I e che il prodotto, il cui componente di sicurezza è il sistema di IA, o il sistema di IA stesso in quanto prodotto, sia soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I. Inoltre, la

disposizione precisa che sono considerati ad alto rischio anche i sistemi di IA di cui all'allegato III.

- **regolamento IA**: il regolamento (UE) 2024/1689 che stabilisce regole armonizzate sull'intelligenza artificiale;
- **decreto legislativo IA**: il decreto legislativo n. 179 del 2026 recante adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689;
- **autorità di vigilanza del mercato**: l'Agenzia per la cybersicurezza nazionale, la Banca d'Italia, la Commissione nazionale per la società e la borsa (CONSOB), l'Istituto per la vigilanza sulle assicurazioni (IVASS) e il Garante per la protezione dei dati personali, secondo quanto previsto dall'articolo 52, paragrafi 2 e 14, del regolamento e dall'articolo 9 dello schema di decreto in esame;
- **autorità del settore finanziario**: la Banca d'Italia, la CONSOB e l'IVASS;
- **Sandbox-CRA**: lo spazio di sperimentazione normativa per la ciberresilienza, istituito ai sensi dell'articolo 19 del presente schema di decreto, in attuazione dell'articolo 33, paragrafo 2, del regolamento;
- **sperimentazione *FinTech***: lo spazio di sperimentazione di cui all'articolo 36, commi da 2-*bis* a 2-*novies*, del decreto-legge n. 34 del 2019.

Si ricorda, in proposito, che i suddetti commi recano disposizioni volte a promuovere l'innovazione e la competizione del mercato dei capitali, attraverso la creazione di uno spazio tecnico-normativo sperimentale e temporaneo per le imprese del settore finanziario che operano attraverso la tecnologia (cd. *Fintech*), con una regolamentazione semplificata, assicurando un livello di protezione adeguato agli investitori. A tali fini, il comma 2-*bis* demanda al Ministro dell'economia e delle finanze (MEF), sentite la Banca d'Italia, la Commissione Nazionale per le Società e la Borsa (CONSOB) e l'istituto per la Vigilanza sulle Assicurazioni (IVASS), l'adozione, entro centottanta giorni dalla data di entrata in della legge di conversione del decreto-legge n. 34 del 2019 (30 giugno 2019), di uno o più regolamenti per definire le condizioni e le modalità di svolgimento di una sperimentazione (cd. *regulatory sandbox*) per le attività che perseguono l'innovazione di servizi e prodotti finanziari, creditizi e assicurativi mediante l'utilizzo nuove tecnologie. Si segnala che, in attuazione di tale disposizione, è stato adottato il decreto ministeriale n. 100 del 2021, recante il regolamento sulla disciplina del Comitato e della sperimentazione *FinTech*.

Articolo 3
(Atti di indirizzo)

L'**articolo 3** prevede che, nei limiti e per le finalità di cui al regolamento (UE) 2024/2847, le **autorità di vigilanza del mercato** possano adottare **atti di indirizzo** in forma di linee guida, raccomandazioni e buone pratiche, negli ambiti di rispettiva competenza.

Ai sensi dell'articolo 2, comma 2, lett. *i)* del provvedimento in esame, le **autorità di vigilanza del mercato** sono:

- l'Agenzia per la cybersicurezza nazionale (ACN);
- la Banca d'Italia;
- la Commissione nazionale per la società e la borsa (CONSOB);
- l'Istituto per la vigilanza sulle assicurazioni (IVASS);
- il Garante per la protezione dei dati personali.

Secondo quanto stabilito dall'articolo in esame, le autorità di vigilanza del mercato hanno la possibilità, ognuno secondo le proprie **competenze**, di adottare i seguenti atti di indirizzo:

- **linee guida;**
- **raccomandazioni;**
- **buone pratiche**.

All'articolo 9 del presente provvedimento (cui si rinvia) sono indicati gli **ambiti di competenza** delle autorità di vigilanza del mercato: l'ACN ha competenza sui requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali; le altre autorità sono competenti limitatamente ai prodotti con elementi digitali che rientrano nell'ambito di applicazione del regolamento e che sono classificati come sistemi di IA ad alto rischio.

All'articolo in esame corrisponde quanto previsto dall'articolo 52, paragrafo 10 del regolamento (UE) 2024/2847 (*Cyber Resilience Act*), secondo cui le autorità di vigilanza del mercato possono fornire agli operatori economici **orientamenti e consulenza** sull'attuazione del presente regolamento, con il sostegno della Commissione e, se del caso, dei CSIRT (*Computer Security Incident Response Team*) e dell'ENISA (*European Union Agency for Cibersecurity*).

Nel nostro Paese il CSIRT Italia opera presso l'Agenzia per la Cybersicurezza Nazionale (ACN) ed è stato istituito dal Decreto Legge n. 82/2021. È l'organismo competente nella prevenzione, gestione e risposta agli incidenti informatici, e

fornisce supporto a soggetti pubblici e privati con l'obiettivo di rafforzare la resilienza complessiva del Paese di fronte alle minacce cibernetiche.

Si ricorda che ai sensi dell'articolo 26 del citato regolamento (UE) 2024/2847, anche la Commissione europea adotta atti di indirizzo sotto forma di orientamenti per assistere gli operatori economici nell'applicazione del medesimo regolamento, con particolare attenzione all'agevolazione della conformità da parte delle microimprese e delle piccole e medie imprese.

Gli orientamenti riguardano almeno gli aspetti seguenti:

- l'ambito di applicazione del regolamento, con particolare attenzione alle soluzioni di elaborazione dati da remoto e ai *software* liberi e *open-source*;
- l'applicazione di periodi di assistenza in relazione a particolari categorie di prodotti con elementi digitali;
- orientamenti destinati ai fabbricanti soggetti al presente regolamento che sono anche soggetti ad altre normative di armonizzazione dell'Unione diverse dal presente regolamento o ad altri atti giuridici dell'Unione correlati;
- il concetto di modifica sostanziale.

Inoltre, la Commissione mantiene un elenco facilmente fruibile degli atti delegati e di esecuzione adottati a norma del regolamento e, nell'elaborare gli orientamenti consulta i portatori di interessi pertinenti.

In attuazione di tale disposizione la Commissione ha adottato le linee guida per l'applicazione del *Cyber Resilience Act* a supporto dei destinatari del provvedimento: produttori, sviluppatori e imprese (Comunicazione C (2026) 5252, del 27 luglio 2026).

Articolo 4
(Autorità di notifica)

L'**articolo 4** individua l'Autorità di notifica e ne definisce i rapporti con l'organismo nazionale di accreditamento

Il **Capo II** dello schema di decreto legislativo in esame (articoli 4-8) disciplina la **Notifica degli organismi di valutazione della conformità**, definendo il quadro istituzionale, procedurale e finanziario per la designazione, la notifica e il controllo degli enti incaricati di verificare il rispetto dei requisiti di cibersicurezza stabiliti dal Regolamento (UE) 2024/2847 (d'ora in avanti, *Cyber Resilience Act* o *CRA*).

L'articolo 4, **comma 1**, individua l'**Agenzia per la cibersicurezza nazionale** (d'ora in avanti, **ACN**) quale **Autorità di notifica**, in ottemperanza di quanto previsto dall'articolo 36 del *Cyber Resilience Act*. Secondo la norma richiamata, difatti, ciascuno Stato membro è tenuto a istituire un'autorità di notifica responsabile dell'istituzione ed esecuzione delle procedure necessarie per valutare, designare e notificare gli organismi di conformità[1].

Ferma restando la responsabilità dell'ACN, il **comma 2** della norma in esame attribuisce i concreti compiti di valutazione e controllo all'**organismo nazionale di accreditamento,** come espressamente consentito dall'articolo 36, paragrafo 2, del *Cyber Resilience Act*. L'organismo nazionale di accreditamento è tenuto ad operare in conformità alle norme di cui al regolamento (CE) n. 765/2008[2].

In Italia, l'organismo autorizzato – ai sensi degli artt. 2, par. 1 n. 11, e 4 reg. (CE) n. 765/2008 – a svolgere l'attività di accreditamento nel territorio nazionale è **Accredia** (Ente italiano di accreditamento), come da designazione effettuata con decreto del Ministro dello sviluppo economico del 22 dicembre 2009, in attuazione dell'art. 4, co. 2, l. 23 luglio 2009 n. 99. Accredia ha natura di associazione privata senza scopo di lucro, avente sede legale a Roma, e opera sotto la vigilanza del Ministero delle imprese e del *made in Italy*.

1 Cfr. anche la definizione di cui all'articolo 3, paragrafo 1 n. 26, CRA.
2 Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e abroga il regolamento (CEE) n. 339/93.

Il **comma 3** stabilisce che i rapporti tra l'ACN e l'organismo nazionale di accreditamento, ai fini dello svolgimento dei compiti di controllo e vigilanza, devono essere regolati da **apposita convenzione**.

Articolo 5
(Domanda e procedura di designazione e notifica degli organismi di valutazione di conformità)

L'**articolo 5** disciplina la procedura relativa alla domanda di notifica che gli organismi devono presentare all'ACN al fine di essere abilitati a valutare la conformità dei prodotti digitali, dettando inoltre disposizioni relative alla copertura dei costi del servizio.

Ai sensi dell'articolo 5, **comma 1**, gli organismi che desiderano valutare la conformità alla normativa nazionale ed europea dei prodotti digitali presentano **domanda di notifica all'ACN**, allegando la certificazione richiesta dall'articolo 42, paragrafo 2, del *Cyber Resilience Act*. La norma europea richiamata richiede, in particolare, una descrizione delle attività di valutazione della conformità, della procedura o delle procedure di valutazione della conformità e del prodotto o dei prodotti con elementi digitali per i quali l'organismo dichiara di essere competente. Tra i documenti richiesti, tanto il comma 1 dell'articolo 5 in esame quanto la norma europea richiamata ricomprendono il **certificato di accreditamento**, che l'organismo nazionale di accreditamento deve rilasciare, al fine di attestare la conformità dell'organismo di valutazione ai requisiti dettagliatamente elencati nell'articolo 39 del *CRA*[3].

Ai sensi del **comma 2**, le concrete modalità procedurali per la designazione e la notifica degli organismi di valutazione della conformità sono definite con provvedimento del direttore generale dell'ACN, e sono pubblicate nel sito *internet* istituzionale di tale Agenzia.

Il **comma 3** impone agli stessi organismi richiedenti il pagamento di una **tariffa**, destinata a coprire i costi relativi alle attività istruttorie di designazione e notifica. Si garantisce, in tal modo, che il sistema possa operare in maniera autosufficiente. In particolare, le tariffe sono determinate – e periodicamente aggiornate, **sulla base del costo effettivo dei servizi** in questione – con decreto del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, su proposta del Direttore generale dell'ACN (articolo 13, comma 1, d.lgs. 3 agosto 2022, n. 123, qui richiamato). Secondo quanto precisato dal **comma 4**, i proventi delle tariffe confluiscono nel bilancio dello Stato ma vengono

3 Volti a garantire, in sostanza, l'indipendenza, l'imparzialità e la professionalità tecnica dell'organismo che presenta domanda di notifica.

destinati, nel medesimo esercizio finanziario, in apposito capitolo al fine di **incrementare la dotazione del bilancio dell'ACN**.

Articolo 6
(Modifiche delle notifiche)

L'**articolo 6** disciplina i casi di limitazione, sospensione o ritiro della notifica.

L'articolo 6, **comma 1**, impone all'organismo nazionale di accreditamento di comunicare all'ACN la **limitazione, sospensione o revoca del certificato di accreditamento**[4]. Tale comunicazione è effettuata, secondo la norma in esame, ai fini dell'attuazione dell'articolo 45 del *Cyber Resilience Act*: vale a dire, allo scopo di consentire all'ACN di disporre la **limitazione, la sospensione o il ritiro della notifica**, "qualora accerti o sia informata che un organismo notificato non è più conforme ai requisiti" previsti dall'art. 39 del citato regolamento europeo, "o non adempie ai suoi obblighi"[5].

Ai sensi del **comma 2**, nel caso di limitazione, sospensione o ritiro della notifica, così come – per altro verso – nell'ipotesi di cessazione dell'attività, l'organismo ha il **divieto assoluto di rilasciare nuovi certificati di conformità** sui prodotti.

Il **comma 3** affida a un decreto del direttore generale dell'ACN il compito di definire le procedure per la limitazione, la sospensione o il ritiro della notifica, nonché per l'adozione delle misure di cui all'articolo 45, paragrafo 2, del *Cyber Resilience Act*.

Si tratta, in particolare, delle "**misure appropriate**" volte a garantire che le pratiche di un organismo, nei confronti del quale sia stata disposta la limitazione, la sospensione o il ritiro della notifica, "siano evase da un altro organismo notificato o siano messe a disposizione delle autorità di notifica e di vigilanza del mercato responsabili, su loro richiesta". Analogamente si dispone qualora l'organismo notificato abbia cessato la propria attività. In tal modo si garantisce,

4 Sul presupposto, evidentemente, in cui accerti che l'organismo di valutazione non presenti – o non presenti più – i requisiti che legittimavano il rilascio del certificato: v. sopra, sub articolo 5.

5 La scelta dell'ACN di limitare, sospendere o ritirare la notifica viene effettuata caso per caso, "in funzione della gravità del mancato rispetto [dei] requisiti o dell'inadempimento [degli] obblighi". L'ACN è tenuta a comunicare tali provvedimenti alla Commissione europea e agli altri Stati membri (art. 45, par. 1, CRA).

da un lato, che l'attività di valutazione[6] non venga interrotta, giacché le pratiche dell'attività in corso passano ad altro organismo notificato, idoneo a evaderle; dall'altro, che la documentazione relativa a tale attività venga conservata e sia utilizzabile dalle autorità di notifica e di vigilanza del mercato, al fine di svolgere i rispettivi controlli.

6 Si ricorda che, come disposto dal comma 2 poco sopra esaminato, in capo all'organismo oggetto del provvedimento di limitazione, sospensione o ritiro vige un divieto assoluto di proseguire tale attività.

Articolo 7
(Ricorso contro le decisioni degli organismi notificati)

L'**articolo 7** prevede la necessità di istituire una procedura di ricorso contro le valutazioni di conformità operate dagli organismi notificati.

L'articolo 7, **comma 1**, impone a ciascun organismo notificato di predisporre, laddove non già disponibile, una procedura di ricorso trasparente e accessibile, in modo da garantire il diritto di difesa delle imprese avverso le decisioni dell'organismo. La norma in esame costituisce attuazione dell'articolo 48 del *Cyber Resilience Act* – qui espressamente richiamato – ai sensi del quale gli Stati membri sono tenuti a garantire una procedura di ricorso contro le decisioni degli organismi notificati.

Articolo 8
(Raccordo informativo con l'autorità di notifica ai sensi del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024)

L'articolo 8 disciplina lo scambio informativo tra l'Autorità di notifica per l'intelligenza artificiale e quella per la cibersicurezza per i prodotti digitali che sono anche classificati come sistemi di IA ad alto rischio.

L'**articolo 8** disciplina lo scambio informativo tra l'Autorità di notifica per l'intelligenza artificiale (vale a dire, l'Agenzia per l'Italia Digitale – AgID) e quella per la cibersicurezza (l'ACN) per i prodotti digitali che sono anche classificati come sistemi di IA ad alto rischio.

L'articolo 8, **comma 1**, richiama espressamente gli articoli 12, paragrafi 2 e 3, del *Cyber Resilience Act*, dei quali pare opportuno rammentare brevemente il contenuto.

L'articolo 12, paragrafo 2, disciplina l'ipotesi in cui **i prodotti digitali integrano modelli di intelligenza artificiale ad alto rischio**, soggetti alla procedura di valutazione della conformità di cui all'articolo 43 del regolamento (UE) 2024/1689 (*AI Act*)[7]. In tal caso, in un'ottica di semplificazione, il citato articolo 12, paragrafo 2, affida agli stessi organismi notificati, ai quali è attribuito il controllo dei sistemi di IA ad alto rischio, la valutazione relativa alla conformità di tali sistemi ai requisiti in tema di cibersicurezza.

Si ricorda che, in materia di intelligenza artificiale, la notificazione degli organismi di valutazione della conformità, sulla base della procedura delineata dagli artt. 28 ss. regolamento IA, è svolta dall'**Agenzia per l'Italia digitale** (AgID), individuata come Autorità nazionale di notifica dall'art. 20, co. 1, lett. *a)*, l. 23 settembre 2025, n. 132 (che attua, *in parte qua*, l'articolo 70 regolamento

7 Si ricorda che la disciplina dettata dall'AI Act si incentra sul livello di rischio associato alle applicazioni di IA, distinguendo, in particolare, tra:
a) sistemi che presentano rischi inaccettabili, per i quali vige un divieto assoluto di immissione nel mercato europeo (art. 5);
b) sistemi ad alto rischio (come definiti, in particolare, dall'art. 6);
c) sistemi a rischio limitato.
I sistemi ad alto rischio, pur di per sé non vietati, comportano una serie di obblighi in capo ai fornitori e agli utilizzatori professionali (cfr. artt. 6-49, 50) assai più stringenti rispetto a quelli derivanti dall'uso dei sistemi a rischio limitato e relativi, ad es., alla necessità di effettuare una preventiva valutazione d'impatto sui diritti fondamentali ovvero di istituire un sistema di gestione dei rischi. Ai sistemi ad alto rischio si applica l'articolata procedura di valutazione della conformità di cui all'art. 43.

