Cyber Resilience Act in Italia: il decreto affida ad ACN la vigilanza del mercato, ma il procedimento sanzionatorio non risulta ancora disciplinato

Cyber Resilience Act in Italia: il 2 ottobre 2026 il Consiglio dei ministri n. 191 ha approvato in esame preliminare il decreto legislativo di adeguamento al regolamento (UE) 2024/2847, il regolamento sulla ciberresilienza. Il testo designa l'Agenzia per la cybersicurezza nazionale come autorità di notifica degli organismi di valutazione della conformità e come autorità di vigilanza del mercato.

La scelta è meno scontata di quanto sembri. Nella stessa seduta il Governo ha approvato anche il decreto di adeguamento al regolamento macchine, e lì la vigilanza resta ai ministeri di settore, comprese le macchine che presentano requisiti di cibersicurezza.

C'è poi un secondo elemento, che nessuna delle sintesi pubblicate in questi giorni ha rilevato. Il decreto rinvia, per il procedimento sanzionatorio, a un regolamento dell'Agenzia che doveva essere adottato entro il 15 ottobre 2024. Sugli atti consultabili quel regolamento non risulta.

Che cosa ha approvato il Consiglio dei ministri

Il comunicato precisa i confini delle due designazioni. Nel primo ruolo l'ACN non valuta né controlla gli organismi: quei

compiti restano all’organismo nazionale di accreditamento. Nel secondo ruolo, quello di vigilanza del mercato, l’Agenzia può avvalersi della Guardia di finanza.

Il riparto con le altre autorità segue le competenze. Per i prodotti che sono anche sistemi di intelligenza artificiale ad alto rischio vigilano le autorità previste dalla disciplina nazionale sull’intelligenza artificiale. Per gli istituti finanziari vigilati vigilano Banca d’Italia, Consob e IVASS. Per i profili di protezione dei dati vigila il Garante privacy. Le autorità operano in coordinamento, anche attraverso accordi per lo scambio di informazioni.

Per microimprese e PMI, start-up comprese, è previsto un canale dedicato di consulenza, definito da ACN e Ministero delle imprese e del Made in Italy. Le tariffe per la valutazione della conformità devono essere proporzionate.

È istituita, sotto la supervisione dell’Agenzia, la Sandbox-CRA. È uno spazio di sperimentazione normativa con ambienti di prova controllati prima dell’immissione sul mercato, con accesso prioritario per micro e piccole imprese. Lo spazio è coordinato con quelli per i servizi finanziari e per l’intelligenza artificiale.

Due elementi del comunicato sono sfuggiti alle sintesi di stampa. I consumatori possono segnalare vulnerabilità, incidenti e minacce direttamente al CSIRT Italia. E le violazioni del regolamento entrano fra le materie per cui si possono promuovere azioni rappresentative a tutela di interessi collettivi.

Perché il decreto arriva adesso

La delega è l’articolo 15 della legge 17 marzo 2026, n. 36, legge di delegazione europea 2025. Il termine è di sei mesi dall’entrata in vigore della legge, avvenuta il 9 aprile 2026. Scadeva quindi intorno al 9 ottobre 2026, una settimana dopo

la seduta.

Il margine è meno stretto di quanto appaia. L’articolo 31, comma 3, della legge 234/2012 proroga di tre mesi il termine della delega quando la scadenza del parere parlamentare cade nei trenta giorni precedenti. L’esame preliminare serve proprio ad aprire quella fase, con i pareri delle commissioni e del Consiglio di Stato.

Resta il ritardo rispetto al calendario europeo. Il capo IV del regolamento, quello sulla notifica degli organismi di valutazione della conformità, si applica dall’11 giugno 2026. Il decreto che designa l’autorità di notifica arriva quasi quattro mesi dopo. Il calendario completo è ricostruito nel pezzo su Cyber Resilience Act e obblighi 2026.

La delega aveva già deciso quasi tutto

Chi legge il comunicato come una scelta compiuta in ottobre legge male la sequenza. Le designazioni erano scritte nella delega da marzo.

