Confartigianato Imprese 80 1946 2026

CNA 80 Artigiani Imprenditori d'Italia

Senato della Repubblica
XIX Legislatura

Commissioni riunite
1ª (Affari costituzionali)
8ª (Ambiente, transizione ecologica, energia, lavori pubblici, comunicazioni, innovazione tecnologica)

Documento di osservazioni e proposte

Schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale al regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza)

(A.G. 447)

3 novembre 2026

Sommario

Premessa.....3

Le imprese interessate 3

Assistenza tecnica alla segnalazione..... 5

Misure per le micro e piccole imprese.....6

Sistema sanzionatorio.....10

Sperimentazione regolamentare.....13

Indicazioni operative dell'Agenzia.....13

Attuazione, consultazione e monitoraggio.....14

Ulteriori suggerimenti e posizioni da sostenere in sede europea.....15

AG 447 - regolamento sulla ciberresilienza

Premessa

Confartigianato Imprese e CNA ringraziano le Commissioni per l'opportunità di contribuire all'esame dello schema di decreto legislativo che adegua l'ordinamento nazionale al regolamento europeo sulla cibersicurezza dei prodotti con elementi digitali.

Le Confederazioni condividono l'obiettivo del regolamento. Prodotti più sicuri tutelano cittadini e imprese e rafforzano la fiducia nel mercato digitale. La capacità di documentare e mantenere nel tempo la sicurezza dei prodotti potrà inoltre rafforzare il rapporto delle imprese con i committenti e con le filiere. Dall'11 dicembre 2027, i prodotti con elementi digitali soggetti al regolamento potranno essere immessi sul mercato solo se conformi ai requisiti applicabili, sottoposti a valutazione della conformità e provvisti di marcatura CE.

Proprio per questo le Confederazioni ritengono che l'attuazione del regolamento debba tenere conto della struttura del sistema produttivo italiano, composto in larghissima parte da micro e piccole imprese. Il regolamento stesso lo riconosce, quando prevede che gli Stati membri intraprendano, se del caso, misure specifiche di accompagnamento per queste imprese (art. 33). Le osservazioni che seguono si concentrano sugli aspetti che auspicabilmente andrebbero migliorati e non da ultimo su alcune posizioni da sostenere in sede europea.

1. Le imprese interessate

Il regolamento non riguarda soltanto i grandi produttori di *hardware* e *software*. Possono esserne interessate anche le *software house* artigiane, gli sviluppatori di applicazioni e gestionali, gli integratori di sistemi, gli installatori di impianti domotici, di sicurezza e di rete, i costruttori di macchine e apparecchiature che incorporano componenti *software*, quando sviluppano, commercializzano, distribuiscono o modificano prodotti con elementi digitali, secondo il ruolo concretamente svolto.

Le sole imprese dei servizi digitali (produzione di *software*, consulenza informatica, servizi di informazione) sono oltre 104.500, con più di 517 mila addetti e un fatturato superiore a 73 miliardi di euro. Il 93,7% di esse ha meno di dieci addetti e il 98,8% meno di cinquanta (elaborazioni Confartigianato Imprese - CNA). Si tratta di dati che descrivono il settore e non di una stima delle imprese soggette al regolamento. Molte operano su commessa, sviluppando soluzioni su misura per i propri clienti.

Per il regolamento è fabbricante chi sviluppa o fabbrica un prodotto con elementi digitali, o lo fa progettare o fabbricare, e lo commercializza con il proprio nome o marchio, anche quando si tratta di un esemplare unico realizzato per un solo cliente. Lo diventa anche chi, non essendo fabbricante,

importatore o distributore, apporta a un prodotto altrui una modifica sostanziale e lo mette a disposizione sul mercato, con obblighi limitati alla parte interessata dalla modifica, salvo che questa incida sulla cibersicurezza dell'intero prodotto (art. 22); importatori e distributori assumono gli obblighi del fabbricante quando immettono il prodotto con il proprio nome o marchio o apportano una modifica sostanziale a un prodotto già immesso sul mercato (art. 21). Le sole prestazioni di installazione, configurazione e manutenzione di *software* di terzi che non costituiscono una modifica sostanziale, cioè che non incidono sulla conformità ai requisiti essenziali di cibersicurezza dell'allegato I, parte I, né modificano la finalità prevista del prodotto, non comportano invece, di per sé, l'assunzione del ruolo di fabbricante, fermi gli eventuali obblighi legati ad altri ruoli, come quello di distributore. Il confine tra le diverse ipotesi, tuttavia, non è sempre netto, ed è proprio sul terreno delle personalizzazioni che si gioca l'attività quotidiana di molte nostre imprese.