IA). Qualora però agli organismi notificati sia richiesto, a norma dell'art. 12, par. 2, *CRA*, di verificare ulteriormente la conformità ai requisiti in tema di cibersicurezza, la norma da ultimo richiamata richiede che si accerti, in occasione della procedura di notifica, la conformità di quegli stessi organismi notificati ai requisiti di cui all'articolo 39 *CRA.*

Una deroga è prevista, tuttavia, nei casi indicati dall'articolo 12, paragrafo 3, riguardanti prodotti digitali che, oltre ad essere classificati come sistemi di IA ad alto rischio, presentano profili particolarmente critici per la cibersicurezza: in tal caso, la valutazione di conformità rispetto ai requisiti essenziali di cibersicurezza continua a svolgersi secondo le procedure previste dal *Cyber Resilience Act*.

Là dove, in base alle norme europee richiamate, gli organismi notificati autorizzati a monitorare i sistemi di IA ad alto rischio siano tenuti, altresì, a verificare la complessiva cibersicurezza del prodotto digitale, l'articolo 8, comma 1, dello schema in esame richiede un **raccordo informativo** tra l'Autorità nazionale di notifica per l'intelligenza artificiale – vale a dire, come ricordato, l'**Agenzia per l'Italia digitale** – e quella per la cibersicurezza. In particolare, l'AgID è tenuta a **informare l'ACN circa gli organismi notificati** a norma degli artt. 28 ss. regolamento IA.

Articolo 9
(Autorità di vigilanza del mercato)

L'**articolo 9** individua le autorità di vigilanza del mercato chiamate ad assicurare l'applicazione del regolamento europeo sulla ciberresilienza. In via generale e relativamente ai requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali, la funzione spetta all'Agenzia per la cybersicurezza nazionale (comma 1). Per i prodotti che sono anche sistemi di intelligenza artificiale (IA) ad alto rischio, la vigilanza spetta alle autorità competenti ai sensi della disciplina sull'IA, ciascuna nel proprio ambito (comma 2).

L'**articolo 9, comma 1**, individua l'**Agenzia per la cybersicurezza nazionale** (ACN), istituita dal decreto-legge n. 82/2021, quale autorità di vigilanza del mercato, relativamente ai **requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali**, ai sensi dell'articolo 52, paragrafo 2, del regolamento (UE) 2024/2847 (cd. regolamento sulla ciberresilienza), e fermo restando quanto previsto al successivo comma 2.

Il regolamento (UE) 2024/2847 (cosiddetto *Cyber Resilience Act*, CRA) stabilisce requisiti di cibersicurezza, cioè di protezione da attacchi informatici, accessi abusivi e malfunzionamenti, per i prodotti con elementi digitali. Si tratta dei programmi informatici (*software*) e delle apparecchiature (*hardware*) che, in base alla loro destinazione o all'uso ragionevolmente prevedibile, si collegano direttamente o indirettamente a un dispositivo o a una rete (art. 2, par. 1). Il regolamento impone obblighi a fabbricanti, importatori e distributori per l'intero ciclo di vita del prodotto.

Il regolamento si applica dall'11 dicembre 2027. Gli obblighi di segnalazione delle vulnerabilità e degli incidenti (art. 14) si applicano però dall'11 settembre 2026 e le disposizioni sulla notifica degli organismi di valutazione della conformità (capo IV) dall'11 giugno 2026 (art. 71). Ai prodotti con elementi digitali si applica il regolamento (UE) 2019/1020 sulla vigilanza del mercato (art. 52, par. 1), cui l'ordinamento nazionale si è adeguato con il decreto legislativo n. 157/2022.

L'articolo 52, comma 2, del regolamento (UE) 2024/2847 prevede che ciascuno Stato membro designi una o più autorità di vigilanza del mercato (già esistenti o di nuova istituzione) al fine di garantire l'efficace attuazione del regolamento medesimo.

La delega per l'adeguamento della normativa nazionale è recata dall'articolo 15, comma 2, lettera *c)*, della legge n. 35/2026 (legge di delegazione europea 2025).

Il **comma 2** si riferisce espressamente ai **prodotti con elementi digitali** che rientrano nell'ambito di applicazione del regolamento sulla ciberresilienza e che, al contempo, sono classificati come **sistemi di IA ad alto rischio**, ai sensi dell'articolo 6 del regolamento (UE) 2024/1689 (cd. *AI Act*).

L'articolo 6 del regolamento (UE) 2024/1689 individua come **sistemi di IA ad alto rischio**: i sistemi che sono componenti di sicurezza di prodotti (o prodotti essi stessi) disciplinati dalla normativa di armonizzazione di cui all'allegato I e soggetti a valutazione di conformità da parte di terzi ai fini dell'immissione sul mercato o della sua messa in servizio; e i sistemi impiegati negli ambiti elencati nell'allegato III del regolamento. Per questi ultimi è prevista una deroga qualora il sistema non presenti un rischio significativo per salute, sicurezza o diritti fondamentali; la deroga non opera mai se il sistema effettua profilazione di persone fisiche. Il fornitore che se ne avvale è tenuto a documentare la valutazione e a registrarsi nella banca dati dell'UE.

Per i predetti prodotti, l'articolo 52, paragrafo 14, del regolamento sulla ciberresilienza, prevede che le autorità responsabili delle attività di vigilanza del mercato, siano le medesime autorità di vigilanza del mercato designate ai fini dell'*AI Act*.

Dunque, il comma in esame prevede che, limitatamente ai prodotti con elementi digitali che rientrano nell'ambito di applicazione del regolamento sulla ciberresilienza e che sono classificati come sistemi di IA ad alto rischio, le autorità responsabili delle attività di vigilanza del mercato siano le autorità indicate all'articolo 5, comma 1, lettere *a)*, *b)* e *c)*, del decreto legislativo n. 179/2026, per gli ambiti ivi previsti e per le attività di cui agli allegati VIII-*bis*, VIII-*ter* e VIII-*quater* al decreto legislativo n. 157/2022 (introdotti dall'articolo 21, comma 1, lettera *c)*, del decreto in commento, alla cui scheda di lettura si rinvia).

Si tratta delle seguenti autorità: l'**Agenzia per la cybersicurezza nazionale** (ACN), la **Banca d'Italia**, la **CONSOB**, l'**IVASS** e il **Garante per la protezione dei dati personali**.

I citati nuovi allegati recano rispettivamente:

- disposizioni relative ai procedimenti di competenza dell'Agenzia per la cybersicurezza nazionale;
- disposizioni relative ai procedimenti di competenza della Banca d'Italia, della Commissione nazionale per la società e la borsa (CONSOB), dell'Istituto per la vigilanza sulle assicurazioni (IVASS);
- disposizioni relative ai procedimenti di competenza del Garante per la protezione dei dati personali.

Più nel dettaglio, si ricorda che il decreto legislativo n. 179/2026 reca l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 (*AI Act*) in materia di poteri delle Autorità nazionali e di utilizzo dell'intelligenza artificiale nella formazione.

L'articolo 5, comma 1, lettere *a)*, *b)* e *c)*, del decreto, ha designato come segue le autorità di vigilanza del mercato ai sensi dell'*AI Act*.

- La lett. *a)* ha designato l'**Agenzia per la cybersicurezza nazionale (ACN)** quale **autorità di vigilanza di mercato sui sistemi di IA**, ai sensi dell'articolo 70 dell'*AI Act*. I sistemi di IA sono sistemi automatizzati progettati per funzionare con livelli di autonomia variabili e che possono presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deducono dall'*input* che riceve come generare *output* quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali (art. 3, n. 1, dell'*AI Act*). Il paragrafo 4 del citato articolo 70, dispone che le autorità nazionali competenti adottano misure per garantire un **livello adeguato di cibersicurezza**.
- La lett. *b)* ha designato le Autorità di vigilanza nel **settore finanziario,** in particolare:
  - la **Banca d'Italia**, quale autorità competente sui sistemi di IA ad alto rischio utilizzati nell'erogazione di finanziamenti o di altri servizi finanziari disciplinati ai sensi del decreto legislativo n. 385 del 1993 (TUB);
  - la **CONSOB**, quale autorità competente **sui sistemi di IA ad alto rischio** utilizzati nell'**erogazione dei servizi finanziari** disciplinati ai sensi del decreto legislativo n. 58 del 1998 (TUF);
  - l'**IVASS**, quale autorità competente **sui sistemi di IA ad alto rischio** utilizzati nell'esercizio dell'**attività assicurativa o riassicurativa e di distribuzione di prodotti assicurativi** disciplinati ai sensi del decreto legislativo n. 209 del 2005.
- La lett. *c)* ha designato il **Garante per la protezione dei dati personali** quale **autorità nazionale di vigilanza del mercato** per quanto concerne l'applicazione di **sistemi di IA ad alto rischio** regolati dall'articolo 74, paragrafo 8, dell'*AI Act*. Si tratta, in primo luogo dei **sistemi di IA** ad **alto rischio** impiegati nel **settore della biometria** (v. Allegato III, punto 1 dell'*AI Act*), quando tali sistemi sono utilizzati **per attività di contrasto, gestione delle frontiere, giustizia e democrazia**. Inoltre, il medesimo paragrafo 8 dell'articolo 74 del regolamento contempla i sistemi di IA ad alto rischio nei settori della **repressione e prevenzione criminale** da parte delle **forze dell'ordine** (v. Allegato III, punto 6), della **migrazione**, dell'**asilo** e della **gestione del controllo delle frontiere** (v. Allegato III, punto 7), dell'**amministrazione della giustizia** e dei **processi democratici** (v. Allegato III, punto 8).

Per quanto riguarda i nuovi allegati VIII-*bis*, VIII-*ter* e VIII-*quater* al decreto legislativo n. 157/2022, si ricorda che il decreto, adottato in attuazione della delega di cui all'articolo 30 della legge n. 118/2022, ha adeguato la normativa nazionale a quanto disposto dal regolamento (UE) 2019/1020 del Parlamento

europeo e del Consiglio, del 20 giugno 2019, sulla **vigilanza del mercato e sulla conformità dei prodotti**, soggetti alla normativa di armonizzazione dell'Unione europea di cui all'allegato I del medesimo regolamento, provvedendo contestualmente alla semplificazione e al riordino del relativo sistema di vigilanza. Quanto all'assetto istituzionale, **l'articolo 3 individua le autorità di vigilanza del mercato** – ai sensi dell'articolo 10 del regolamento e nel rispetto dei princìpi di competenza, adeguatezza, sussidiarietà, differenziazione e unitarietà dei processi decisionali – in **otto amministrazioni**: il Ministero dello sviluppo economico (ora Ministero delle imprese e del *made in Italy*), il Ministero della salute, il Ministero del lavoro e delle politiche sociali, il Ministero dell'interno, il Ministero della transizione ecologica (ora Ministero dell'ambiente e della sicurezza energetica), il Ministero delle infrastrutture e della mobilità sostenibili (ora Ministero delle infrastrutture e dei trasporti), il Ministero delle politiche agricole alimentari e forestali (ora Ministero dell'agricoltura, della sovranità alimentare e delle foreste) e l'ENAC. Gli **ambiti di competenza** di tali autorità sono disciplinati dagli **allegati I-VIII** al decreto legislativo.

Per quanto concerne i **profili finanziari delle disposizioni di cui al presente articolo e di cui all'articolo 10**, la relazione tecnica evidenzia che le funzioni di vigilanza determinano maggiori oneri per l'ACN, che dovrà impiegare adeguate risorse professionali e supporti tecnologici, anche in coerenza con l'articolo 52, paragrafo 8, del regolamento (UE) 2024/2847. Sul punto, l'articolo 26 dello schema di decreto in esame (alla cui scheda di lettura si rinvia) reca le disposizioni finanziare per l'attuazione degli articoli 9, comma 1 e 10, comma 1.

- ***L'*Omnibus *digitale sull'intelligenza artificiale (IA)***

Il c.d. ***Omnibus* digitale sull'IA** (regolamento (UE) 2026/1744) ha recentemente modificato il c.d. ***AI Act*** (regolamento (UE) 2024/1689) al fine di **posticipare** l'**applicazione** delle norme sui sistemi di intelligenza artificiale considerati ad **alto rischio**:

- dal 2 agosto 2026 al **2 dicembre 2027**, per i sistemi **autonomi** in **settori sensibili**, ad esempio biometria, infrastrutture critiche, istruzione, occupazione, migrazione, asilo e controllo delle frontiere;
- dal 2 agosto 2027 al **2 agosto 2028**, per i sistemi di intelligenza artificiale **integrati in prodotti**.

Articolo 10
(Poteri e misure di vigilanza del mercato dell'Agenzia)

L'**articolo 10** disciplina l'attribuzione dei **poteri dell'Agenzia per la cybersicurezza nazionale** (ACN), in quanto autorità di vigilanza del mercato ai fini dell'attuazione del regolamento sulla ciberresilienza.

L'articolo 10 precisa quali sono i **poteri dell'Agenzia per la cybersicurezza nazionale** (ACN), designata dall'articolo 9, comma 1, del presente schema di decreto, quale autorità di vigilanza del mercato ai fini dell'attuazione del regolamento sulla ciberresilienza.

Il **comma 1** attribuisce all'Agenzia i **poteri** e le **misure di vigilanza** previsti: dal capo V del regolamento (UE) 2024/2847 (regolamento sulla ciberresilienza), dal capo V del regolamento (UE) 2019/1020 (regolamento sulla vigilanza del mercato e sulla conformità dei prodotti), nonché dal decreto legislativo n. 157/2022 (semplificazione e riordino del sistema di vigilanza del mercato).

Per quanto riguarda i **poteri** attribuiti all'agenzia, si riporta quanto segue.

Il capo V del regolamento (UE) 2024/2847 (articoli 52-60)

- L'**articolo 52** stabilisce, in via generale, l'applicabilità ai prodotti con elementi digitali del regolamento (UE) 2019/1020 (par. 1) e l'obbligo per ciascuno Stato membro di designare una o più autorità di vigilanza del mercato (par. 2). Tali autorità vigilano anche sugli obblighi dei gestori di software *open source* di cui all'articolo 24 (par. 3); collaborano con le autorità nazionali di certificazione della cibersicurezza, con i CSIRT (*Computer Security Incident Response Team*) designati come coordinatori e con l'ENISA (*European Union Agency for Cybersecurity*) (parr. 4-5), con le altre autorità di vigilanza del mercato (par. 6) e con le autorità di protezione dei dati (par. 7). Gli Stati membri assicurano loro adeguate risorse finanziarie, tecniche e umane (par. 8). Le autorità possono fornire orientamenti agli operatori economici (par. 10), informano i consumatori sulle modalità di reclamo e di segnalazione (par. 11), riferiscono annualmente alla Commissione in merito ai risultati delle pertinenti attività di vigilanza del mercato (par. 13) e monitorano i periodi di assistenza dei prodotti determinati dai fabbricanti (par. 16). Il paragrafo 15 istituisce un gruppo di cooperazione amministrativa (ADCO) dedicato.
- L'**articolo 53** consente alle autorità, su richiesta motivata, l'**accesso ai dati** necessari per valutare progettazione, sviluppo, produzione e gestione delle vulnerabilità dei prodotti, inclusa la documentazione interna dell'operatore economico.
- L'**articolo 54** disciplina la procedura nazionale per i **prodotti che presentano un rischio di cibersicurezza significativo**: valutazione, anche in cooperazione

con il CSIRT; richiesta di misure correttive, ritiro o richiamo; in mancanza, misure provvisorie di divieto o limitazione, notificate alla Commissione e agli Stati membri. Il paragrafo 2 precisa che le autorità di vigilanza del mercato tengono conto anche dei fattori di rischio non tecnici.

- Gli **articoli 55 e 56** disciplinano, rispettivamente, la **procedura di salvaguardia dell'Unione** e la **procedura a livello di Unione** per i prodotti che presentano un rischio di cibersicurezza significativo.
- L'**articolo 57** riguarda i **prodotti conformi** che presentano comunque un **rischio significativo**, ad esempio per la salute, i diritti fondamentali o i servizi dei soggetti essenziali di cui alla direttiva (UE) 2022/2555 (NIS 2).
- L'**articolo 58** concerne la **non conformità formale dei prodotti** (marcatura CE, dichiarazione di conformità UE, documentazione tecnica).
- L'**articolo 59** consente alle autorità di vigilanza del mercato di stipulare **accordi con altre autorità** competenti per la realizzazione di attività congiunte nell'ottica di garantire la cibersicurezza e la tutela dei consumatori in relazione a specifici prodotti.
- L'**articolo 60** prevede **indagini a tappeto** per particolari prodotti, coordinate di norma dalla Commissione, che possono comprendere ispezioni di prodotti acquistati sotto un'identità di copertura.

Il capo V del regolamento (UE) 2019/1020 (articoli 14-21)

- L'**articolo 14** dispone che gli Stati membri conferiscono alle autorità di vigilanza del mercato i **poteri necessari**, da esercitare secondo il principio di proporzionalità (parr. 1-2). I poteri possono essere esercitati direttamente, mediante il ricorso ad altre autorità pubbliche o previa autorizzazione giurisdizionale (par. 3). Il paragrafo 4 elenca una serie di poteri conferiti alle autorità fra cui: **richiesta di documenti**, **specifiche** tecniche, **dati** e informazioni, compreso l'accesso al *software* incorporato (lett. *a)*); richiesta di **informazioni sulla catena di approvvigionamento** e sulla **proprietà dei siti *web*** (lett. *b)* e *c)*); effettuare **ispezioni** in loco e **controlli** fisici, accesso a locali, terreni e mezzi di trasporto (lett. *d)* ed *e)*); avvio di **indagini** di propria iniziativa (lett. *f)*); imposizione di **misure appropriate e correttive** (lett. *g)* e *h)*); imposizione di **sanzioni** (lett. *i)*); **acquisizione di campioni**, anche in forma anonima, e sottoporli a ingegneria inversa (lett. *j)*); in assenza di altri mezzi efficaci, la **rimozione di contenuti** da interfacce *online* o limitazione dell'accesso ad essa (lett. *k)*).
- Gli **articoli da 15 a 21** disciplinano: il **recupero dei costi** dagli operatori in caso di non conformità al regolamento (art. 15); le **misure appropriate** per garantire la vigilanza del mercato, nonché quelle **correttive** (come il ripristino della conformità del prodotto, il divieto alla messa a disposizione, il ritiro o la distruzione dello stesso) (art. 16); gli obblighi di **trasparenza** e **riservatezza** delle autorità (art. 17); i **diritti procedurali** degli operatori economici (art. 18); le misure in caso di prodotti che presentano un **rischio grave** (art. 19); il sistema di **informazione rapida** (art. 20); gli **impianti di prova** dell'Unione (art. 21).