La lettera b) dell’articolo 15 indica l’ACN come autorità di notifica ai sensi dell’articolo 36 del regolamento. La lettera c) la indica come autorità di vigilanza del mercato ai sensi dell’articolo 52, limitatamente ai requisiti orizzontali di cibersicurezza. I due rinvii corrispondono: l’articolo 36 è intitolato alle autorità di notifica, l’articolo 52 alla vigilanza del mercato.

La lettera d) chiede forme di coordinamento con le autorità individuate dal decreto legislativo 12 ottobre 2022, n. 157, cioè l’ossatura nazionale della vigilanza del mercato.

La lettera f) è quella che rende possibile la trasposizione. Consente di definire il sistema sanzionatorio anche in deroga ai limiti dell’articolo 32, comma 1, lettera d), della legge

234/2012, che ferma le sanzioni amministrative fra 150 e 150.000 euro.

L’aritmetica spiega perché la deroga non sia un dettaglio tecnico. Il massimale più alto del regolamento è di 15 milioni di euro o del 2,5 per cento del fatturato mondiale annuo. Senza la deroga il legislatore delegato si sarebbe fermato a un centesimo di quella cifra.

La stessa lettera f) chiede altre tre cose: coordinamento con l’impianto sanzionatorio del decreto-legge 105/2019 e del decreto legislativo 138/2024, coerenza procedurale con l’articolo 17, comma 4-quater, del decreto-legge 82/2021, e misure deflative del procedimento o del contenzioso.

Gli introiti delle sanzioni sono versati all’entrata del bilancio dello Stato e riassegnati alla dotazione dell’Agenzia. Il comma 3 quantifica l’onere sulle risorse dell’ACN in 2.100.000 euro per il 2026, 5.875.000 per il 2027, 9.125.000 per il 2028 e 6.925.000 annui dal 2029. Vanno letti sulla dotazione ordinaria del capitolo, che l’articolo 18 del decreto-legge 14 giugno 2021, n. 82 fissa in 110 milioni per il 2026 e 122 milioni annui dal 2027.

Due architetture nella stessa seduta

Il decreto di adeguamento al regolamento macchine, approvato il 2 ottobre insieme a quello sulla ciberresilienza, costruisce un’architettura diversa. Individua come autorità di vigilanza il Ministero delle imprese e del Made in Italy e il Ministero del lavoro, anche per le macchine che presentano requisiti di intelligenza artificiale e cibersicurezza.

Nello stesso testo il MIMIT è autorità di notifica degli organismi, l’accreditamento spetta ad ACCREDIA, le sanzioni sono irrogate dalle Camere di commercio e i proventi sono

riassegnati alle autorità di vigilanza.

La lettura della redazione è questa: nella stessa giornata il Governo ha adottato due modelli. Per i prodotti con elementi digitali la vigilanza del mercato passa all'autorità cyber. Per le macchine con requisiti di cibersicurezza resta ai ministeri di settore. Il criterio discriminante non è la materia, è l'atto europeo di riferimento.

Lo stesso confronto ridimensiona il circuito dei proventi sanzionatori. Compare nel decreto CRA e nel decreto macchine, e per l'ACN esiste dal 2021. Va raccontato come estensione di una tecnica consolidata, non come invenzione del CRA.

Che cosa l'ACN era già, e che cosa diventa

La novità va circoscritta con precisione. L'articolo 7, comma 1, lettera e), del decreto-legge 82/2021 attribuisce già all'ACN il ruolo di autorità nazionale di certificazione della cibersicurezza ai sensi dell'articolo 58 del regolamento (UE) 2019/881. Quel ruolo comprende l'accertamento delle violazioni e l'irrogazione delle sanzioni, funzioni assorbite dall'ex Ministero dello sviluppo economico.

L'Agenzia non arriva quindi nuova ai poteri sanzionatori sui prodotti. La novità è la vigilanza del mercato in senso tecnico. L'articolo 52, paragrafo 1, del regolamento sulla ciberresilienza dichiara applicabile il regolamento (UE) 2019/1020 ai prodotti con elementi digitali, e con esso il corredo di richiami, ritiri e divieti di immissione sul mercato.

La vigilanza non diventa però interamente cyber. I requisiti di cibersicurezza del regolamento delegato (UE) 2022/30 sulle apparecchiature radio restano sotto la sorveglianza del mercato del MIMIT, e il decreto macchine conferma

l’impostazione.