Al fabbricante il regolamento chiede, per ogni prodotto, valutazione dei rischi, documentazione tecnica, valutazione della conformità e marcatura CE, oltre a un periodo di assistenza di sicurezza di norma non inferiore a cinque anni. Per chi realizza soluzioni su misura, ogni prodotto diverso consegnato a un cliente richiede la propria documentazione e la propria valutazione, e gli obblighi di assistenza delle diverse commesse si sommano nel tempo.

Una parte degli obblighi è già operativa. Dall'11 settembre 2026 i fabbricanti devono segnalare le vulnerabilità attivamente sfruttate e gli incidenti gravi che hanno un impatto sulla sicurezza del prodotto di cui vengono a conoscenza, anche per i prodotti immessi sul mercato prima dell'applicazione generale del regolamento. Le disposizioni sugli organismi di valutazione della conformità si applicano dall'11 giugno 2026, mentre gli altri obblighi dei fabbricanti si applicheranno dall'11 dicembre 2027. I prodotti immessi sul mercato prima di quella data non devono essere riadeguati, salvo che siano oggetto di successive modifiche sostanziali; per essi resta fermo l'obbligo di segnalazione.

L'analisi di impatto della regolamentazione che accompagna lo schema riconosce che questi oneri potranno incidere in misura proporzionalmente maggiore sulle piccole e medie imprese. Le difficoltà trovano riscontro nei dati europei. In un'indagine condotta dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA) tra febbraio e marzo 2026, con 194 risposte di piccole e medie imprese europee, il 57% delle microimprese partecipanti ha dichiarato di non avere una persona, interna o esterna, specificamente responsabile della cibersicurezza. Soltanto il 13% dei partecipanti dichiara una comprensione buona o molto buona dei requisiti di documentazione tecnica, e il 14% delle procedure di valutazione della conformità. La stessa ENISA avverte che il campione, a partecipazione

volontaria, non è rappresentativo e riflette verosimilmente le imprese più attente al tema: nella generalità delle imprese la situazione potrebbe essere meno favorevole.

Lo schema, tuttavia, traduce la consapevolezza di questi oneri in misure in gran parte programmatiche. Le osservazioni che seguono riguardano tre ambiti: le misure di sostegno, il sistema sanzionatorio, l'attuazione.

2. Assistenza tecnica alla segnalazione

L'obbligo di segnalazione si applica dal settembre 2026, con termini stringenti: un preallarme entro 24 ore, una notifica entro 72 ore, una relazione finale e l'informazione agli utilizzatori interessati. L'assistenza tecnica che i CSIRT (*Computer Security Incident Response Team*) devono prestare in particolare alle micro, piccole e medie imprese (art. 17, paragrafo 6, del regolamento) si applicherà invece soltanto dal dicembre 2027. Per circa quindici mesi, dunque, le imprese sono tenute a effettuare le segnalazioni senza che lo schema assicuri espressamente, per questa fase, un servizio dedicato con prestazioni e tempi definiti, proprio quando devono imparare a qualificare gli eventi e a utilizzare la piattaforma europea di segnalazione.

Lo schema finanzia l'adeguamento del Portale per le segnalazioni dell'Agenzia per la cybersicurezza nazionale (art. 17), e la relazione tecnica ne giustifica la spesa anche in ragione delle «connesse attività di supporto» ai soggetti interessati, includendo tra i compiti dell'Agenzia l'orientamento e la consulenza agli operatori economici. Il testo dell'art. 17, tuttavia, non prevede espressamente un servizio di assistenza per le imprese di minori dimensioni.

Nulla impedisce al legislatore nazionale di anticipare questo servizio. Le Confederazioni chiedono pertanto che il CSIRT Italia offra, dall'entrata in vigore del decreto, assistenza alle micro e piccole imprese per l'intero ciclo delle segnalazioni, con modelli guidati e strumenti di ausilio alla compilazione conformi ai formati e alle procedure europee, e con tempi di risposta definiti.