Il decreto legislativo n. 157 del 2022

Il decreto legislativo n. 157/2022, adottato in attuazione della delega di cui all'articolo 30 della legge n. 118/2022, ha adeguato la normativa nazionale a quanto disposto dal regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio, del 20 giugno 2019, sulla **vigilanza del mercato e sulla conformità dei prodotti**, soggetti alla normativa di armonizzazione dell'Unione europea di cui all'allegato I del medesimo regolamento, provvedendo contestualmente alla semplificazione e al riordino del relativo sistema di vigilanza.

Il decreto, all'articolo 3, individua le **autorità di vigilanza del mercato per i diversi settori** della normativa di armonizzazione (per il cui elenco si rimanda alla scheda di lettura dell'articolo 9). Tali autorità svolgono le relative funzioni con i **poteri di cui al capo V del regolamento (UE) 2019/1020** e svolgono i **controlli** previsti dalla normativa armonizzata dell'Unione europea nell'ambito delle rispettive competenze, anche mediante i propri uffici territoriali, le autorità incaricate del controllo di cui al successivo articolo 4 e gli altri enti ai quali è demandato lo svolgimento delle attività di vigilanza. Restano ferme le attribuzioni delle autorità di pubblica sicurezza, quali autorità di controllo del mercato in materia di esplosivi per uso civile e articoli pirotecnici. Le autorità di vigilanza del mercato **cooperano** al fine dello svolgimento delle attività di rispettiva competenza, anche mediante lo **scambio di informazioni, elementi o dati** in proprio possesso, e rendono disponibili sui propri siti *internet* le informazioni sui prodotti, sulle procedure e sulle normative applicabili.

L'articolo 21 dello schema di decreto in esame (alla cui scheda di lettura si rinvia) inserisce l'ACN tra le autorità di vigilanza del mercato del d.lgs. n. 157/2022.

Come già rilevato per la scheda relativa all'articolo 9 dello schema in esame, si ricorda che la relazione tecnica evidenzia che le funzioni di vigilanza determinano **maggiori oneri per l'ACN**: si rimanda, sul punto, a quanto previsto dall'articolo 26 dello schema di decreto.

Il **comma 2** precisa che, nell'esercizio dei propri poteri, l'Agenzia può avvalersi della **collaborazione del Corpo della Guardia di finanza**, ai sensi degli articoli 2, comma 2, lettera *m)*, e 3, comma 1, del decreto legislativo n. 68/2001. Restano comunque fermi gli obblighi e i meccanismi di cooperazione previsti dal regolamento e dal decreto legislativo n. 157/2022.

Per quanto riguarda il d.lgs. n. 68/2001:

- l'articolo 2, comma 2, affida al Corpo della guardia di finanza **compiti di prevenzione, ricerca e repressione delle violazioni** in una serie di materie e, in particolare, alla lettera *m)* in via generale in "ogni altro interesse economico-finanziario nazionale o dell'Unione europea";
- l'articolo 3, comma 1, prevede la **collaborazione con organi costituzionali** in relazione alle proprie competenze in materia economica e finanziaria e, previe

intese con il Comando generale, con organi istituzionali, Autorità indipendenti ed enti di pubblico interesse che ne facciano richiesta.

Secondo la relazione illustrativa, la previsione è funzionale a un'efficace vigilanza sugli obblighi previsti dal regolamento sulla ciberresilienza, in ragione delle competenze della Guardia di finanza in materia economica e finanziaria e dei suoi compiti di prevenzione, ricerca e repressione delle violazioni. Si tratterebbe di una **collaborazione ad ampio spettro**, ulteriore rispetto al ruolo che il d.lgs. n. 157/2022 (all'articolo 4) già attribuisce al Corpo, insieme all'Agenzia delle dogane e dei monopoli, quale autorità incaricata del controllo dei prodotti che entrano nel mercato dell'Unione (ai sensi dell'articolo 25 del regolamento (UE) 2019/1020).

La relazione tecnica precisa che tale collaborazione rientra tra i compiti istituzionali della Guardia di finanza. Ricorda inoltre che l'ACN, ai sensi dell'articolo 5, comma 5, del decreto-legge n. 82/2021, stipula convenzioni con altre istituzioni pubbliche, incluse le forze di polizia, per collaborare allo svolgimento dei propri compiti.

Infine, il **comma 3** demanda ad un **decreto del Presidente del Consiglio dei ministri**, da adottarsi ai sensi dell'articolo 17, comma 3, della legge n. 400/1988 e di concerto con il Ministro dell'economia e delle finanze, la definizione delle **modalità** e i **termini** per l'**esercizio dei poteri** di cui ai commi 1 e 2.

Articolo 11
(Poteri di vigilanza delle Autorità del settore finanziario e del Garante per la protezione dei dati personali)

L'**articolo 11** disciplina i poteri di vigilanza delle Autorità del settore finanziario **nei confronti degli istituti finanziari vigilati**.

In particolare il **comma 1** prevede che, in quanto autorità di vigilanza del mercato ai sensi dell'articolo 9, comma 2, dello schema di decreto legislativo (si veda la relativa scheda), **le Autorità del settore finanziario**, dispongono, **nei confronti degli istituti finanziari vigilati**, dei poteri previsti dal capo V del regolamento (UE) 2024/2847 relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali, nonché del Capo V del regolamento (UE) 2019/1020, **sulla vigilanza del mercato e sulla conformità dei prodotti** e dal decreto legislativo n. 157 del 2022, concernente l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2019/1020 e la semplificazione e il riordino del relativo sistema di vigilanza del mercato.

Ai sensi dell'articolo 1, lettera m) dello schema di decreto legislativo, le «autorità del settore finanziario» sono la Banca d'Italia, la CONSOB e l'IVASS, in qualità di autorità nazionali di vigilanza del mercato di cui alla lettera b), per il settore finanziario.

Il **Capo V del regolamento (UE) 2024/2847** contiene le disposizioni in materia di Vigilanza del mercato. In particolare nel citato Capo sono contenute le norme relative alla vigilanza del mercato e controllo dei prodotti con elementi digitali nel mercato dell'Unione (art. 52), all'accesso ai dati e alla documentazione da parte delle medesime autorità di vigilanza (art. 53), alla procedura a livello nazionale relativa ai prodotti con elementi digitali che presentano un rischio di cibersicurezza significativo (art. 54), alla procedura di salvaguardia dell'Unione (art. 55), alla procedura a livello di Unione relativa ai prodotti con elementi digitali che presentano un rischio di cibersicurezza significativo (art. 56), ai poteri dell'autorità nei casi di prodotti con elementi digitali conformi che tuttavia presentano un rischio di cibersicurezza significativo (art. 57), ai casi di non conformità formale (art. 58), alle attività congiunte delle autorità di vigilanza del mercato (art. 59) e alle indagini a tappeto (art. 60).

Il **Capo V del regolamento (UE) 2019/1020**, contenente anch'esso le disposizioni in materia di Vigilanza del mercato, disciplina i poteri delle autorità di vigilanza del mercato (art. 14), il recupero dei costi da parte delle autorità di vigilanza del mercato (art. 15), le misure di vigilanza del mercato (art. 16), l'uso delle informazioni, segreto professionale e commerciale (art. 17), i diritti procedurali degli operatori economici (art. 18), i poteri riguardanti i prodotti che

presentano un rischio grave (art. 19), il Sistema di informazione rapida (art. 20) e gli impianti di prova dell'Unione (art. 20).

Restano fermi i **poteri previsti dall'articolo 22 della legge 28 dicembre 2005, n. 262**, che disciplina **la collaborazione con le autorità di vigilanza, di cui all'articolo 5, comma 1, lettera *b)* del decreto legislativo 7 ottobre 2026, n. 179, da parte del Corpo della guardia di finanza**, nell'esercizio dei poteri di vigilanza informativa e ispettiva.

Le autorità di cui all'articolo 5, comma 1, lettera b) del decreto legislativo 7 ottobre 2026, n. 179 sono: la Banca d'Italia, quale autorità competente sui sistemi di IA ad alto rischio utilizzati nell'erogazione di finanziamenti o di altri servizi finanziari disciplinati ai sensi del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385, la CONSOB, quale autorità competente sui sistemi di IA ad alto rischio utilizzati nell'erogazione dei servizi finanziari disciplinati ai sensi del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, l'IVASS, quale autorità competente sui sistemi di IA ad alto rischio utilizzati nell'esercizio dell'attività assicurativa o riassicurativa e di distribuzione di prodotti assicurativi disciplinati ai sensi del codice delle assicurazioni private, di cui al decreto legislativo 7 settembre 2005, n. 209;

Il **comma 2** dispone che le Autorità del settore finanziario nell'esercizio dei poteri di cui al comma 1, possano avvalersi della collaborazione del Corpo della Guardia di finanza ai sensi degli articoli 2, comma 2, lettera *m)*, e 3, comma 1, del decreto legislativo 19 marzo 2001, n. 68.

L'articolo 2, comma 2, lettera m) del decreto legislativo 19 marzo 2001, n. 68 dispone che alla Guardia di finanza siano demandati compiti di prevenzione, ricerca e repressione delle violazioni in materia di ogni altro interesse economico-finanziario nazionale o dell'Unione europea, mentre il comma 1 dell'articolo 3 recita che il Corpo della Guardia di finanza, in relazione alle proprie competenze in materia economica e finanziaria, collabora con gli organi costituzionali e che la stessa collaborazione, previe intese con il Comando generale, può essere fornita agli organi istituzionali, alle Autorità indipendenti e agli enti di pubblico interesse che ne facciano richiesta.

Il **comma 3** precisa che le Autorità del settore finanziario **stipulano un protocollo d'intesa con il Corpo della guardia di finanza** per disciplinare lo **scambio di informazioni per finalità di prevenzione, accertamento e repressione** degli illeciti di natura economico finanziaria.

Infine il **comma 4** prevede che in quanto autorità di vigilanza del mercato ai sensi dell'articolo 9, comma 2, del presente decreto, anche il

Garante per la protezione dei dati personali dispone dei poteri e delle misure di vigilanza previsti dal capo V del regolamento (UE) 2024/2847 relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali, nonché del Capo V del regolamento (UE) 2019/1020, **sulla vigilanza del mercato e sulla conformità dei prodotti** e dal decreto legislativo n. 157 del 2022, concernente l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2019/1020 e la semplificazione e il riordino del relativo sistema di vigilanza del mercato.

Articolo 12
(Collaborazione tra Autorità)

L'**articolo 12** disciplina la **collaborazione tra le autorità di vigilanza del mercato**, prevedendo strumenti di cooperazione e coordinamento finalizzati a favorire lo scambio di informazioni e l'esercizio delle rispettive competenze. A tal fine, la disposizione prevede la stipula di appositi accordi tra le amministrazioni interessate, in conformità a quanto previsto dall'articolo 15 della legge n. 241 del 1990. La collaborazione riguarda sia le autorità di vigilanza del mercato sia le autorità incaricate del controllo dei prodotti che entrano nel mercato dell'Unione europea, nonché gli altri soggetti individuati dalla normativa vigente, nel rispetto di quanto previsto dal decreto legislativo n. 157 del 2022.

Il **comma 1** prevede che, ai fini dell'attuazione dell'articolo 52, paragrafo 14, del regolamento (UE) 2024/2847, le **autorità di vigilanza del mercato** stabiliscano, mediante appositi **accordi** conclusi ai sensi dell'articolo 15 della legge n. 241 del 1990, i **meccanismi di cooperazione e di scambio informativo**.

L'articolo 52 sopra citato disciplina il coordinamento tra le autorità di vigilanza del mercato designate ai sensi del regolamento (UE) 2024/2847 e quelle designate ai sensi del regolamento (UE) 2024/1689 sull'intelligenza artificiale, con riferimento ai prodotti con elementi digitali classificati come sistemi di intelligenza artificiale ad alto rischio, ai sensi dell'articolo 6 del regolamento sull'intelligenza artificiale. In particolare, il paragrafo 14 prevede che le autorità designate ai sensi del regolamento sull'intelligenza artificiale siano responsabili delle attività di vigilanza del mercato previste dal regolamento sulla ciberresilienza per tali prodotti e che cooperino, ove opportuno, con le autorità designate ai sensi di quest'ultimo regolamento. È, inoltre, previsto lo scambio delle informazioni pertinenti ai fini dell'esercizio delle rispettive funzioni, nonché la collaborazione con i CSIRT designati come coordinatori e con l'ENISA per quanto riguarda la sorveglianza sull'attuazione degli obblighi di segnalazione di cui all'articolo 14 del regolamento sulla ciberresilienza.

Il richiamo all'articolo 15 della legge n. 241 del 1990 individua lo strumento giuridico attraverso il quale le amministrazioni interessate possono formalizzare le modalità di cooperazione e di scambio informativo nell'ambito delle rispettive competenze.

Si ricorda, in proposito, che il citato articolo 15 disciplina gli accordi tra pubbliche amministrazioni (cc.dd. accordi orizzontali), mediante i quali è

possibile disciplinare lo svolgimento in collaborazione di attività di interesse comune. La medesima disposizione rinvia, per quanto concerne la relativa disciplina, all'articolo 11, commi 2 e 3, della legge n. 241 del 1990, concernente gli accordi tra privati e pubbliche amministrazioni (cc.dd. accordi verticali). In particolare, è previsto che:

- tali accordi siano stipulati, a pena di nullità, in forma scritta, salvo che sia diversamente stabilito dalla legge;
- ad essi si applicano, ove non diversamente previsto e in quanto compatibili, i principi del codice civile in materia di obbligazioni e contratti;
- tali accordi devono necessariamente recare la motivazione di cui all'articolo 3 della legge n. 241 del 1990;
- essi sono soggetti ai medesimi controlli previsti per i provvedimenti amministrativi.

Il **comma 2**, fermo restando quanto disposto dal decreto legislativo n. 157 del 2022, che adegua la normativa italiana al regolamento UE 2019/1020 in materia di vigilanza del mercato e conformità dei prodotti, attribuisce alle autorità di vigilanza del mercato, alle autorità incaricate del controllo dei prodotti che entrano nel mercato dell'Unione europea (Agenzia delle dogane e dei monopoli e la Guardia di finanza) e agli altri soggetti individuati dall'articolo 3, commi 1 e 2, del medesimo decreto legislativo, la **facoltà di definire tra loro**, sempre mediante gli accordi di cui al già citato articolo 15 della legge n. 241 del 1990, il **coordinamento operativo** e lo **scambio informativo** nell'ambito delle rispettive competenze.

In particolare, i soggetti individuati dall'articolo 3, commi 1 e 2, del decreto legislativo n. 157 del 2022 sono i seguenti:

- Ministero delle imprese e del *made in Italy*;
- Ministero della salute;
- Ministero del lavoro e delle politiche sociali;
- Ministero dell'interno;
- Ministero dell'ambiente e della sicurezza energetica;
- Ministero delle infrastrutture e dei trasporti;
- Ministero dell'agricoltura, della sovranità alimentare e delle foreste;
- Ente nazionale per l'aviazione civile (ENAC).

Articolo 13
(Collaborazione dell'Agenzia e delle autorità del settore finanziario con il Garante per la protezione dei dati personali)

L'**articolo 13** introduce la possibilità di prevedere forme di collaborazione tra l'Agenzia per la cybersicurezza nazionale, le autorità del settore finanziario e il Garante per la protezione dei dati personali.

In particolare il **comma 1** dispone che possono essere previste **forme di coordinamento operativo e di scambio informativo tra l'Agenzia** per la cybersicurezza nazionale, le **autorità del settore finanziario** e **il Garante per la protezione dei dati personali** per assicurare, ove necessario, **la tempestiva e completa condivisione dei dati e delle informazioni** utili all'esercizio delle funzioni di rispettiva competenza, anche nell'ambito degli accordi di cui all'articolo 7, comma 5, del decreto-legge 14 giugno 2021, n. 82.

L'articolo 7, comma 5, del decreto-legge n.82 del 2021 dispone che nel rispetto delle competenze del Garante per la protezione dei dati personali, l'Agenzia per la cybersicurezza nazionale consulta il Garante e collabora con esso, anche in relazione agli incidenti che comportano violazioni di dati personali. L'Agenzia e il Garante possono stipulare appositi protocolli d'intenti che definiscono altresì le modalità della loro collaborazione nell'ambito delle risorse disponibili a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica.

La disposizione in commento **attua inoltre la previsione dell'articolo 52, paragrafo 7, del regolamento (UE) 2024/2847**, che dispone che **le autorità di vigilanza del mercato collaborano, all'occorrenza, con le autorità preposte alla vigilanza del diritto dell'Unione in materia di protezione dei dati**.

Sempre secondo la disposizione citata, rientra in tale cooperazione la comunicazione a dette autorità di qualsiasi risultanza pertinente per l'esercizio delle loro competenze, anche nell'ambito della fornitura di orientamenti e consulenze a norma del paragrafo 10 del citato articolo (che prevede che le autorità di vigilanza del mercato possono fornire agli operatori economici orientamenti e consulenza sull'attuazione del regolamento, con il sostegno della Commissione e, se del caso, dei CSIRT e dell'ENISA), se tali orientamenti e consulenze riguardano il trattamento dei dati personali.