Un elemento pratico non è stato scritto da nessuna delle fonti disponibili. L’articolo 16, comma 11, del decreto-legge 82/2021 ha inserito nell’articolo 135, comma 1, del codice del processo amministrativo la lettera h-bis, che riserva alla competenza funzionale inderogabile le controversie sui provvedimenti dell’ACN. Un richiamo, un ritiro o un divieto di immissione si impugnano quindi davanti al giudice amministrativo in sede funzionalmente competente, non davanti al foro dell’impresa.

Esiste infine un raccordo con il Garante privacy che il decreto non deve inventare. L’articolo 7, comma 5, impone già all’ACN di consultare il Garante e di collaborare con esso, anche sugli incidenti che comportano violazioni di dati personali, con possibilità di protocolli d’intenti. La domanda aperta è se quel protocollo sia mai stato adottato.

Il regolamento che non risulta adottato

Qui il quadro cambia, e cambia la lettura del decreto.

L’articolo 17, comma 4-quater, del decreto-legge 82/2021 non descrive un procedimento. Prevede che la disciplina del procedimento sanzionatorio dell’Agenzia sia definita con regolamento, adottato con decreto del Presidente del Consiglio, sentito il Comitato interministeriale per la cybersicurezza e acquisito il parere delle commissioni parlamentari competenti. Il regolamento può essere adottato anche in deroga all’articolo 17 della legge 400/1988.

Quel comma è stato introdotto dall’articolo 11 della legge 28 giugno 2024, n. 90, pubblicata in Gazzetta ufficiale il 2 luglio 2024 ed entrata in vigore il 17 luglio 2024. Il termine per l’adozione era di novanta giorni, quindi scadeva il 15

ottobre 2024.

Lo stesso comma fissa la regola transitoria. Fino all’entrata in vigore del regolamento, ai procedimenti sanzionatori si applicano le sezioni I e II del capo I della legge 24 novembre 1981, n. 689.

La verifica dell’adozione dà esito negativo, e conviene dire come è stata condotta. Nella pagina degli atti generali dell’ACN, aggiornata al 23 settembre 2026, sotto la legge 90/2024 è elencato un solo decreto del Presidente del Consiglio. È quello del 30 aprile 2025 sui contratti di beni e servizi informatici, che attua un altro articolo della stessa legge.

Il regolamento non compare neppure fra gli atti del Governo sottoposti a parere della I Commissione della Camera nella XIX legislatura, che è la sede in cui furono esaminati i regolamenti dell’Agenzia del 2021. Nessuna ricerca restituisce una pubblicazione in Gazzetta ufficiale.

Qui serve una precisazione di metodo. Questo è un riscontro negativo su fonti consultabili, non una dichiarazione di mancata adozione, e va preso per quello che è. Prima di pubblicare conviene chiedere conferma all’Agenzia.

Allo stato degli atti reperibili, quindi, il procedimento sanzionatorio dell’ACN resta quello transitorio della legge 689/1981. E la cosa non riguarda soltanto il CRA.

L’articolo 1, comma 6, della legge 90/2024 applica la sanzione da 25.000 a 125.000 euro espressamente nel rispetto dell’articolo 17, comma 4-quater. Gli articoli 2 e 3 rinviano alla stessa sanzione, per il mancato adeguamento alle segnalazioni dell’Agenzia e per i soggetti del perimetro di sicurezza nazionale cibernetica.

Allo stesso regolamento rinvia anche lo schema di decreto legislativo sull’intelligenza artificiale, all’articolo 24,

comma 3. Sommando il decreto CRA si arriva a cinque insiemi di sanzioni che poggiano su un atto atteso dall’ottobre 2024 e di cui non si trova traccia.

C’è infine una conseguenza processuale che il decreto, per quanto si legge nel comunicato, non risolve. La legge 689/1981 porta l’opposizione all’ordinanza ingiunzione davanti al giudice ordinario, giudice di pace o tribunale secondo il valore. Il risultato possibile è una biforcazione: giudice amministrativo per il ritiro del prodotto, giudice ordinario per l’opposizione alla sanzione pecuniaria. Va verificata sul testo quando sarà pubblicato.