Per le imprese soggette sia al regolamento sia alla disciplina NIS2, inoltre, lo stesso evento può dover essere segnalato in più flussi, con tempi e contenuti diversi. Il regolamento incoraggia gli Stati a dotarsi di un punto di accesso nazionale unico (considerando 72), e la legge di delegazione europea 2025 (L. 36/2026) all’art. 15, comma 2, lettera a) chiede di coordinare la nuova disciplina con il d.lgs. 138/2024 e con il DL 105/2019 (. Si chiede quindi che il Portale delle segnalazioni di cui all'art. 17 consenta di inserire una sola volta i dati comuni e di inoltrarli ai destinatari competenti, nel rispetto dei termini, dei contenuti, delle competenze e delle regole di riservatezza e di protezione dei dati propri di ciascuna disciplina.

Lo stesso considerando 72 contempla punti di accesso unici nazionali anche per le notifiche previste dal regolamento (UE) 2016/679, senza pregiudizio per l'indipendenza delle autorità di protezione dei dati. Si chiede pertanto che l'Agenzia per la cybersicurezza nazionale e il Garante per la protezione dei dati personali valutino modalità per evitare la duplicazione dei dati comuni quando il medesimo soggetto è tenuto, per uno stesso evento, alle notifiche previste da entrambe le discipline, nel rispetto delle procedure europee di segnalazione, dell'autonomia degli obblighi, dei destinatari e dei termini, e delle regole di riservatezza e di protezione dei dati.

3. Misure per le micro e piccole imprese

Il Capo V dello schema è dedicato alle microimprese e alle piccole imprese. L'art. 18 affida all'Agenzia, quale Centro nazionale di coordinamento, la promozione di iniziative per le competenze delle micro, piccole e medie imprese, e stabilisce che il Ministero delle imprese e del *made in Italy* e l'Agenzia definiscano le modalità di attuazione delle misure previste dall'art. 33, paragrafo 1, del regolamento: formazione, canale di consulenza dedicato, sostegno alle attività di prova e valutazione della conformità. Colloca però questo adempimento «nell'ambito degli accordi» dell'art. 12, comma 2, che riguardano il coordinamento tra le autorità di vigilanza, sono formulati come facoltativi («possono essere disciplinati») e non hanno un termine di adozione. Secondo la relazione tecnica, la formazione e il sostegno alle prove rientrano nelle competenze già attribuite all'Agenzia e saranno svolti con le risorse disponibili, mentre il canale dedicato sarà assicurato con gli strumenti di comunicazione esistenti, «anche attraverso l'attivazione di un indirizzo di posta elettronica dedicato o di un'apposita interfaccia sui siti istituzionali».

L'art. 18 è previsto a invarianza finanziaria. L'autorizzazione di spesa dell'art. 26, che cresce fino a oltre 9 milioni di euro nel 2028 per poi stabilizzarsi intorno ai 7 milioni annui, finanzia la vigilanza, il Portale delle segnalazioni e le missioni di cooperazione internazionale connesse alla sperimentazione regolamentare; la parte prevalente, a regime quasi 6 milioni annui, è destinata all'incremento dell'organico dell'Agenzia. Nessuna quota è riservata ai servizi per le imprese di minori dimensioni.

Si chiede pertanto che gli accordi dell'art. 18 siano resi autonomi rispetto alla cornice facoltativa dell'art. 12, comma 2, e che il loro obbligo di adozione sia esplicitato con un termine certo, ad esempio novanta giorni dall'entrata in vigore del decreto. Gli accordi dovrebbero individuare un responsabile del canale e livelli minimi di servizio, con tempi massimi di presa in carico e risposte informative scritte, che non costituiscono pareri di conformità né atti vincolanti per le autorità, in

raccordo con le Camere di commercio, i poli europei dell'innovazione digitale e le associazioni di categoria.

Nell'indagine ENISA già richiamata, tra i supporti più richiesti figurano modelli e liste di controllo: il 73% dei partecipanti indica quelli per la documentazione tecnica, il 71% quelli per documentare le pratiche di sviluppo sicuro, oltre la metà quelli per la gestione delle vulnerabilità e la valutazione dei rischi. Lo schema non fissa scadenze né specifica gli strumenti. Si chiede che gli accordi prevedano un programma, con tempi e risorse individuati, per rendere disponibili gratuitamente e in lingua italiana modelli e liste di controllo per la documentazione tecnica, la valutazione dei rischi, la gestione delle vulnerabilità e la risposta agli incidenti, insieme a brevi percorsi formativi per titolari e sviluppatori, in raccordo con gli strumenti europei, i *Competence Center* e i poli europei dell'innovazione digitale.