Le autorità preposte alla vigilanza del diritto dell'Unione in materia di protezione dei dati hanno il potere di richiedere qualsiasi documentazione

creata o conservata a norma del presente regolamento e di accedervi, qualora l'accesso a tale documentazione sia necessario per lo svolgimento dei loro compiti. Esse informano le autorità di vigilanza del mercato designate dello Stato membro interessato di tale richiesta.

Articolo 14
(Reclami alle autorità di vigilanza del mercato e segnalazioni al CSIRT Italia)

L'**articolo 14** disciplina la procedura di esame dei **reclami presentati dai consumatori** alle autorità di vigilanza del mercato e la **procedura per la segnalazione** al CSIRT Italia da parte dei consumatori di eventuali **rischi informatici**.

In particolare, il **comma 1** dispone che le autorità di vigilanza del mercato ricevono, secondo le rispettive competenze, i **reclami** ai sensi dell'articolo 52, paragrafo 11, del regolamento (UE) 2024/2847.

Ai sensi dell'articolo 2, comma 2, lett. *i)* del provvedimento in esame, le **autorità di vigilanza del mercato** sono:

- l'Agenzia per la cybersicurezza nazionale (ACN);
- la Banca d'Italia;
- la Commissione nazionale per la società e la borsa (CONSOB);
- l'Istituto per la vigilanza sulle assicurazioni (IVASS);
- il Garante per la protezione dei dati personali.

L'articolo 52, § 11 del regolamento pone in capo alle autorità di vigilanza del mercato il compito di informare i consumatori riguardo a dove possono presentare reclami che potrebbero indicare una non conformità di un prodotto al regolamento e forniscono ai consumatori informazioni su dove e come accedere ai meccanismi per facilitare la segnalazione di vulnerabilità, incidenti e minacce informatiche che possono incidere sui prodotti con elementi digitali.

Le autorità sono tenute a trattare le segnalazioni secondo procedure adottate da ciascuna. Tali procedure devono in ogni caso rispettare le **garanzie** di cui all'articolo 107, commi 6 e 7, del **codice del consumo** (decreto legislativo n. 206 del 2005).

Il codice del consumo prevede che le autorità di vigilanza del mercato, ciascuna per i prodotti di propria competenza, debbano garantire ai consumatori la possibilità di sporgere reclami con riguardo alla sicurezza dei prodotti, alle attività di controllo e vigilanza relativi a prodotti specifici nonché ai casi in cui i rimedi offerti dai consumatori in caso di richiamo di prodotti non siano soddisfacenti, garantendo l'informazione dell'interessato in merito alle eventuali azioni intraprese (articolo 107, comma 6). Le autorità valutano il reclamo e se questo non è manifestamente infondato e sussistono i presupposti per adottare un

provvedimento, assicurano adeguato seguito al reclamo e forniscono al reclamante informazioni riguardo le eventuali misure intraprese (articolo 107, comma 7).

Il **comma 2** demanda a un **decreto del direttore generale** dell'ACN (Agenzia per la cybersicurezza nazionale) la definizione di una **procedura per la trattazione dei reclami** di competenza.

Il **comma 3** prevede che il reclamo ricevuto da un'autorità di vigilanza non competente sia **trasmesso d'ufficio all'autorità competente**, dandone comunicazione al reclamante.

Infine, il **comma 4** rinvia al medesimo decreto del direttore generale dell'ACN di cui al comma 2 la disciplina procedure per la **segnalazione**, da parte dei consumatori, al **CSIRT Italia**, di **vulnerabilità, incidenti e minacce informatiche**.

Il CSIRT Italia opera presso l'Agenzia per la Cybersicurezza Nazionale (ACN) ed è stato istituito dal decreto-legge n. 82 del 2021. È l'organismo competente nella prevenzione, gestione e risposta agli incidenti informatici, e fornisce supporto a soggetti pubblici e privati con l'obiettivo di rafforzare la resilienza complessiva del Paese di fronte alle minacce cibernetiche.

CAPO IV – DISPOSIZIONI SANZIONATORIE

Articolo 15
(Poteri sanzionatori delle autorità di vigilanza del mercato e procedimento di irrogazione delle sanzioni)

L'**articolo 15** disciplina i **poteri sanzionatori** e i procedimenti applicabili dalle autorità di vigilanza del mercato con riguardo all'irrogazione delle sanzioni amministrative per violazioni del regolamento, rinviando alla normativa di settore dell'**ACN**, della **Banca d'Italia**, della **Consob** e dell'**IVASS**, nonché, in via residuale, alla legge generale sulle sanzioni amministrative.

Il **comma 1** prevede che le autorità di vigilanza del mercato irroghino le **sanzioni** individuate dall'articolo 64 del regolamento (UE) 2024/2847, in caso di violazione del regolamento stesso. Ciascuna autorità opera secondo le proprie competenze e conclude il procedimento sanzionatorio entro un **termine ragionevole**.

Si ricorda che, secondo quanto previsto all'articolo 2, comma 2, lettera *l)*, del presente provvedimento, le **autorità di vigilanza del mercato** sono:

- l'Agenzia per la cybersicurezza nazionale (ACN);
- la Banca d'Italia;
- la Commissione nazionale per la società e la borsa (CONSOB);
- l'Istituto per la vigilanza sulle assicurazioni (IVASS);
- il Garante per la protezione dei dati personali.

Quanto all'**individuazione delle sanzioni**, la norma in commento rinvia all'articolo 64 del regolamento (UE) 2024/2847. Tale disposizione precisa il trattamento sanzionatorio per una serie di fattispecie:

- la non conformità ai requisiti essenziali di cibersicurezza (allegato I del regolamento) e agli obblighi di cui agli articoli 13 (obblighi dei fabbricanti) e 14 (obblighi di segnalazione dei fabbricanti) è soggetta a sanzioni amministrative pecuniarie fino a 15 milioni di euro o, se l'autore della violazione è un'impresa, fino al 2,5 per cento del fatturato mondiale totale annuo dell'esercizio precedente, se superiore;
- la non conformità agli obblighi di cui agli articoli da 18 a 23 (obblighi dei rappresentanti autorizzati, degli importatori, dei distributori, casi in cui si applicano gli obblighi dei fabbricanti, identificazione degli

operatori economici) all'articolo 28 (dichiarazione di conformità UE), all'articolo 30, paragrafi da 1 a 4 (regole per la marcatura CE), all'articolo 31, paragrafi da 1 a 4 (documentazione tecnica), all'articolo 32, paragrafi 1, 2 e 3 (procedure di valutazione della conformità per prodotti con elementi digitali), all'articolo 33, paragrafo 5 (documentazione tecnica in formato semplificato per le misure di sostegno per le microimprese e le PMI) e agli articoli 39 (requisiti relativi agli organismi notificati), 41 (affiliate e subappaltatori degli organismi notificati), 47 (obblighi operativi degli organismi notificati), 49 (obbligo di informazione a carico degli organismi notificati) e 53 (accesso ai dati e documentazione) è soggetta a sanzioni amministrative pecuniarie fino a 10 milioni di euro o, se l'autore della violazione è un'impresa, fino al 2 per cento del fatturato mondiale totale annuo dell'esercizio precedente, se superiore;

- la fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati e alle autorità di vigilanza del mercato è soggetta a sanzioni amministrative pecuniarie fino a 5 milioni di euro o, se l'autore della violazione è un'impresa, fino all'1 per cento del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Il paragrafo 5 dell'articolo 64 stabilisce inoltre i criteri da considerare nella determinazione dell'importo della sanzione amministrativa pecuniaria, tra cui la natura, la gravità e la durata della violazione e delle sue conseguenze, l'eventuale precedente applicazione di sanzioni per violazioni analoghe, le dimensioni e la quota di mercato dell'operatore economico. Il paragrafo 10 del medesimo articolo esclude invece l'applicazione delle sanzioni amministrative pecuniarie ai fabbricanti che si qualificano come microimprese o piccole imprese per il mancato rispetto dei termini di segnalazione di cui all'articolo 14, paragrafo 2, lettera *a)*, o paragrafo 4, lettera *a)*, nonché per le violazioni del regolamento commesse dai gestori di *software open source*.

Quanto alla previsione della conclusione del procedimento sanzionatorio entro un termine ragionevole, si richiama la sentenza della Corte costituzionale n. 151 del 2021, la quale ha dichiarato inammissibili le questioni di legittimità costituzionale dell'articolo 18 della legge n. 689 del 1981. Tale disposizione, nel disciplinare la conclusione della fase decisoria del procedimento amministrativo sanzionatorio, non prevede un termine per l'emissione dell'ordinanza-ingiunzione o dell'ordinanza di archiviazione degli atti, stabilendo la legge unicamente il termine di prescrizione quinquennale del diritto alla riscossione delle somme dovute per le violazioni amministrative, a differenza di quanto previsto da specifiche normative di settore, che hanno introdotto un termine di decadenza per l'adozione dei provvedimenti sanzionatori, determinato dalla legge o, in alcuni casi, dalla stessa autorità procedente in via regolamentare ovvero in sede di avvio

del procedimento. Pur ritenendo essenziale la previsione legislativa di un limite temporale per l'adozione del provvedimento sanzionatorio, il cui inutile decorso produca la consumazione del potere, la Corte non ha potuto tuttavia sanare la denunciata omissione legislativa, in quanto l'individuazione di termini adeguati è rimessa alla valutazione del legislatore. La Corte ha quindi sottolineato l'esigenza di un tempestivo intervento normativo in materia.

Il **comma 2** prevede che le modalità di adozione delle sanzioni da parte dell'**Agenzia per la cybersicurezza nazionale** siano definite con il regolamento previsto dall'articolo 17, comma 4-*quater*, del decreto-legge n. 82 del 2021, introdotto dall'articolo 11, comma 1, della legge n. 90 del 2024.

La disposizione appena richiamata prevede che la disciplina del procedimento sanzionatorio amministrativo dell'Agenzia sia definita con regolamento e che esso stabilisca termini e modalità con riguardo alle violazioni della normativa in materia di cybersicurezza, disponendone:

- l'accertamento;
- la contestazione;
- la notificazione;
- l'irrogazione delle relative sanzioni di competenza dell'Agenzia.

Il regolamento è adottato, entro novanta giorni dalla data di entrata in vigore della disposizione (ma allo stato non risulta essere stato ancora adottato), con decreto del Presidente del Consiglio dei ministri, anche in deroga all'articolo 17 della legge n. 400 del 1988, sentito il Comitato interministeriale per la cybersicurezza e acquisito il parere delle competenti Commissioni parlamentari. Fino alla data di entrata in vigore del regolamento, ai procedimenti sanzionatori si applicano, per ciascuna fase procedimentale, le disposizioni contenute nelle sezioni I e II del capo I della legge n. 689 del 1981 sul procedimento sanzionatorio amministrativo.

Il **comma 3** dispone che alle sanzioni di cui al presente capo irrogate dalla **Banca d'Italia** si applica **la procedura sanzionatoria di cui all'articolo 145 del testo unico delle leggi in materia bancaria e creditizia**, di cui al decreto legislativo 1° settembre 1993, n. 385.

L'articolo **145 del testo unico delle leggi in materia bancaria e creditizia**, di cui al decreto legislativo 1° settembre 1993, n. 385 prevede che la Banca d'Italia contestati gli addebiti ai soggetti interessati, tenuto conto del complesso delle informazioni raccolte, applica le sanzioni con provvedimento motivato. I soggetti interessati possono, entro trenta giorni dalla contestazione, presentare deduzioni e chiedere un'audizione personale in sede di istruttoria, cui possono partecipare anche con l'assistenza di un avvocato. Il procedimento sanzionatorio è retto dai principi del contraddittorio, della conoscenza degli atti istruttori, della

verbalizzazione nonché della distinzione tra funzioni istruttorie e funzioni decisorie. Il provvedimento di applicazione delle sanzioni previste dal presente titolo è pubblicato senza ritardo e per estratto sul sito web della Banca d'Italia. Nel caso in cui avverso il provvedimento di applicazione della sanzione sia adita l'autorità giudiziaria, la Banca d'Italia menziona l'avvio dell'azione giudiziaria e l'esito della stessa nel proprio sito web a margine della pubblicazione. La Banca d'Italia, tenuto conto della natura della violazione e degli interessi coinvolti, può stabilire modalità ulteriori per dare pubblicità al provvedimento, ponendo le relative spese a carico dell'autore della violazione. Nel provvedimento di applicazione della sanzione la Banca d'Italia dispone la pubblicazione in forma anonima del provvedimento sanzionatorio quando quella ordinaria: a) abbia ad oggetto dati personali ai sensi del decreto legislativo 30 giugno 2003, n. 196, la cui pubblicazione appaia sproporzionata rispetto alla violazione sanzionata; b) possa comportare rischi per la stabilità dei mercati finanziari o pregiudicare lo svolgimento di un'indagine penale in corso; c) possa causare un pregiudizio sproporzionato ai soggetti coinvolti, purché tale pregiudizio sia determinabile. Se le situazioni sopra descritte hanno carattere temporaneo, la pubblicazione è effettuata quando queste sono venute meno. Contro il provvedimento che applica la sanzione è ammesso ricorso alla corte di appello di Roma.

Il **comma 4** prevede che alle sanzioni irrogate dalla **Consob si applica la procedura sanzionatoria di cui agli articoli da 195 a 195-*ter*, 195-*quinquies* e 196-*ter* del testo unico delle disposizioni in materia di intermediazione finanziaria**, di cui al decreto legislativo 24 febbraio 1998, n. 58.

Gli articoli citati non disciplinano esclusivamente gli aspetti procedurali delle sanzioni. In particolare mentre l'articolo 195 disciplina effettivamente la procedura sanzionatoria, l'articolo 195.1 stabilisce i principi sulle sanzioni amministrative, l'articolo 195.2 l'ipotesi di concorso di sanzioni amministrative di competenza della Banca d'Italia e della Consob, l'articolo 195-*bis* la pubblicazione delle sanzioni e l'articolo 195-*ter* la comunicazione all'ABE e all'AESFEM sulle sanzioni applicate. Con l'articolo 195-*quinquies* dispone l'inapplicabilità di specifiche disposizioni della legge 24 novembre 1981, n. 689 e l'articolo 196-*ter* disciplina la possibilità che il soggetto destinatario della lettera di contestazione di addebiti da parte di Consob e Banca d'Italia possa presentare impegni tali da far venir meno i profili di lesione degli interessi tutelati e le relative conseguenze.

Il **comma 5** infine dispone che alle irrogate dall'**IVASS** si applica la procedura sanzionatoria di cui agli articoli 311-*septies*, 324-*octies* e 325- *ter* del codice delle assicurazioni private, di cui al decreto legislativo 7 settembre 2005, n. 209.

L'articolo 311-*septies* disciplina la procedura sanzionatoria prevedendo che l'IVASS nel termine di centoventi giorni dall'accertamento dell'infrazione, ovvero nel termine di centottanta giorni per i soggetti residenti all'estero, provvede alla contestazione degli addebiti nei confronti dei possibili responsabili della violazione. Entro il termine di sessanta giorni dalla notifica della contestazione, il destinatario può presentare all'IVASS deduzioni difensive e istanza di audizione, cui può partecipare anche con l'assistenza di un avvocato. L'IVASS, tenuto conto degli elementi istruttori acquisiti agli atti, applica le sanzioni o dispone l'archiviazione del procedimento con provvedimento motivato. Il procedimento sanzionatorio è retto dai principi del contraddittorio, della conoscenza degli atti istruttori, della verbalizzazione nonché della distinzione tra funzioni istruttorie e funzioni decisorie. La tutela giurisdizionale davanti al giudice amministrativo è disciplinata dal codice del processo amministrativo. I ricorsi sono notificati all'IVASS che provvede alla difesa in giudizio con propri legali. L'opposizione non sospende l'esecuzione del provvedimento.

L'articolo 324-*octies* ha ad oggetto la procedura di applicazione delle sanzioni amministrative nei confronti degli intermediari e degli esponenti aziendali o del personale della società di intermediazione assicurativa o riassicurativa mentre l'articolo 325-*ter* disciplina la pubblicazione delle sanzione prevedendo che i provvedimenti di applicazione delle sanzioni, le sentenze dei giudici amministrativi che decidono i ricorsi e i decreti che decidono i ricorsi straordinari al Presidente della Repubblica sono pubblicati per estratto nel Bollettino e sul sito internet dell'IVASS. L'IVASS, tenuto conto della violazione e degli interessi coinvolti, può stabilire modalità ulteriori per dare pubblicità al provvedimento, ponendo le relative spese a carico dell'autore della violazione, le fattispecie nelle quali l'Ivass può disporre la pubblicazione in forma anonima del provvedimento sanzionatorio e quelli nei quali la medesima autorità può escludere la pubblicazione del provvedimento sanzionatorio.

Il **comma 6** prevede che, per quanto non diversamente disposto dal provvedimento in commento e dalle procedure proprie di ciascuna autorità, trovi applicazione, in quanto compatibile, la **legge n. 689 del 1981**.

Si segnala che l'articolo in commento non prevede un espresso rinvio a una specifica procedura sanzionatoria per il Garante per la protezione dei dati personali, pur ricompreso, come anticipato, tra le autorità di vigilanza del mercato ai sensi dell'articolo 2, comma 2, lettera *l)*, del presente provvedimento.

In base a tale legge l'applicazione della sanzione amministrativa pecuniaria avviene secondo il seguente procedimento:

- accertamento, contestazione-notifica al trasgressore;
- pagamento in misura ridotta o inoltro di memoria difensiva all'autorità amministrativa: archiviazione o emanazione di ordinanza ingiunzione di pagamento da parte dell'autorità amministrativa;

- eventuale opposizione all'ordinanza ingiunzione davanti all'autorità giudiziaria (giudice di pace o tribunale);
- accoglimento dell'opposizione, anche parziale, o rigetto (sentenza soggetta agli ordinari mezzi di impugnazione, secondo le disposizioni applicabili);
- eventuale esecuzione forzata per la riscossione delle somme.