Il decreto sull’intelligenza artificiale chiude il cerchio

Per i prodotti che sono anche sistemi di intelligenza artificiale ad alto rischio il decreto CRA rinvia alle autorità della disciplina nazionale. Quella disciplina ha una base e un attuativo. La base è l’articolo 20 della legge 23 settembre 2025, n. 132, che designa AgID e ACN come autorità nazionali. L’attuativo è lo schema trasmesso alla Presidenza del Senato il 3 luglio 2026 come Atto del Governo n. 421, approvato in esame preliminare il 10 giugno 2026.

Lo schema designa AgID autorità nazionale di notifica, all’articolo 4. All’articolo 5, comma 1, lettera a), designa l’ACN autorità di vigilanza del mercato ai sensi dell’articolo 70 del regolamento (UE) 2024/1689. La lettera b) riserva Banca d’Italia, Consob e IVASS ai settori vigilati, la lettera c) limita il Garante all’articolo 74, paragrafo 8. L’articolo 6 fa dell’ACN il punto di contatto unico nazionale.

Il rinvio del decreto CRA è quindi circolare. Per un prodotto che è anche sistema ad alto rischio la vigilanza del mercato torna all’ACN, cioè alla stessa autorità che il CRA ha designato.

La simmetria va oltre il riparto. L’articolo 10 dello schema applica all’ACN il decreto legislativo 157/2022, cioè la stessa cornice nazionale su cui si innesta il decreto CRA, con l’esclusione degli articoli 11 e 12. Gli articoli da 26 a 31 istituiscono lo spazio di sperimentazione italiano per l’intelligenza artificiale, cogestito da AgID e ACN e coordinato con la sperimentazione fintech del decreto-legge 34/2019.

Letta accanto a quello schema, la Sandbox-CRA perde il carattere di primizia. È il terzo anello di una catena di spazi sperimentali, e il decreto CRA lo dichiara quando ne chiede il coordinamento con gli altri due.

Gli obblighi che scattano l’11 settembre 2026, anche sui prodotti venduti anni fa

Gli orientamenti della Commissione sull’articolo 26 del regolamento sono la comunicazione C(2026) 5252 final del 27 luglio 2026. Il titolo è indicativo: approvazione del contenuto di una bozza di comunicazione. Il documento dice che gli orientamenti saranno adottati formalmente quando tutte le versioni linguistiche saranno disponibili, e che solo da quel momento si applicheranno.

L’allegato conta 84 pagine. Due passaggi interessano direttamente chi produce in Italia.

Il primo è il paragrafo 210. L’articolo 14 del regolamento, quello sugli obblighi di segnalazione, si applica dall’11 settembre 2026 a tutti i prodotti nell’ambito del regolamento, compresi quelli immessi sul mercato prima dell’11 dicembre 2027. Lo stesso paragrafo precisa che gli obblighi di segnalazione proseguono anche dopo la fine del periodo di supporto, a differenza degli obblighi di gestione delle

vulnerabilità. Chi ha venduto un prodotto connesso anni fa deve quindi segnalare oggi, anche su un prodotto che non aggiorna più.

Il secondo è il paragrafo 212, e riduce lo spazio di un argomento ricorrente. La Commissione allinea la nozione di venire a conoscenza fra CRA, NIS2 e GDPR. Richiama il considerando 31 del regolamento di esecuzione (UE) 2024/2690 e le linee guida 9/2022 del comitato europeo per la protezione dei dati.

Il momento da cui decorrono i termini è quindi già armonizzato a livello europeo. Quello che resta disallineato è il lato italiano.

Si prenda una vulnerabilità sfruttata attivamente in un dispositivo connesso venduto in Italia. L'articolo 14 impone la notifica simultanea al CSIRT designato come coordinatore e all'ENISA, tramite la piattaforma unica di segnalazione. I termini sono preallarme entro 24 ore, notifica entro 72 ore e relazione finale entro 14 giorni. In Italia quel CSIRT è il CSIRT Italia.