Per le micro e piccole imprese che non dispongono di una funzione interna di sicurezza, gli accordi potrebbero inoltre promuovere, tramite i poli europei dell'innovazione digitale e il Centro nazionale di coordinamento, la messa a disposizione di strumenti tecnici gratuiti e di servizi di orientamento per il monitoraggio delle vulnerabilità dei componenti, la predisposizione e l'aggiornamento della distinta dei componenti *software* e la preparazione delle segnalazioni. Potrebbero altresì favorire servizi condivisi di assistenza offerti da soggetti terzi, anche in forma associativa, secondo criteri trasparenti e con accesso indipendente dall'adesione associativa. Restano fermi gli obblighi del fabbricante, la terzietà dell'Agenzia quale autorità di vigilanza e le competenze degli organismi notificati.

Il canale dedicato e i materiali di supporto dovranno essere accessibili a tutte le imprese interessate, anche non associate. Poiché, come rileva la stessa indagine ENISA, le imprese si informano attraverso più canali, si propone una diffusione coordinata tramite i siti istituzionali, le Camere di commercio, le associazioni di categoria e i poli dell'innovazione.

Questi servizi richiedono risorse. La legge di delegazione riferisce le risorse per l'Agenzia ai compiti previsti dal regolamento (art. 15, comma 2, lettera g), della legge 36/2026): tra questi rientra l'assistenza alle segnalazioni che il regolamento affida ai CSIRT, mentre lo schema affida all'Agenzia, insieme al Ministero, anche la definizione delle misure di sostegno, compreso il canale dedicato. Le scriventi Confederazioni sono consapevoli che l'autorizzazione di spesa dell'art. 26 è già dettagliatamente ripartita su specifiche voci riportate nella relazione tecnica, non prevedendo più dal 2029 stanziamenti finalizzati a sviluppo delle piattaforme e formazione, e che l'art. 18 è oggi soggetto alla clausola di invarianza. Si chiede pertanto di includere l'art. 18 tra le disposizioni alla cui

attuazione è destinata l'autorizzazione di spesa dell'art. 26, comma 1, e che la relazione tecnica individui e quantifichi, nell'ambito dell'autorizzazione complessiva e anche in termini di personale dedicato, le risorse annue da destinare ai servizi dell'art. 18, distinguendo le esigenze anteriori all'11 dicembre 2027 da quelle a regime. A queste risorse potrebbe aggiungersi, quando effettivamente disponibile, una parte dei proventi delle sanzioni, che lo schema destina al bilancio dell'Agenzia (art. 16): il regolamento invita gli Stati a valutarne l'impiego per rafforzare le capacità di cibersicurezza delle piccole e medie imprese (considerando 122).

Il progetto *SECURE* (*Strengthening EU SMEs Cyber Resilience*), coordinato dall'Agenzia e finanziato dal Programma Europa digitale, prevede inoltre complessivamente circa 16 milioni di euro di sostegno finanziario diretto alle piccole e medie imprese europee per l'adeguamento al regolamento. Secondo quanto comunicato dall'Agenzia, alla prima procedura, con una dotazione di circa 5 milioni, sono pervenute 259 proposte. Si chiede che gli accordi dell'art. 18 colleghino il canale dedicato a queste e alle altre opportunità europee, assicurando alle imprese informazione aggiornata e orientamento alla partecipazione. Si tratta di finanziamenti competitivi, che possono integrare i servizi nazionali ma non ne assicurano da soli la continuità.

La partecipazione ai finanziamenti può incontrare anche ostacoli linguistici. Nelle procedure che richiedono documentazione e candidature in inglese, come *SECURE*, tali requisiti possono rendere più difficile l'accesso delle micro e piccole imprese. Si chiede che, nell'ambito degli accordi dell'art. 18, il canale dedicato integri i materiali disponibili con schede informative, risposte alle domande frequenti, guide alla compilazione e traduzioni di cortesia dei documenti essenziali dei principali bandi per l'adeguamento al regolamento, in raccordo con i rispettivi gestori, indicando chiaramente i documenti ufficiali di riferimento e la lingua richiesta per la candidatura.