Con riferimento al termine di conclusione del procedimento si rinvia a quanto esposto sopra.

Infine, si segnala che l'articolo in commento attua il criterio direttivo specifico di cui all'articolo 15, comma 2, lettera *f)* della legge n. 36 del 2026 (legge di delegazione europea 2025), ossia "definire il sistema sanzionatorio prevedendo sanzioni effettive, dissuasive e proporzionate alla gravità, alla durata e all'eventuale reiterazione della violazione degli obblighi derivanti dal regolamento (UE) 2024/2847". La tabella di concordanza specifica che rispetto all'applicabilità delle sanzioni ai soggetti pubblici, sul cui tema il regolamento lascia discrezionalità agli Stati membri (articolo 64, paragrafo 7), si è optato per la loro esclusione.

Articolo 16
(Devoluzione dei proventi)

L'**articolo 16** disciplina la **destinazione dei proventi delle sanzioni amministrative pecuniarie**, prevedendo la loro riassegnazione al bilancio dell'**Agenzia per la cybersicurezza nazionale**, per le sanzioni irrogate dalla medesima Agenzia, e facendo salve le disposizioni delle rispettive normative per le sanzioni irrogate dalle **autorità del settore finanziario** e dal **Garante per la protezione dei dati personali**.

Il **comma 1** prevede che i **proventi delle sanzioni amministrative** pecuniarie irrogate dall'**Agenzia per la cybersicurezza nazionale** ai sensi del presente provvedimento siano **versati all'entrata del bilancio dello Stato**. Tali proventi sono poi riassegnati, nel medesimo esercizio finanziario, al capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze relativo alle somme da assegnare all'Agenzia per la cybersicurezza nazionale (articolo 18 del decreto-legge n. 82 del 2021).

Si segnala che la norma di delega contenuta all'articolo 15 della legge di delegazione europea 2025 (legge n. 36 del 2026) individua tra i principi e i criteri direttivi specifici, la previsione che gli introiti derivanti dall'irrogazione delle sanzioni siano versati all'entrata del bilancio dello Stato per essere riassegnati all'apposito capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze per incrementare la dotazione del bilancio dell'Agenzia per la cybersicurezza nazionale (articolo 15, comma 2, lettera *f)*, numero 4), della legge n. 36 del 2026).

Il **comma 2** dispone che con riguardo ai proventi delle sanzioni amministrative irrogate dalle autorità del settore finanziario e dal Garante per la protezione dei dati personali, di cui all'articolo 9, comma 2, del presente decreto, **resta fermo quanto previsto dalle rispettive normative di settore**.

- ***La destinazione dei proventi delle sanzioni amministrative nel settore finanziario***

Il quadro normativo nazionale che disciplina l'attribuzione delle somme derivanti dall'irrogazione di sanzioni amministrative pecuniarie da parte delle Autorità di vigilanza del settore finanziario, bancario e assicurativo risponde al principio generale del conferimento dei proventi al **bilancio dello Stato**, fatte salve specifiche eccezioni di riassegnazione a fondi di tutela. Tale assetto

garantisce la terzietà e l'indipendenza delle singole Autorità, escludendo che i proventi sanzionatori possano integrare i rispettivi bilanci di funzionamento.

1. Sanzioni in Materia Finanziaria e di Intermediazione (Banca d'Italia e Consob)

Con riferimento ai provvedimenti sanzionatori adottati in applicazione del **Testo Unico della Finanza (TUF - D. Lgs. 24 febbraio 1998, n. 58)**, la destinazione delle somme è governata dall'**articolo 195.1, comma 5**. La disposizione prevede che i proventi affluiscano all'entrata del bilancio dello Stato. In deroga parziale a tale principio, il medesimo comma, fa salvo quanto previsto dall'articolo **32-ter.1, comma 2 del TUF** che stabilisce che una quota pari al **50 per cento dei proventi** delle sanzioni applicate per la violazione delle norme del TUF in materia di intermediari (di cui alla Parte II del medesimo Testo Unico) sia devoluta al **"Fondo per la tutela stragiudiziale dei risparmiatori e degli investitori"**, istituito presso la Consob. Tale fondo è finalizzato ad agevolare l'accesso dei risparmiatori ai meccanismi di risoluzione alternativa delle controversie (ADR).

2. Sanzioni in Materia Bancaria e Creditizia (Banca d'Italia)

Per quanto concerne i procedimenti sanzionatori promossi nell'esercizio della vigilanza bancaria, creditizia e finanziaria ai sensi del **Testo Unico Bancario (TUB – D. Lgs. 1° settembre 1993, n. 385)**, l'**articolo 145** del medesimo testo normativo, avente ad oggetto la disciplina sanzionatoria dispone che le somme riscosse a titolo di sanzione pecuniaria sono interamente devolute **al bilancio dello Stato**.

3. Sanzioni in Materia Assicurativa (IVASS)

Nel settore della vigilanza assicurativa, l'irrogazione e la riscossione delle sanzioni sono disciplinate dal **Codice delle Assicurazioni Private (CAP - D. Lgs. 7 settembre 2005, n. 209)**, con particolare riferimento all'**articolo 328** in materia di riscossione coattiva. Tale norma tuttavia non indica la destinazione dei proventi delle sanzioni amministrative limitandosi a prevedere che la destinazione alla CONSAP S.p.A. dei proventi di specifiche sanzioni amministrative. In ragione di ciò secondo le regole generali della contabilità pubblica, in mancanza di una destinazione speciale le somme afferiscono al bilancio dello Stato.

Con riferimento al **Garante per la protezione dei dati personali**, l'articolo 166, comma 7, del decreto legislativo n. 196 del 2003 (Codice in materia di protezione dei dati personali) prevede che i proventi delle sanzioni, nella misura del 50 per cento del totale annuo, siano riassegnati al fondo di cui all'articolo 156, comma 8, del medesimo decreto legislativo (relativo alle spese di funzionamento del Garante), per essere destinati alle specifiche attività svolte dal Garante con riguardo alla sensibilizzazione e alla ispezione, nonché all'attuazione del regolamento (UE) 2016/679.

CAPO V – MISURE PER LE MICROIMPRESE E LE PICCOLE IMPRESE E DI SEMPLIFICAZIONE

Articolo 17
(Terminale per le segnalazioni al CSIRT Italia)

L'**articolo 17** prevede che l'Agenzia per la cybersicurezza nazionale adegui il Portale segnalazioni per consentire le notifiche previste dal regolamento sulla ciberresilienza e per collegarlo alla piattaforma unica di segnalazione gestita da **ENISA**.

L'**articolo 17**, composto da un solo comma, prevede che, ai fini dell'attuazione dell'articolo 16 del regolamento (UE) 2024/2847, l'Agenzia per la cybersicurezza nazionale adegui il proprio Portale segnalazioni per gli adempimenti di notifica e per il collegamento alla piattaforma di segnalazione di ENISA.

L'articolo 16 del **regolamento (UE) 2024/2847** disciplina il sistema attraverso cui le segnalazioni di vulnerabilità e incidenti vengono raccolte e condivise tra le autorità europee, e si compone di sei paragrafi.

Al paragrafo 1, si stabilisce che ENISA crea e gestisce la piattaforma, con punti di accesso elettronici nazionali ed europei. Serve per le notifiche obbligatorie di cui all'articolo 14 e quelle volontarie di cui all'articolo 15.

Il fabbricante deve segnalare le **vulnerabilità attivamente sfruttate** e gli **incidenti gravi che incidono sulla sicurezza del prodotto**. Le segnalazioni raggiungono il **CSIRT** (*Computer Security Incident Response Team*) competente – il gruppo nazionale di risposta agli incidenti informatici – ed ENISA attraverso questa infrastruttura comune. Sono possibili anche segnalazioni volontarie da persone fisiche o giuridiche.

Il paragrafo 2 dispone che il primo CSIRT che riceve la notifica la inoltri senza ritardo ai CSIRT degli Stati in cui il fabbricante indica che il prodotto è disponibile. Eccezionalmente può rinviare la condivisione per ragioni di cibersicurezza, motivando la decisione a ENISA e indicando quando procederà.

Occorre distinguere due situazioni:

- **Ritardo verso gli altri CSIRT:** il rinvio riguarda la diffusione tra autorità nazionali; normalmente ENISA continua ad avere accesso alle informazioni.
- **Limitazione anche dell'accesso di ENISA:** è ammessa soltanto in circostanze particolarmente eccezionali e per la notifica della vulnerabilità prevista entro 72 ore. Il fabbricante deve indicare una delle tre condizioni stabilite dall'articolo: sfruttamento conosciuto limitato a uno Stato membro, possibile pregiudizio agli interessi essenziali di quello Stato oppure rischio di cybersicurezza elevato e imminente derivante dalla diffusione.

- Il paragrafo 3 stabilisce che i CSIRT trasmettano alle autorità nazionali di vigilanza del mercato le informazioni necessarie per svolgere i loro compiti. Queste verificano il rispetto del regolamento e possono intervenire sui prodotti che presentano rischi, richiedendo misure correttive o restrittive. La segnalazione può quindi alimentare anche l'attività di controllo del mercato.
- Il paragrafo 4 prescrive che ENISA debba proteggere la piattaforma con misure tecniche, operative e organizzative proporzionate. Se un incidente la compromette, deve informare tempestivamente la rete dei CSIRT e la Commissione.

  Stante il disposto del paragrafo 5, ENISA e la rete dei CSIRT definiscono le specifiche di sicurezza. Le vulnerabilità ancora prive di rimedi richiedono protocolli rigorosi e accesso limitato a chi necessita delle informazioni.

  Infine, il paragrafo 6 stabilisce che nelle procedure di divulgazione coordinata, il CSIRT può ritardare la diffusione per motivi giustificati, per il tempo strettamente necessario e fino al consenso delle parti coinvolte. Resta possibile la notifica volontaria del fabbricante.

Articolo 18
(Misure per le microimprese e le piccole e medie imprese, comprese le start-up*)*

L'**articolo 18** reca misure di sostegno alle microimprese e alle piccole e medie imprese (PMI), comprese le *start-up* (imprese di nuova costituzione a carattere innovativo). In particolare, prevede iniziative dell'ACN per lo sviluppo delle competenze (comma 1), affida al MIMIT e all'ACN la definizione delle modalità di attuazione delle azioni di sostegno (comma 2) e fissa criteri per le tariffe della valutazione della conformità (comma 3).

L'articolo 18 si compone di tre commi e promuove misure di cybersicurezza per le microimprese e le piccole e medie imprese, comprese le *start-up*.

Nello specifico, al **comma 1**, si prevede che l'Agenzia per la cybersicurezza nazionale, in qualità di Centro nazionale di coordinamento ai sensi dell'articolo 7, comma 1, lettera *aa)*, del decreto-legge n. 82/2021 (legge n. 109/2021), promuova iniziative volte a **rafforzare le competenze digitali in un contesto cyberresiliente**, nonché a **sviluppare le capacità in materia di cybersicurezza e resilienza**.

Ai sensi dell'articolo 7, comma 1, lettere *aa)* del decreto-legge n. 82/2021, l'Agenzia per la cybersicurezza nazionale è designata quale Centro nazionale di coordinamento ai sensi dell'articolo 6 del regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio, istitutivo del Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e della rete dei centri nazionali di coordinamento.

Al **comma 2** si prevede che, nell'ambito degli accordi di cui all'articolo 12, comma 2, del presente decreto, il Ministero delle imprese e del made in Italy e l'Agenzia per la cybersicurezza nazionale definiscano, secondo le rispettive competenze, le **modalità e le procedure necessarie** ai fini dell'attuazione dell'articolo 33, paragrafo 1, del regolamento (UE) 2024/2847, prevedendo altresì il coordinamento operativo con le amministrazioni competenti e le altre autorità di vigilanza del mercato.

Il paragrafo 1 dell'articolo 33 del Regolamento (UE) 2024/2847 riguarda le **misure di sostegno che gli Stati membri devono predisporre, ove opportuno, per microimprese e piccole imprese** nell'applicazione del regolamento.

Si prevedono **tre tipi di intervento**:

- **formazione e sensibilizzazione**: gli Stati membri dovrebbero organizzare attività specifiche per spiegare come applicare il regolamento;
- **un canale dedicato di assistenza**: dovrebbe essere creato un punto di contatto attraverso il quale micro e piccole imprese possano ricevere consulenza e risposte sui dubbi relativi all'attuazione del regolamento; il canale può coinvolgere anche le autorità pubbliche locali;
- **sostegno per test e valutazione della conformità**: gli Stati membri dovrebbero aiutare le imprese nelle attività necessarie a verificare che i prodotti rispettino i requisiti del regolamento, eventualmente con il supporto del **Centro europeo di competenza per la cybersicurezza.**

Infine, il **comma 3** prevede che, nella determinazione delle tariffe applicabili alle procedure di valutazione della conformità, l'organismo di valutazione della conformità tenga conto delle **esigenze delle microimprese e delle piccole e medie imprese, comprese le *start-up***, assicurando che tali tariffe siano proporzionate alle loro specifiche caratteristiche ed esigenze. L'organismo **limita** inoltre **l'esecuzione delle procedure di esame e delle prove previste dal regolamento ai casi in cui esse risultino effettivamente necessarie**, adottando un approccio proporzionato e basato sul rischio. Secondo la relazione illustrativa, la disposizione è coerente con l'articolo 32, paragrafo 6, del regolamento del regolamento (UE) 2024/2847.

L'articolo 32, paragrafo 6, del regolamento prevede che, nel definire le tariffe per le procedure di valutazione della conformità, si tenga conto degli interessi e delle esigenze specifici delle microimprese e delle PMI, comprese le *start-up*, e che tali tariffe «sono ridotte proporzionalmente» a tali interessi ed esigenze. Il riferimento all'applicazione della procedura d'esame e delle prove «solo ove opportuno» e secondo un approccio basato sul rischio è contenuto nel considerando 96 del regolamento.

CAPO VI – SPAZI DI SPERIMENTAZIONE NORMATIVA

Articolo 19
(Istituzione e gestione dello spazio di sperimentazione normativa per la ciberresilienza)

L'**articolo 19,** composto da **6 commi**, istituisce la "**Sandbox-CRA**" quale spazio di sperimentazione normativa per la ciberresilienza, sotto la supervisione e l'orientamento dell'ACN in qualità di autorità di vigilanza del mercato (**comma 1**). Essa prevede ambienti di **prova controllati** nei quali i **prodotti innovativi con elementi digitali** possono essere **sviluppati** e **testati**, ai fini della verifica della loro conformità, per un periodo limitato precedente all'immissione sul mercato (**comma 2**). La disciplina di dettaglio è demandata a un decreto del direttore generale dell'Agenzia e prevede un **accesso prioritario** per le micro e piccole imprese (**commi 3 e 4**). I servizi possono avvalersi **dell'infrastruttura di calcolo** ad alte prestazioni dell'Agenzia (**comma 5**). Per i prodotti vigilati da Banca d'Italia, CONSOB, IVASS e Garante privacy, l'Agenzia **coinvolge** tali autorità (**comma 6**).

Nel dettaglio, il **comma1 istituisce** la **"Sandbox-CRA"** sotto la supervisione, l'orientamento e il sostegno diretti dell'**Agenzia nazionale per la cybersicurezza** (ACN), in qualità di autorità di vigilanza del mercato.

A tale riguardo, l'articolato specifica che tale disposizione attua l'articolo 33, paragrafo 2, del *Cyber Resilience Act* (regolamento (UE) 2024/2837), che consente agli Stati membri di **istituire spazi di sperimentazione normativa** per la **ciberresilienza**, intesi come ambienti di prova controllati per lo sviluppo e la verifica di conformità dei prodotti innovativi con elementi digitali, per un periodo limitato anteriore all'immissione sul mercato. Tali spazi devono garantire un accesso aperto, equo e trasparente, con particolare riguardo alle microimprese, alle piccole imprese e alle *start-up*. Essi operano sotto la **supervisione delle autorità di vigilanza del mercato**, i cui poteri correttivi e di sorveglianza restano impregiudicati.

A tale riguardo, l'articolo 52, paragrafo 2, del citato regolamento, richiamato anche dal testo del comma, prevede la possibilità per gli Stati membri di designare una o più autorità di vigilanza del mercato per garantire l'efficace applicazione del regolamento.

Il **comma 2 specifica** che la "Sandbox-CRA" prevede **ambienti di prova controllati** per prodotti innovativi con elementi **digitali** per facilitarne lo sviluppo, la progettazione, la convalida e le prove ai fini della **conformità** al regolamento per un periodo di tempo limitato precedente alla loro immissione sul mercato.

Il **comma 3 demanda** a un **decreto** del **direttore dell'ACN** la disciplina relativa a:

a) le modalità di **gestione**, di **funzionamento** e di **cessazione** della "Sandbox-CRA";

b) i **servizi** erogati nell'ambito della "Sandbox-CRA";

c) l'ambito di **applicazione** soggettivo;

d) i criteri di **ammissibilità** e di **selezione** dei **progetti** di sperimentazione, prevedendo, l'accesso prioritario e agevolato alle **microimprese** e alle **piccole imprese**, comprese le *start-up*;

Tale lettera riproduce le disposizioni di cui all'articolo 33, paragrafo 2, ultimo periodo del *Cyber Resilience Act* che prescrive agli Stati membri di garantire un accesso aperto, equo e trasparente agli spazi di sperimentazione normativa e, in particolare, ne facilitano l'accesso delle microimprese e delle piccole imprese, comprese le *start-up*.

e) i requisiti della **domanda di partecipazione** alla Sandbox-CRA e le procedure per la sua valutazione, da concludersi entro novanta giorni dalla data di presentazione della domanda medesima, nonché le modalità di **partecipazione**, **monitoraggio** e **uscita** dalla Sandbox-CRA;

f) la **durata massima** della **partecipazione** alla sperimentazione, proporzionata alla complessità e alla portata del progetto, e i criteri per la sua eventuale proroga;

g) le modalità e le procedure per lo svolgimento di **ulteriori** eventuali **fasi** della sperimentazione normativa, se previste da atti di esecuzione della Commissione europea o da buone pratiche riconosciute a livello europeo;

h) ogni **altro aspetto** relativo all'**istituzione** e al **funzionamento** della Sandbox-CRA e ai relativi servizi

Il **comma 4** dispone che il decreto di cui al comma precedente è adottato tenendo conto degli **atti di esecuzione della Commissione europea** e delle **buone pratiche** riconosciute a livello europeo in materia di spazi di sperimentazione normativa per la ciberresilienza e può essere aggiornato periodicamente.