Se il fabbricante è anche soggetto NIS2, al medesimo CSIRT Italia arriva una seconda notifica, su base giuridica diversa e con termini quasi identici. Il quadro NIS2 è ricostruito nel pezzo su NIS2 e decreto legislativo 138/2024. Se vi sono dati personali si aggiunge la notifica al Garante, con il termine di 72 ore dell'articolo 33 del GDPR.

La lettura della redazione si riassume in una frase. La Commissione ha armonizzato l'orologio, l'Italia non ha armonizzato il contatore: stesso destinatario, basi giuridiche diverse, procedimenti e regimi sanzionatori separati.

Le norme armonizzate, e il mese che

le separa dall’applicazione piena

La richiesta di normazione è la decisione di esecuzione C(2025) 618 final del 3 febbraio 2025, adottata sulla base dell’articolo 10, paragrafo 1, del regolamento 1025/2012. È indirizzata a CEN, Cenelec ed ETSI, e fanno fede le sole versioni inglese, francese e tedesca.

L’allegato I elenca 41 voci con tre scadenze. Due voci sono fissate al 30 agosto 2026: la 1 su progettazione, sviluppo e produzione e la 15 sulla gestione delle vulnerabilità. Ventisei voci, dalla 16 alla 41, sono fissate al 30 ottobre 2026. Tredici voci, dalla 2 alla 14, sono rinviate al 30 ottobre 2027.

L’articolo 1, paragrafo 2, ripartisce il lavoro fra le tre organizzazioni. L’articolo 2, paragrafo 3, impone che le voci 39, 40 e 41 siano sviluppate in un ambito riservato, con rappresentanti di organizzazioni stabilite nell’Unione. Sono i dispositivi con security box, i gateway dei contatori intelligenti e le smartcard o elementi sicuri. Il programma di lavoro congiunto delle tre organizzazioni, versione 1 del 2 aprile 2025, ricalca le stesse scadenze.

Il dato editoriale non è la proroga di cui si discute da luglio, che alla chiusura di questo pezzo resta una bozza non adottata. È che le tredici norme orizzontali sui requisiti essenziali sono attese al 30 ottobre 2027, poco più di un mese prima dell’applicazione piena del regolamento, fissata all’11 dicembre 2027.

Gli atti che completano il quadro, e quelli che ancora mancano

Il regolamento di esecuzione (UE) 2025/2392 del 28 novembre 2025 stabilisce la descrizione tecnica delle categorie di prodotti importanti e critici, riempiendo gli allegati III e

IV del regolamento. Senza quell'atto la classificazione del prodotto resta indeterminata, quindi è il presupposto del percorso di conformità su cui vigilerà l'ACN.

Gli orientamenti dell'articolo 26 esistono nel contenuto ma non sono ancora applicabili, come si è visto. Il decreto italiano assegna la vigilanza a un'autorità che dovrà applicare un documento approvato e non ancora in vigore.

Una nota degli orientamenti rinvia infine al programma di lavoro della Commissione per il 2026. Quel programma prevede un European Product Act, destinato ad aggiornare il nuovo quadro legislativo e le regole su vigilanza del mercato e normazione. L'impianto su cui il decreto innesta l'ACN è quindi esso stesso in revisione.

Che cosa guardare nei prossimi mesi

Sei punti, in ordine di prossimità.

1. I pareri delle commissioni parlamentari e del Consiglio di Stato, e l'esame definitivo entro il termine prorogato della delega.
2. Il testo pubblicato, su tre elementi: l'entità delle sanzioni dentro la deroga, il procedimento applicabile e il giudice competente.
3. Il regolamento sul procedimento sanzionatorio dell'ACN: se sia stato adottato, e in caso contrario quando lo sarà.
4. L'adozione formale degli orientamenti dell'articolo 26, che vale anche per la nozione di venire a conoscenza.
5. Lo stato delle norme armonizzate, con l'eventuale modifica della richiesta di normazione e le date di chiusura delle procedure ETSI.
6. L'eventuale protocollo d'intenti fra ACN e Garante privacy ai sensi dell'articolo 7, comma 5, del decreto-legge 82/2021.

https://www.ictsecuritymagazine.com/articoli/cyber-resilience-act-italia-decreto-acn-vigilanza-mercato/