Il **comma 5** prevede che l'erogazione dei **servizi** disciplinati dal decreto di cui al comma 3 può avvenire anche attraverso l'utilizzo dell'infrastruttura di *high performance computing* di proprietà dell'ACN idonea a consentire *test* regolatori e verifiche di conformità.

Il sistema di calcolo ad alte prestazioni (*High Performance Computing, HPC*) dell'ACN, denominato **Megaride**, è nato su iniziativa dell'Agenzia e del Ministero dell'Università e della Ricerca, ed è stato inaugurato il 27 giugno 2025 presso il polo di San Giovanni a Teduccio dell'Università degli Studi di Napoli Federico II. La gestione del *data center* è affidata al consorzio Cineca. L'Agenzia si avvale di una quota della capacità di calcolo dell'infrastruttura per finalità di monitoraggio, prevenzione e contrasto della minaccia cibernetica, anche mediante il ricorso ad algoritmi di intelligenza artificiale.

Il **comma 6 disciplina** l'ipotesi in cui la sperimentazione nell'ambito della Sandbox-CRA abbia ad oggetto prodotti con elementi digitali sottoposti alla vigilanza delle **autorità del settore finanziario –** ossia, come indicato dalla relazione illustrativa, la banca d'Italia, la Consob, l'IVASS **–** e del **Garante per la protezione dei dati personali**, di cui all'articolo 9, comma 2, del decreto in rassegna. In tali casi, il comma in esame dispone che **l'ACN coinvolge le predette autorità** per i profili di rispettiva competenza. Le modalità di collaborazione sono definite con **decreto** del direttore generale dell'Agenzia, adottato d'intesa con le autorità stesse.

Articolo 20
(Promozione dell'innovazione e coordinamento con gli altri spazi di sperimentazione)

L'**articolo 20**, composto da **quattro commi**, definisce gli strumenti con cui la **Sandbox-CRA** si **raccorda**, da un lato, con le **infrastrutture europee** e **nazionali** di sostegno all'i**nnovazione digitale** e, dall'altro, con gli altri regimi di **sperimentazione normativa** già operanti nell'ordinamento, con specifico riguardo al settore finanziario e a quello dell'intelligenza artificiale.

Nel dettaglio, il **comma 1** consente all'**ACN**, nell'esercizio delle funzioni di gestione della Sandbox-CRA, di **avvalersi di strutture e soggetti esterni**, anche mediante la stipula di specifici **accordi di collaborazione**. I soggetti e gli strumenti indicati sono:

- gli **impianti di prova e sperimentazione** (*Testing and Experimentation Facilities*, TEF);
- i **poli europei dell'innovazione digitale** (*European Digital Innovation Hubs*, EDIH);
- gli spazi di sperimentazione normativa istituiti in **altri settori**;
- i **laboratori universitari** di ricerca e di sperimentazione;
- i **centri di eccellenza**;
- il **supporto tecnico della AI Factory italiana** (IT4LIA).

A riguardo, si ricorda che TEF ed EDIH sono strumenti finanziati nell'ambito del programma Europa digitale (regolamento (UE) 2021/694): i primi offrono infrastrutture per la prova di soluzioni tecnologiche in condizioni reali, i secondi servizi di accompagnamento alla transizione digitale di imprese e pubbliche amministrazioni.

IT4LIA è la ***AI Factory* italiana**, inserita nella rete europea delle AI Factories promossa dall'impresa comune EuroHPC e ospitata dal Cineca, che, con il finanziamento del Ministero dell'università e della ricerca e dell'Agenzia per la cybersicurezza nazionale e il cofinanziamento della Commissione europea, mette gratuitamente a disposizione di startup, imprese, pubbliche amministrazioni e istituzioni accademiche le risorse di supercalcolo (tra cui il sistema Leonardo) e servizi specialistici per lo sviluppo, la sperimentazione e la verifica di affidabilità e conformità di soluzioni di intelligenza artificiale

Il **comma 2** attribuisce alla Sandbox-CRA la **facoltà** di promuovere la **partecipazione** a iniziative di **cooperazione transfrontaliera e a progetti pilota**. Tali attività sono preordinate a un duplice obiettivo: l'elaborazione di buone pratiche condivise e il reciproco riconoscimento degli esiti delle sperimentazioni.

Il **comma 3** rinvia a un **decreto del Presidente del Consiglio dei ministri (d.P.C.M.)** la definizione delle modalità di **collaborazione e coordinamento tra la Sandbox-CRA e la sperimentazione FinTech**. Il decreto è adottato su proposta dell'ACN, d'intesa con le autorità del settore finanziario, che la relazione illustrativa individua nella Banca d'Italia, nella Consob e nell'IVASS, e sentito il **Ministero dell'economia e delle finanze**.

Si ricorda che la disciplina italiana del Comitato e della **sperimentazione *FinTech*** (c.d. "*sandbox* regolamentare") è contenuta in apposito regolamento, di cui al decreto 30 aprile 2021, n. 100, che il Ministero dell'economia e delle finanze ha emanato in attuazione dell'**articolo 36, commi 2-*bis*** e seguenti, del decreto-legge n. 34 del 2019.

Il **Comitato *FinTech*** è stato istituito presso il Ministero dell'economia e delle finanze con il compito di individuare gli obiettivi, definire i programmi e porre in essere le azioni per favorire lo **sviluppo** della **tecno-finanza**, anche in cooperazione con soggetti esteri, nonché di formulare proposte di carattere normativo e agevolare il contatto degli operatori del settore con istituzioni e autorità.

In quest'ambito, è stata avviata una **sperimentazione**, che coinvolge gli operatori *FinTech*, volta al perseguimento dell'**innovazione** di servizi e prodotti nei settori finanziario, creditizio, assicurativo e dei mercati regolamentati, mediante nuove tecnologie, quali l'intelligenza artificiale (IA) e i registri distribuiti (*Distributed ledger technology* – DLT).

Per accedere alla sperimentazione, gli operatori devono presentare all'autorità di vigilanza competente per materia **progetti** relativi ad attività che offrono servizi, prodotti o processi innovativi nel **settore bancario, finanziario o assicurativo** e che arrecano benefici per gli utenti finali o contribuiscono all'efficienza del mercato. I progetti devono essere in uno stato sufficientemente avanzato per la sperimentazione e sostenibili da un punto di vista economico e finanziario.

In tal modo, la ***regulatory sandbox*** consente agli operatori *FinTech* di **testare soluzioni innovative**, potendo beneficiare del costante **dialogo con le autorità di vigilanza** (Banca d'Italia, CONSOB e IVASS). Allo stesso tempo, le autorità responsabili per la regolamentazione possono **osservare le dinamiche dello sviluppo tecnologico** e individuare gli **interventi normativi** più opportuni ed efficaci per agevolare lo sviluppo del *FinTech*, contenendo già in avvio la diffusione di potenziali rischi.

Per maggiori approfondimenti, si rinvia al relativo paragrafo del tema web *FinTech* pubblicato sul sito istituzionale della Camera dei deputati.

Il **comma 4 demanda** a un ulteriore **d.P.C.M.** la definizione delle modalità di **collaborazione e coordinamento tra la Sandbox-CRA e lo Spazio di sperimentazione italiano per l'IA** previsto dall'articolo 26 del decreto legislativo IA. Il comma specifica che tale decreto è adottato su

proposta dell'ACN, d'intesa con l'Agenzia per l'Italia digitale (**AgID**), sentiti, per i profili di rispettiva competenza, le **autorità del settore finanziario** (anche in questo caso identificate dalla relazione nella Banca d'Italia, nella Consob e nell'IVASS) e il **Garante per la protezione dei dati personali**.

Si segnala che l'AgID e l'ACN sono designate quali **Autorità nazionali per l'intelligenza artificiale** dall'articolo 20 della legge n. 132 del 2025.

Con riferimento allo **spazio di sperimentazione italiano per l'IA**, si ricorda che l'articolo 57 del regolamento (UE) 2024/1689 (*AI Act*) impone a ciascuno Stato membro di istituire almeno uno spazio di sperimentazione normativa per l'IA operativo entro il **2 agosto 2027**. Tali spazi sono configurati come ambienti controllati e temporalmente delimitati, finalizzati a promuovere l'innovazione, sostenere lo **sviluppo**, la **sperimentazione** e la **convalida** di **sistemi di IA**, nonché a favorire la certezza del diritto e l'**accesso** al **mercato**, in particolare per PMI e *start-up*.

L'articolo 26 del **decreto legislativo 7 ottobre 2026, n. 179** ha istituito lo **Spazio di sperimentazione italiano per l'intelligenza artificiale**, affidandone la vigilanza all'**AgID** e all'**ACN**. Lo strumento mira a favorire innovazione, competitività, cooperazione con le autorità competenti, **apprendimento normativo** e **accesso al mercato** europeo dei sistemi di IA, con priorità per le PMI e le *start-up*. L'articolo prevede, inoltre, che i **fornitori**, anche potenziali, possano sperimentare soluzioni innovative in un ambiente controllato, disciplinato da decreti congiunti di AgID e ACN. A decreti congiunti delle due Autorità è altresì rimandata la definizione delle **modalità di accesso, gestione, funzionamento, nonché i criteri di eleggibilità** per la **partecipazione** dei soggetti interessati allo Spazio di sperimentazione.

Per maggiori dettagli, si rimanda all'apposito *dossier* relativo al citato provvedimento.

Alla luce di quanto esposto, si valuti l'opportunità di specificare il riferimento normativo del "decreto legislativo IA", a cui il comma 4, ultimo periodo, rinvia.

CAPO VII – ULTERIORI MODIFICAZIONI E INTEGRAZIONI DELLA NORMATIVA DI SETTORE E DISPOSIZIONI DI COORDINAMENTO

Articolo 21
(Modifiche al decreto legislativo 12 ottobre 2022, n. 157)

L'**articolo 21** inserisce l'**Agenzia per la cybersicurezza nazionale** (ACN) nell'elenco delle autorità di vigilanza del mercato (**lett. a**), affida a specifico decreto del Presidente del Consiglio dei ministri la disciplina dei parametri per il calcolo dei costi delle attività di vigilanza della suddetta Agenzia effettuate in relazione ai prodotti risultati non conformi (**lett. b**) e regola le competenze delle autorità di vigilanza del mercato rispetto al regolamento europeo sui requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali (**lett. c**).

L'articolo 21 si compone di un solo comma e apporta tre modifiche testuali al decreto legislativo n. 157/2022 relativo al sistema di vigilanza del mercato (v. più avanti il *box* di approfondimento).

In particolare, la norma in commento mira a una razionalizzazione normativa che coinvolge, da un lato, il decreto legislativo n. 157 citato e, dall'altro, il decreto legislativo n. 179/2026, adottato al fine di adeguare la normativa nazionale alla disciplina del regolamento (UE) 2024/1689 – cd. AI Act – con particolare attenzione ai poteri delle Autorità nazionali e all'utilizzo dell'intelligenza artificiale nella formazione.

In proposito, occorre premettere che l'articolo 10 del decreto legislativo n. 179/2026:

- ha conferito all'Autorità per la cybersicurezza nazionale (ACN) **poteri di vigilanza del mercato** e sulla **conformità dei prodotti** di cui al regolamento (UE) 2019/1020**,** estendendo nei confronti dell'ACN la disciplina prevista nel decreto legislativo n. 157/2022, nei **limiti di compatibilità** con le disposizioni dell'AI ACT (comma 1) ;
- ha demandato a un **decreto** del Presidente del Consiglio dei ministri, da adottare entro **90 giorni** dalla data di entrata in vigore del decreto legislativo n. 179/2026 (avvenuta il 23 ottobre 2026), la determinazione dei **parametri** sulla base dei quali recuperare i **costi delle attività di vigilanza** effettuate dall'ACN nei confronti dei prodotti non conformi (comma 2).

• La vigilanza del mercato e la conformità dei prodotti: la disciplina del regolamento (UE) 2019/1020 e del decreto legislativo n. 157/2022

Il **decreto legislativo n. 157/2022** adegua la normativa nazionale alla disciplina europea sulla vigilanza del mercato e sulla conformità dei prodotti, di cui al regolamento (UE) 2019/1020. Il regolamento disciplina anche il monitoraggio, l'applicazione delle norme e i requisiti relativi alla sicurezza e la conformità dei prodotti, al fine di garantire che i prodotti immessi sul mercato unico rispettino la normativa europea e non rappresentino rischi per la salute, la sicurezza o l'ambiente.

Il regolamento si applica ai prodotti disciplinati dalla normativa di armonizzazione dell'Unione e a quelli importati nell'Unione Europea e non soggetti a una legislazione specifica. Per alcuni prodotti, prima dell'immissione sul mercato europeo deve esistere un operatore economico[8] stabilito nell'Unione. In capo agli operatori economici gravano una serie di obblighi, tra cui mantenere le dichiarazioni di conformità e di prestazione dell'Unione Europea, informare le autorità in presenza di un prodotto rischioso, cooperare con l'autorità ove richiesto nonché apporre alcune informazioni – come nomi e dati di contatto – sul prodotto, sull'imballaggio e sulla relativa documentazione.

Si aggiunge, inoltre, che le **autorità di vigilanza del mercato**, designate dagli Stati membri, svolgono un'attività di sorveglianza, di controllo, di indagine, prescrittiva e sanzionatoria nei confronti dei prodotti e degli operatori economici.

Per ulteriori approfondimenti sul contenuto del regolamento, si veda l'apposita pagina di eur-lex.

L'Italia ha adottato il decreto legislativo n. 157 del 2022 al fine di uniformare il proprio quadro normativo a quello unionale. Si rammenta che, mediante tale decreto, il Governo ha dato attuazione alla delega di cui all'**articolo 30** della legge n. 118 del 2022 (legge annuale per il mercato e la concorrenza 2021).

Per i profili di interesse in questa sede, il citato decreto legislativo n. 157 del 2022 individua le **autorità di vigilanza del mercato (articolo 3)**, esse sono: il Ministero delle imprese e del *made in Italy*; il Ministero della salute; il Ministero del lavoro; il Ministero dell'interno, il Ministero dell'ambiente e della sicurezza energetica; il Ministero delle infrastrutture e dei trasporti; il Ministero dell'agricoltura, della sovranità alimentare e delle foreste e l'Ente nazionale per l'aviazione civile. Gli ambiti di competenza di tali autorità sono disciplinati dagli **allegati I-VIII** al decreto legislativo.

Inoltre, l'articolo 10 del decreto legislativo disciplina il **recupero dei costi delle attività di vigilanza**, attribuendo alle autorità il compito di rivalersi, nei confronti dell'operatore interessato, per le spese sostenute per le attività svolte verso i prodotti risultati non conformi. In tali costi rientrano quelli necessari per la realizzazione di prove, per l'adozione di misure relative al divieto di immissione nel mercato di un prodotto, di magazzinaggio e delle attività inerenti ai prodotti risultati non conformi e oggetto di misure correttive prima della loro immissione sul mercato.

8 Con il termine operatore economico si intendono il fabbricante, il rappresentante autorizzato, l'importatore o il distributore, nonché il prestatore di servizi di logistica.

Come anticipato nel *box* di approfondimento, l'articolo 3, comma 1, del decreto legislativo n. 157 del 2022 individua le autorità di vigilanza del mercato (e i rispettivi ambiti di competenza, disciplinati dagli allegati I-VIII al decreto legislativo), tra le quali, a seguito della modifica apportata dall'articolo 21, comma 1, **lett. a)**, in commento, occorre considerare anche **l'Autorità per la cybersicurezza nazionale** (nuova lettera **h-*bis*)** dell'articolo 3, comma 1 del decreto legislativo n. 157 del 2022).

Come sottolineato dalla relazione illustrativa allegata al provvedimento in esame, tale integrazione è disposta al fine di adeguare l'ordinamento nazionale alla modifica apportata dall'articolo 66 del regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio (c.d. CRA), relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali. Il citato articolo 66 ha difatti inserito il CRA nell' allegato I del reg. 2019/1020, che elenca la normativa di armonizzazione dell'Unione.

L'articolo 21, comma 1, **lett. b),** si sofferma sulla disciplina dei **parametri** sulla base dei quali recuperare i **costi delle attività di vigilanza** effettuate dall'ACN nei confronti dei prodotti non conformi.

Tale disciplina viene demandata ad apposito decreto del Presidente del Consiglio dei ministri, da adottarsi su proposta dell'ACN, di concerto con il Ministro dell'economia e delle finanze, entro novanta giorni dalla data di entrata in vigore del decreto legislativo n. 179/2026, avvenuta il 23 ottobre 2026. Si è già avuto modo di anticipare che tale decreto è previsto dall'articolo 10, comma 2, del decreto legislativo n. 179/2026.

Sul piano testuale, la novità è introdotta mediante l'aggiunta del comma 3-*bis* all'articolo 10 del decreto legislativo n. 157/2022, che disciplina infatti il **rimborso** a carico dell'operatore interessato dei **costi derivanti dalle attività di vigilanza** effettuate in relazione ai prodotti risultati non conformi.

Si osservi che l'articolo 10, comma 3, del citato decreto legislativo n. 157/2022 già demandava a un decreto del **MIMIT**, da adottarsi, di concerto con il MEF e le autorità di vigilanza, entro **sessanta giorni** dall'entrata in vigore del decreto legislativo, la determinazione dei parametri per il calcolo dei costi delle attività di vigilanza effettuate in relazione ai prodotti risultati non conformi. Alla data di pubblicazione del presente *dossier,* come confermato anche dalla banca dati del Dipartimento per il programma di Governo della Presidenza del Consiglio dei Ministri, tale decreto non risulta essere stato adottato.

Rimanendo nel sistema di vigilanza del mercato delineato dal citato articolo 3 comma 1, del decreto legislativo n. 157 del 2022, si aggiunge che l'articolo 21, al comma 1, **lett. c)**, interviene sugli ambiti di competenza

dell'ACN, introducendo tre allegati (**VIII-*bis,* VIII-*ter,* VIII-*quater,*** consultabili in calce al presente provvedimento, che regolano le competenze tra le Autorità di vigilanza del mercato) dopo l'allegato VIII del d.lgs. n. 157/2022.

In tale decreto legislativo gli allegati indicano, per ciascuna autorità, la normativa di cui l'autorità controlla il rispetto e le altre amministrazioni con cui condivide la competenza. I nuovi allegati svolgono questa funzione per il regolamento sulla ciberresilienza (CRA).

La regola generale è che la vigilanza spetta all'ACN (per un approfondimento in merito, si rimanda alla scheda di lettura dell'articolo 9 del presente provvedimento). Un'eccezione è rappresentata dall'articolo 52, par. 14, del CRA, secondo cui, per i prodotti con elementi digitali che sono classificati come sistemi di intelligenza artificiale ad alto rischio le autorità responsabili delle attività di vigilanza del mercato sono le medesime autorità di vigilanza del mercato designate ai fini dell'*AI Act.* Si tratta, in Italia, dell'ACN, di **Banca d'Italia**, della **CONSOB**, dell'**IVASS** e del **Garante per la protezione dei dati personali.**

Articolo 22
(Funzioni dell'Agenzia per la cybersicurezza nazionale)

L'**articolo 22** designa l'**Agenzia per la cybersicurezza nazionale** (ACN) quale **autorità di notifica** e **autorità di vigilanza del mercato** ai sensi del regolamento (UE) 2024/2847 e le attribuisce, a tal fine, tutte le funzioni previste dal medesimo regolamento.

Il **comma 1** novella l'articolo 7, comma 1, del decreto-legge n. 82 del 2021, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale, introducendovi la lettera *aa-bis)* con cui viene individuata l'**agenzia per la Cybersicurezza Nazionale (ACN)** quale **autorità di notifica** e **autorità di vigilanza del mercato** ai sensi, rispettivamente, degli articoli 36 e 52 del regolamento (UE) 2024/2847.

In particolare, l'articolo 36 del regolamento disciplina le funzioni dell'autorità di notifica, cui compete istituire e attuare le procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità, nonché per il loro controllo, anche con riferimento agli obblighi previsti dall'articolo 41. La disposizione consente inoltre agli Stati membri di affidare le attività di valutazione e controllo a un organismo nazionale di accreditamento, ai sensi e in conformità del regolamento (CE) n. 765/2008. Qualora, invece, l'autorità di notifica deleghi o affidi ad altro organismo, non avente natura di ente pubblico, le attività di valutazione, notifica o controllo, tale organismo deve essere dotato di personalità giuridica, rispettare, *mutatis mutandis*, i requisiti previsti dall'articolo 37 e predisporre misure idonee a coprire le responsabilità derivanti dalle proprie attività. Resta in ogni caso ferma la piena responsabilità dell'autorità di notifica per i compiti svolti dall'organismo incaricato.

Con riferimento alla funzione di autorità di vigilanza del mercato, l'articolo 52 del regolamento (UE) 2024/2847 prevede che gli Stati membri designino una o più autorità competenti, anche individuandole tra quelle già esistenti, al fine di garantirne l'efficace attuazione. Alle autorità designate sono attribuite le attività di vigilanza del mercato relative ai prodotti con elementi digitali rientranti nell'ambito di applicazione del regolamento, comprese quelle concernenti il rispetto degli obblighi previsti per i gestori di *software open source*. In caso di inosservanza di tali obblighi, le autorità richiedono l'adozione delle opportune misure correttive. L'articolo disciplina inoltre la cooperazione e lo scambio di informazioni con le autorità nazionali di certificazione della cibersicurezza, i gruppi di risposta agli incidenti di sicurezza informatica (CSIRT), l'Agenzia dell'Unione europea per la cibersicurezza (ENISA), le autorità competenti in materia di protezione dei dati personali e le altre autorità di vigilanza del mercato

interessate. È altresì previsto che gli Stati membri assicurino alle autorità designate adeguate risorse finanziarie, tecniche e umane. Le medesime autorità possono fornire orientamenti e consulenza agli operatori economici e sono tenute a informare i consumatori sulle modalità di presentazione dei reclami e di accesso ai meccanismi di segnalazione delle vulnerabilità, degli incidenti e delle minacce informatiche che possono interessare i prodotti con elementi digitali. Esse riferiscono annualmente alla Commissione europea sui risultati delle pertinenti attività di vigilanza e comunicano senza indugio alla Commissione e alle pertinenti autorità nazionali garanti della concorrenza le informazioni potenzialmente rilevanti ai fini dell'applicazione del diritto dell'Unione in materia di concorrenza. Sono infine previsti specifici meccanismi di cooperazione amministrativa, anche attraverso l'istituzione di un apposito gruppo di cooperazione (ADCO), nonché forme di coordinamento con le autorità designate ai sensi del regolamento (UE) 2024/1689 per i prodotti con elementi digitali classificati come sistemi di intelligenza artificiale ad alto rischio. Per tali prodotti, il regolamento individua nelle autorità designate ai sensi dell'AI Act le autorità responsabili delle attività di vigilanza del mercato previste dal regolamento sulla ciberresilienza, prevedendo la cooperazione e lo scambio di informazioni con le altre autorità competenti, i CSIRT designati come coordinatori e l'ENISA.

Si ricorda, peraltro, che l'articolo 2, comma 2, lettera *l*) dello schema di decreto in esame precisa che sono autorità di vigilanza del mercato, oltre all'Agenzia per la cybersicurezza nazionale, anche la Banca d'Italia, la Commissione nazionale per la società e la borsa (CONSOB), l'Istituto per la vigilanza sulle assicurazioni (IVASS) e il Garante per la protezione dei dati personali.

Articolo 23
(Modifiche al codice del consumo, di cui al decreto legislativo 6 settembre 2005, n. 206)

L'**articolo 23** aggiunge il **regolamento europeo sulla ciberresilienza** all'elenco delle disposizioni in allegato al codice del consumo la cui violazione può dare luogo a un'azione per la **tutela degli interessi collettivi** dei consumatori.

L'articolo 23 agisce sull'**allegato II-*septies*** del decreto legislativo n. 206/2005 (c.d. codice del consumo), che contiene un elenco di normative di rilievo per i consumatori. Tale allegato è richiamato principalmente dall'articolo 140-*ter* del codice, che reca le definizioni e l'ambito di applicazione inerenti alle azioni rappresentative a tutela degli interessi dei consumatori.

In particolare, in presenza di violazione di una delle disposizioni raccolte nell'allegato II-*septies*, l'ente legittimato ha facoltà di promuovere un'azione rappresentativa, nazionale o transfrontaliera, per la **tutela degli interessi collettivi** dei consumatori e finalizzata a ottenere un provvedimento **inibitorio** o **compensativo**.

La legittimazione a promuovere tali azioni è riconosciuta alle **associazioni dei consumatori e degli utenti** iscritte nell'elenco tenuto dal Ministero delle imprese e del *made in Italy*, agli **organismi pubblici** indipendenti nazionali responsabili dell'applicazione delle norme dell'Unione sulla tutela degli interessi dei consumatori, nonché agli **enti designati dagli altri Stati membri** e inseriti nell'apposito elenco redatto dalla Commissione europea. Le associazioni iscritte nell'elenco ministeriale possono chiedere l'iscrizione nell'**elenco della Commissione,** così da poter proporre anche **azioni rappresentative transfrontaliere**; a tal fine devono rispettare requisiti volti a garantirne l'indipendenza e la trasparenza, ad accertare che lo scopo statutario e l'attività pubblica consistano nella tutela degli interessi dei consumatori e a escludere le associazioni assoggettate a procedure per la regolazione dell'insolvenza.

Ciò premesso, l'articolo 23 dello schema di decreto in commento aggiunge il regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali, nel novero di queste disposizioni (per un approfondimento sul regolamento, si rimanda alla scheda di lettura dell'articolo 1 del presente dossier).

Sul piano pratico ne consegue che anche la violazione della disciplina del regolamento europeo sulla ciberresilienza da parte di professionisti[9] può dare luogo ad azioni rappresentative promosse per conto dei consumatori.

9 L'articolo 140-*ter*, comma 1, lett. b), definisce professionista "qualsiasi persona fisica o giuridica che, indipendentemente dal fatto che si tratti di un soggetto pubblico o privato, agisce, anche tramite un altro soggetto che opera in suo nome o per suo conto, per fini relativi alla propria attività commerciale, imprenditoriale, artigianale o professionale".

CAPO VIII – DISPOSIZIONI TRANSITORIE, FINANZIARIE E FINALI

Articolo 24
(Attuazione da parte dell'Agenzia per la cybersicurezza nazionale degli obblighi di cui al decreto legislativo 12 ottobre 2022, n. 157)

L'**articolo 24** stabilisce che l'ACN, in quanto autorità di vigilanza del mercato, pubblichi sul proprio sito le informazioni relative ai prodotti, alle procedure e alle normative applicabili (**comma 1**) e individui i laboratori di prova di cui avvalersi (**comma 2**).

L'articolo 24 si compone di due commi.

Il **comma 1** prevede che l'ACN pubblichi sul proprio sito internet istituzionale le informazioni di cui all'articolo 3, comma 4, del decreto legislativo n. 157/2022, entro novanta giorni dalla data di entrata in vigore del decreto. Tale disposizione prevede che i siti delle autorità di vigilanza del mercato forniscano agli operatori economici e agli utilizzatori finali, senza ulteriori oneri e in un'apposita sezione facilmente individuabile, l'accesso alle **informazioni** relative ai prodotti, alle procedure e alle normative applicabili.

Il **comma 2** prevede che l'ACN, con decreto del direttore generale, proceda alla ricognizione e all'individuazione dei **laboratori di prova**, ai sensi dell'articolo 8 del decreto legislativo n. 157/2022. Si osserva che per la ricognizione e per l'individuazione non è fissato un termine.

L'articolo 8 del d.lgs. n. 157/2022 prevede che ciascuna autorità di vigilanza effettui la ricognizione degli impianti e dei laboratori di prova esistenti e accreditati, cioè riconosciuti competenti dall'organismo nazionale di accreditamento ai sensi del regolamento (CE) n. 765/2008. In base alle risultanze, l'autorità individua ulteriori laboratori per le prove non svolte da quelli esistenti. I termini previsti dall'articolo 8 (trenta giorni dall'entrata in vigore del decreto e, per l'individuazione, il 31 dicembre 2022) riguardavano la prima attuazione del d.lgs. n. 157/2022. I laboratori svolgono le prove richieste dalle autorità di vigilanza mediante prove fisiche e accertamenti tecnici, anche con strumenti digitali, su campioni di prodotti, compresi quelli venduti *online*.

Articolo 25
(Abrogazioni)

L'**articolo 25** dispone l'**abrogazione**, a decorrere dall'**11 dicembre 2027**, delle misure relative ai **requisiti essenziali** delle **apparecchiature radio** in materia di protezione delle reti, tutela dei dati personali e della vita privata e prevenzione delle frodi, contenute nel decreto legislativo di attuazione della direttiva europea sulla messa a disposizione sul mercato di apparecchiature radio.

Nel dettaglio, l'**articolo 25** dispone l'**abrogazione,** a decorrere dall'**11 dicembre 2027**, delle lettere *d)*, *e)* e *f)* dell'articolo 3, comma 3, del decreto legislativo n. 128 del 2016, recante l'attuazione della direttiva 2014/53/UE concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE.

Pertanto, la disposizione in rassegna elimina dal novero dei **requisiti essenziali**, ai quali deve conformarsi la **fabbricazione delle apparecchiature radio** di determinate categorie o classi, i seguenti:

- non danneggiare la **rete o il suo funzionamento**, né abusare delle risorse della rete arrecando quindi un deterioramento inaccettabile del servizio (lett. *d)* del citato d.lgs.);
- contenere elementi di salvaguardia per garantire la **protezione dei dati personali** e della **vita privata** dell'utente e dell'abbonato (lett. *e)* del citato d.lgs.);
- supportare **caratteristiche speciali** che consentano di tutelarsi dalle frodi (lett. *f)* del citato d.lgs.).

Come riportato dall'analisi tecnico-normativa del provvedimento in esame, tale abrogazione è finalizzata ad adeguare l'ordinamento nazionale al regolamento delegato (UE) 2026/339, che dispone l'abrogazione, a decorrere dall'11 dicembre 2027, del regolamento delegato (UE) 2022/30, al quale rinviano le lettere d), e) e f) dell'articolo 3, comma 3, del decreto legislativo n. 128 del 2016.

Per una maggiore evidenza grafica delle modifiche apportate dalla novella in commento, si rimanda al seguente **testo a fronte**.

Attuazione della direttiva 2014/53/UE concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE. (D.Lgs. 128/2016)	
Testo previgente	**Modificazioni apportate dall'art. 25 del A.G. 447 (a decorrere dall'11/12/27)**
Art. 3 *(Requisiti essenziali)*	Art. 3 *(idem)*
1. Le apparecchiature radio sono fabbricate in modo da garantire: a) a protezione della salute e della sicurezza di persone e di animali domestici e beni, compresi gli obiettivi riguardanti i requisiti di sicurezza previsti dalla direttiva 2014/35/UE e la relativa normativa di attuazione, ma senza applicazione di limiti minimi di tensione; b) un adeguato livello di compatibilità elettromagnetica ai sensi della direttiva 2014/30/UE e la relativa normativa di attuazione.	*Identico*
2 Le apparecchiature radio sono fabbricate in modo da utilizzare efficacemente lo spettro radio e supportare l'uso efficiente dello spettro radio stesso al fine di evitare interferenze dannose.	*Identico*
3. Le apparecchiature radio di determinate categorie o classi sono fabbricate in modo tale da garantire la conformità ai seguenti requisiti essenziali: a) interagire con accessori diversi dai dispositivi di ricarica per le categorie o le classi di apparecchiature radio di cui all'allegato I *bis*, parte I, che sono specificamente menzionati al comma 4-bis del presente articolo;	3. Le apparecchiature radio di determinate categorie o classi sono fabbricate in modo tale da garantire la conformità ai seguenti requisiti essenziali: a) interagire con accessori diversi dai dispositivi di ricarica per le categorie o le classi di apparecchiature radio di cui all'allegato I *bis*, parte I, che sono specificamente menzionati al comma 4-*bis* del presente articolo;

Attuazione della direttiva 2014/53/UE concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE. (D.Lgs. 128/2016)	
Testo previgente	**Modificazioni apportate dall'art. 25 del A.G. 447 (a decorrere dall'11/12/27)**
b) interagire con altre apparecchiature radio via rete; c) poter essere collegate a interfacce del corrispondente tipo in tutta l'Unione; **d) non danneggiare la rete o il suo funzionamento, né abusare delle risorse della rete arrecando quindi un deterioramento inaccettabile del servizio;** **e) contenere elementi di salvaguardia per garantire la protezione dei dati personali e della vita privata dell'utente e dell'abbonato;** **f) supportare caratteristiche speciali che consentano di tutelarsi dalle frodi;** g) supportare caratteristiche speciali che consentano l'accesso ai servizi d'emergenza; h) supportare caratteristiche speciali che facilitino il loro uso da parte di utenti disabili; i) supportare caratteristiche speciali che garantiscano che sia caricato un software nell'apparecchiatura radio, soltanto se è stata dimostrata la conformità della combinazione dell'apparecchiatura radio e del *software*.	b) interagire con altre apparecchiature radio via rete; c) poter essere collegate a interfacce del corrispondente tipo in tutta l'Unione; g) supportare caratteristiche speciali che consentano l'accesso ai servizi d'emergenza; h) supportare caratteristiche speciali che facilitino il loro uso da parte di utenti disabili; i) supportare caratteristiche speciali che garantiscano che sia caricato un software nell'apparecchiatura radio, soltanto se è stata dimostrata la conformità della combinazione dell'apparecchiatura radio e del *software*.
4. Il Ministero attua, conformemente alla normativa vigente, gli atti delegati, adottati dalla Commissione europea che specificano a quali categorie o classi di apparecchiature radio si applicano ciascuno dei requisiti di cui al precedente comma, lettere da a) ad i). Il Ministero attua altresì, conformemente	*Identico*

Attuazione della direttiva 2014/53/UE concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE. (D.Lgs. 128/2016)	
Testo previgente	**Modificazioni apportate dall'art. 25 del A.G. 447 (a decorrere dall'11/12/27)**
alla normativa vigente, gli atti delegati adottati dalla Commissione europea che modificano la parte I dell'allegato I *bis* alla luce del progresso scientifico e tecnologico o degli sviluppi del mercato per garantire un'interoperabilità minima comune tra le apparecchiature radio e i relativi dispositivi di ricarica, nonché migliorare la convenienza dei consumatori, ridurre i rifiuti ambientali ed evitare la frammentazione del mercato, per quanto riguarda sia le apparecchiature radio che possono essere ricaricate mediante cavo sia le apparecchiature radio che possono essere ricaricate tramite mezzi diversi dal cavo.	
4-*bis.* Le apparecchiature radio che rientrano nelle categorie o nelle classi di cui all'allegato I *bis*, parte I, sono costruite in modo da essere conformi alle specifiche relative alle capacità di ricarica di cui a tale allegato per la pertinente categoria o classe di apparecchiature radio.	*Identico*

Articolo 26, commi 1-3
(Disposizioni finanziarie)

L'**articolo 26, ai commi da 1 a 3**, reca la **quantificazione degli oneri** derivanti dall'attuazione delle disposizioni di cui agli articoli 9, comma1, 10, comma 1, 17 e 20, individuando altresì le **fonti di copertura finanziaria**; destina una quota delle risorse all'incremento della dotazione organica di livello non dirigenziale; reca la clausola di invarianza finanziaria relativamente alle rimanenti disposizioni.

Nel dettaglio, l'**articolo 1 autorizza la spesa per l'attuazione** delle disposizioni di cui agli articoli 9, comma 1 (che individua l'Agenzia per la cybersicurezza nazionale quale autorità di vigilanza del mercato), 10, comma 1 (che attribuisce all'Agenzia i poteri di vigilanza del mercato nonché di adeguamento della normativa nazionale alle disposizioni del rilevante regolamento (UE)), 17 (riguardante il terminale per le segnalazioni al CSIRT Italia) e 20 (che disciplina la promozione dell'innovazione e il coordinamento con gli altri spazi di sperimentazione) del presente decreto.

In particolare, è autorizzata la spesa di euro:

- 2.100.000 per l'anno 2026,
- 5.875.000 per il 2027
- 9.125.000 il 2028 e
- 6.925.000 annui a decorrere dall'anno 2029.

A tali spese si provvede mediante corrispondente riduzione dell'autorizzazione di spesa di cui all'articolo 15, comma 3, della legge di delegazione europea 2025 (legge n. 36 del 2026).

Il citato articolo 15 della legge di delegazione europea 2025 reca la delega legislativa per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, in materia di requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali. Il comma 3, in particolare, quantifica le risorse necessarie per far fronte all'attuazione della delega nello stesso ammontare indicato per il comma 1 in esame, e cioè in euro 2.100.000 per il 2026, 5.875.000 per il 2027, 9.125.000 per il 2028 e 6.925.000 annui a decorrere dal 2029. A tal fine viene ridotto in maniera corrispondente il **fondo per il recepimento della normativa europea** (articolo 41-bis della legge n. 234/2012).

Il **comma 2** precisa che quota parte delle risorse di cui al comma 1, quantificata in euro:

- 900.000 per l'anno 2026,
- 2.700.000 per il 2027 e
- 5.850.000 annui a decorrere dall'anno 2028

fermo restando quanto previsto dall'articolo 12, comma 5, del decreto-legge n. 82 del 2021, convertito, con modificazioni, dalla legge n. 109 del 2021, è volta a **incrementare la dotazione organica** del personale di livello non dirigenziale dell'Agenzia.

Il citato articolo 12, comma 5, del decreto-legge n. 82 del 2021 (recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale) stabilisce che, fermo restando l'adeguamento della dotazione organica di livello dirigenziale generale e non generale di cui all'articolo 6, comma 1-*bis*, e le relative decorrenze, la rimanente dotazione organica è progressivamente rideterminata, in linea con il processo di crescita della capacità operativa dell'Agenzia, con decreti del Presidente del Consiglio dei ministri di concerto con il Ministro dell'economia e delle finanze, nei limiti delle risorse finanziarie destinate al personale di cui all'articolo 18, comma 1. Dei provvedimenti adottati in materia di dotazione organica è data tempestiva e motivata comunicazione alle Commissioni parlamentari competenti e al COPASIR.

In attuazione di quanto disposto da tale lettera b), è stato emanato il D.P.C.M. 24 luglio 2024 recante ripartizione del Fondo per l'attuazione della Strategia nazionale di cybersicurezza e del fondo per la gestione della cybersicurezza, su proposta dell'Agenzia per la cybersicurezza nazionale.

Il **comma 3**, infine, reca la **clausola di invarianza finanziaria** relativamente a tutte le disposizioni a eccezione di quanto previsto dal comma 1. In particolare, le amministrazioni interessate provvedono agli adempimenti previsti dal presente decreto con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri a carico della finanza pubblica.

Articolo 26, comma 4
(Personale dell'Agenzia per la cybersicurezza nazionale)

L'**articolo 26, comma 4**, interviene sulla disciplina del personale dell'**Agenzia per la cybersicurezza nazionale** (**ACN**), ampliando le fattispecie che consentono la **cessazione del rapporto di lavoro o di servizio presso l'Agenzia**, con conseguente **ricollocazione** presso altre amministrazioni, del personale appartenente ai segmenti professionali di **direttore centrale** e di **direttore**. La disposizione prevede, altresì, l'**incremento** delle risorse del **fondo destinato a finanziare la ricollocazione** del personale interessato.

La disposizione in esame modifica il decreto legge n. 25 del 2025, recante disposizioni urgenti in materia di reclutamento e funzionalità delle pubbliche amministrazioni, intervenendo, in particolare, sull'articolo 12-*quinquies*, concernente il personale dell'Agenzia per la cybersicurezza nazionale".

Si ricorda che l'**articolo 12-*quinquies* del decreto-legge n. 25 del 2025**, al comma 1, ha incrementato le risorse per il funzionamento dell'Agenzia per la cybersicurezza nazionale (ACN) di 1 milione di euro per l'anno 2025, di 4 milioni di euro per l'anno 2026 e di 5 milioni di euro annui a decorrere dall'anno 2027, provvedendo, al comma 2, alla copertura dei relativi oneri. Per il personale appartenente ai segmenti professionali di direttore centrale e direttore che abbia tenuto comportamenti che determinino un grave pregiudizio per la sicurezza nazionale nello spazio cibernetico, il comma 3 prevede la cessazione del rapporto di lavoro con l'ACN. La cessazione comporta, per il personale di ruolo, la ricollocazione presso il ministero di originaria appartenenza, ovvero, nei restanti casi, presso la Presidenza del Consiglio. Il comma 4 rinvia, a fini dell'applicazione delle previsioni di cui al comma precedente, alle disposizioni, per quanto compatibili, in materia di destituzione per motivi disciplinari, recate dal regolamento del personale dell'ACN. Il comma 5 istituisce un fondo per finanziare la ricollocazione del personale.

La **lettera *a)*** della disposizione in commento introduce un nuovo comma 3-*bis* nel *corpus* dell'articolo 12-*quinquies*, **ampliando le fattispecie** che possono determinare la **cessazione del rapporto di lavoro o di servizio presso l'Agenzia**, con conseguente ricollocazione del personale appartenente ai segmenti professionali di direttore centrale e di direttore.

In particolare, la ricollocazione, nel **limite di due unità** per la qualifica di direttore centrale e di **una unità** per la qualifica di direttore, è possibile anche in relazione a:

- processi di riorganizzazione;
- processi funzionali al più efficiente assolvimento delle funzioni dell'Agenzia a tutela della cybersicurezza.

In tal senso, la norma richiama le competenze e le attività attribuite dalla legge n. 132 del 2025. Si segnala, in proposito, l'attribuzione all'Agenzia per la cybersicurezza nazionale (ACN) del compito di promuovere e sviluppare ogni iniziativa finalizzata a valorizzare l'intelligenza artificiale come risorsa per il rafforzamento della cybersicurezza nazionale (articolo 18 della legge n. 132 del 2025).

Secondo quanto precisato dalla disposizione in commento, la ricollocazione è assicurata con le **medesime modalità individuate dal comma 3** dell'articolo 12-*quinquies*, senza ricorrere, tuttavia, alle facoltà assunzionali delle amministrazioni destinatarie e con **salvaguardia della posizione giuridica e del trattamento economico** avente natura fissa e continuativa.

Si ricorda che l'appena richiamato comma 3 prevede, al primo periodo, che – per il personale appartenente ai segmenti professionali di direttore centrale e direttore dell'ACN che abbia tenuto comportamenti che determinino un grave pregiudizio per la sicurezza nazionale nello spazio cibernetico – è disposta la cessazione del rapporto di lavoro o di servizio con la medesima Agenzia, anche in assenza di profili di responsabilità disciplinare. Si stabilisce, conseguentemente, al secondo periodo, la ricollocazione, del personale di ruolo per il quale è stata disposta la cessazione dal servizio, anche in sovrannumero, presso il ministero di originaria appartenenza, ovvero presso la Presidenza del Consiglio, nei restanti casi, con la salvaguardia della sola posizione giuridica maturata presso l'ACN. Si specifica, al terzo periodo, che è esclusa la ricollocazione presso il contingente speciale del personale addetto al DIS e ai servizi di informazione per la sicurezza, istituito presso la Presidenza del Consiglio dei ministri e nei ruoli delle Forze armate e delle Forze di polizia. Al quarto periodo, quindi, si prevede che la ricollocazione sia effettuata a valere delle facoltà assunzionali delle amministrazioni di destinazione e sulle risorse disponibili del Fondo istituito dal comma 5 dello stesso articolo (v. *infra*).

Viene quindi prevista la ricollocazione del personale interessato dal nuovo comma 3-*bis*, anche in sovrannumero, con salvaguardia della posizione giuridica e, a differenza del citato comma 3, **anche del trattamento economico** avente natura fissa e continuativa, presso il **Ministero di originaria appartenenza**, ovvero, nei restanti casi, presso la **Presidenza del Consiglio**. È **esclusa**, come previsto dal citato comma 3, la ricollocazione presso il **contingente speciale del personale addetto al DIS e ai servizi di informazione per la sicurezza**, istituito presso la Presidenza

del Consiglio dei ministri e nei ruoli delle Forze armate e delle Forze di polizia. La ricollocazione è effettuata a valere sulle risorse di cui al comma 5 (su cui *v. infra*).

Per quanto riguarda l'ambito soggettivo di applicazione della disposizione in commento, si evidenzia che il personale di ruolo dell'ACN è inquadrato nell'Area manageriale e alte professionalità e nell'Area operativa (DPCM 9 dicembre 2021, n. 224, art. 2).

Nell'Area manageriale e alte professionalità sono previsti i seguenti segmenti professionali:

- Direttore centrale (*Principal director*);
- Direttore (*Director*);
- Consigliere (*Advisor*);
- Esperto (*Expert*).

I segmenti di Direttore centrale e Direttore, sui quali interviene il comma in commento, corrispondono al livello dirigenziale, rispettivamente, generale e non generale.

Le **assunzioni** sono disposte, mediante pubblico concorso, per l'Area manageriale e alte professionalità nei segmenti professionali di Esperto e Consigliere (DPCM 224/2021, art. 8, comma 1). I passaggi al segmento professionale di Direttore centrale sono disposti a scelta per merito dal Direttore generale sulla base della valutazione dell'attività lavorativa del dipendente, effettuata secondo modalità e criteri predeterminati dal Direttore generale (DPCM 224/2021, art. 57, comma 2); i passaggi ai segmenti professionali di Direttore e di Consigliere sono disposti dal Direttore generale, sulla base dell'istruttoria e delle proposte effettuate da un Comitato, presieduto dal Vice Direttore generale e composto dai Capi dei Servizi (DPCM 224/2021, art. 58, comma 2).

La dotazione organica delle posizioni di livello generale (segmento direttore centrale) di livello non generale (segmento direttore) è fissata, rispettivamente, in 12 e 40 unità (DPCM 29 settembre 2025, che ha rideterminato la dotazione organica complessiva dell'ACN in 669 unità a decorrere dall'anno 2026).

La **lettera *b)*** interviene sul comma 5 dell'articolo 12-*quinquies* del decreto-legge n. 25 del 2025, **estendendo l'utilizzo del fondo** ivi previsto **anche alle ricollocazioni** disciplinate dal nuovo comma 3-*bis* e rideterminandone la dotazione finanziaria (v. *supra*).

La dotazione del fondo, istituito nello stato di previsione del Ministero dell'economia e delle finanze, resta fissata in 280 mila euro per ciascuno degli anni 2025 e 2026 ed è elevata a 1,5 milioni di euro annui a decorrere dal 2027. I maggiori oneri derivanti dalla disposizione, pari a 1,22 milioni di euro annui a decorrere dal 2027, trovano copertura mediante corrispondente riduzione del Fondo di cui all'articolo 1, comma 200, della legge n. 190 del 2014.

Si ricorda che il suddetto Fondo, istituito nello stato di previsione del Ministero dell'economia e delle finanze per far fronte a esigenze indifferibili che si manifestano nel corso della gestione, è ripartito annualmente con uno o più decreti del Presidente del Consiglio dei ministri, su proposta del Ministro dell'economia e delle finanze.

Articolo 27
(Protezione dei dati e riservatezza)

L'**articolo 27** prescrive il **rispetto** della **normativa** posta a tutela della **protezione dei dati personali** con riferimento alle attività di coordinamento operativo e informativo, nonché di scambio delle informazioni poste in essere dalle diverse autorità coinvolte nella regolazione e nella vigilanza del rispetto dei requisiti essenziali di cybersicurezza imposti ai prodotti con elementi digitali immessi sul mercato.

L'**articolo 27** chiarisce che le diverse attività di **coordinamento operativo** e **informativo** tra le istituzioni e autorità coinvolte, nonché gli **scambi di informazioni** regolati da appositi accordi e protocolli d'intesa, previsti dal provvedimento in esame, avvengono, anche in deroga all'obbligo del segreto d'ufficio, in **conformità** alla **normativa** posta a garanzia della **protezione dei dati personali**, nonché nel rispetto dei **principi** di **necessità**, **proporzionalità** e **minimizzazione**.

Si ricorda che i principi di minimizzazione, necessità e proporzionalità risultano essere fondamentali per garantire un trattamento dei dati lecito, corretto e conforme alla disciplina dettata dal GDPR (Reg. UE 2016/679) e dalle altre fonti normative poste a tutela della protezione dei dati personali.

Nello specifico, il principio di "**minimizzazione dei dati**" impone che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (cfr. art. 5, par. 1, *lett. c)* del GDPR).

In merito al principio di "**necessità del trattamento**" il Considerando n. 40 del GDPR chiarisce che affinché il trattamento dei dati personali possa considerarsi lecito, esso si deve fondare sul consenso dell'interessato ovvero su altra base giuridica legittima, tenuto conto della necessità di ottemperare all'obbligo legale al quale il titolare del trattamento è soggetto o della necessità di esecuzione di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali adottate su richiesta dello stesso. Peraltro, l'art. 6 ("liceità del trattamento") del GDPR enuclea le ipotesi in cui il trattamento è da considerarsi lecito in quanto necessario per perseguire determinate finalità o assolvere a specifici obblighi di legge. Allo stesso modo, il requisito della necessità è richiesto quando occorre trattare categorie particolari di dati personali ai sensi del successivo art. 9.

Con riferimento, invece, al principio di "**proporzionalità del trattamento**", il Considerando n. 4 stabilisce che il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il principio di proporzionalità è, poi, richiamato sia

nelle disposizioni in materia di liceità del trattamento di cui all'art. 6, sia nelle norme che regolano il trattamento di categorie particolari di dati personali di cui all'art. 9.

La relazione illustrativa riporta che la disposizione in esame è volta a consentire un efficace scambio informativo tra le diverse autorità citate nel provvedimento in esame, con particolare riferimento a quelle coinvolte nell'attività di vigilanza del mercato.

Con riferimento al rispetto della riservatezza dei dati da parte delle autorità coinvolte nelle attività di vigilanza, il **Regolamento UE 2024/2847** al **considerando n. 119**, prevede che al fine di garantire una cooperazione fiduciosa e costruttiva tra le autorità di vigilanza del mercato a livello nazionale e dell'Unione, è opportuno che tutte le parti coinvolte nell'applicazione del predetto regolamento rispettino la riservatezza delle informazioni e dei dati ottenuti nello svolgimento dei loro compiti.

In attuazione di quanto appena riportato, l'**art. 63 del Regolamento** dispone puntualmente che tutte le parti che prendono parte all'applicazione delle prescrizioni contenute nel provvedimento europeo sono tenute a rispettare a riservatezza delle informazioni e dei dati ottenuti nello svolgimento dei loro compiti e delle loro attività in modo da tutelare, con particolare riferimento:

- ai diritti di proprietà intellettuale e le informazioni commerciali riservate o i segreti commerciali di una persona fisica o giuridica (*lett. a)*);
- all'efficace attuazione del Regolamento, in particolare per quanto riguarda ispezioni, indagini o audit (*lett. b)*);
- agli interessi di sicurezza pubblica e nazionale (*lett. c)*);
- all'integrità del procedimento penale o amministrativo (*lett. d)*).

La norma precisa, inoltre, che le informazioni scambiate in via riservata tra le autorità di vigilanza del mercato e tra queste ultime e la Commissione non sono divulgate senza il preventivo accordo con l'autorità da cui provengono le predette informazioni.

Inoltre, il rispetto delle prescrizioni in materia di riservatezza non pregiudicano i diritti e gli obblighi della Commissione, degli Stati membri e degli organismi notificati in materia di scambio delle informazioni e di diffusione degli avvisi di sicurezza, né gli obblighi delle persone interessate di fornire informazioni a norma del diritto penale degli Stati membri.

Infine, la Commissione e gli Stati membri possono scambiare, ove necessario, informazioni sensibili con le autorità competenti dei paesi terzi con i quali abbiano concluso accordi di riservatezza, bilaterali o multilaterali, che garantiscano un livello di protezione adeguato.