Occorre inoltre coordinare la programmazione degli incentivi con i tempi necessari per la valutazione delle domande, la stipula degli accordi e la realizzazione degli interventi. In alcune procedure europee, come risulta dalle indicazioni ufficiali del progetto *SECURE*, le attività svolte prima della firma dell'accordo non sono finanziabili, mentre la firma è prevista diversi mesi dopo la chiusura della procedura. Questo vincolo produce un disincentivo all'adeguamento tempestivo: l'impresa che, dopo aver presentato la domanda, anticipa gli interventi rinuncia al finanziamento delle attività già realizzate; quella che attende la firma rinvia l'adeguamento. Quando l'attesa si sovrappone all'applicazione degli obblighi, il problema riguarda anche interventi necessari a rimuovere non conformità. L'obbligo di intervenire resta fermo, ma le condizioni del sostegno

dovrebbero favorirne l'adempimento tempestivo: tempi più brevi delle procedure riducono uno degli ostacoli all'adeguamento.

Le scriventi Confederazioni auspicano pertanto che il parere impegni il Governo, nell'ambito degli accordi dell'art. 18 e nella predisposizione di eventuali misure nazionali di sostegno all'adeguamento al regolamento, a prevedere che i bandi consentano l'avvio delle attività e l'ammissibilità delle relative spese dalla presentazione di una domanda completa, subordinatamente alla concessione e nel rispetto dell'eventuale regime di aiuti di Stato applicabile; a pubblicare cronoprogrammi e termini definiti per le fasi di competenza delle amministrazioni; ad assicurare periodi congrui di realizzazione. Si chiede inoltre che il Governo e l'Agenzia, anche nel ruolo di coordinatore di progetti europei, promuovano nelle sedi competenti e nei limiti delle regole dei programmi dell'Unione soluzioni analoghe per i finanziamenti europei, e che il canale dedicato ne illustri tempi, condizioni di ammissibilità e rischi dell'avvio anticipato.

Un ulteriore punto riguarda la valutazione della conformità da parte di terzi, necessaria per alcune categorie di prodotti. Il regolamento prevede che le tariffe degli organismi notificati siano ridotte in proporzione per le piccole e medie imprese (art. 32, paragrafo 6). L'art. 18, comma 3, dello schema riprende il principio della proporzionalità delle tariffe, ma non l'obbligo espresso di riduzione. Si chiede di integrarlo in questo senso e di prevedere che gli organismi rendano pubblici i criteri e le modalità di applicazione delle riduzioni, anche come elemento verificato in sede di notifica. Poiché il regolamento chiede agli Stati di adoperarsi perché vi sia un numero sufficiente di organismi notificati entro l'11 dicembre 2026 (art. 35, paragrafo 2), si chiede inoltre che il Governo riferisca sullo stato delle notifiche e sulla capacità disponibile in Italia, includendo i tempi di accreditamento, designazione e notifica, e che nella determinazione delle tariffe dell'art. 5 siano rese trasparenti le attività remunerate, evitando duplicazioni di oneri rispetto alle valutazioni già svolte da Accredia. Il regolamento consente altresì agli Stati di accettare, per la documentazione dei fabbricanti e per le comunicazioni con le autorità, una lingua ampiamente compresa, per contenere i costi di traduzione delle imprese di minori dimensioni (considerando 94): si chiede che l'Agenzia accetti anche la lingua inglese e che ne sia favorita l'accettazione da parte degli organismi notificati stabiliti in Italia, ai quali il regolamento rimette la scelta per la documentazione relativa alla valutazione della conformità (art. 31, paragrafo 4).

Infine, l'art. 21 rinvia la determinazione dei parametri per il calcolo dei costi delle attività di vigilanza sui prodotti risultati non conformi al decreto del Presidente del Consiglio dei ministri previsto dall'art. 10, comma 2, del d.lgs. 179/2026. Si chiede che l'art. 21 indichi i criteri per l'adozione di tale

decreto: il recupero dovrebbe essere circoscritto ai costi diretti effettivamente sostenuti e documentati, secondo parametri pubblici, trasparenti e prevedibili, evitando addebiti non correlati alle attività effettivamente svolte o sproporzionati rispetto ai costi sostenuti. Per le micro e piccole imprese che rimuovano tempestivamente, entro il termine della diffida di cui alla sezione 4, non conformità esclusivamente formali e prive di incidenza sulla sicurezza del prodotto, l'art. 21 dovrebbe inoltre prevedere una riduzione proporzionata del recupero, distinguendo i minori costi derivanti dalla tempestiva regolarizzazione dall'eventuale agevolazione ulteriore, di cui la relazione tecnica valuti gli effetti finanziari, e mantenendo distinto il recupero dei costi dal trattamento sanzionatorio.

4. Sistema sanzionatorio

L'art. 15 dello schema rinvia integralmente alle sanzioni previste dall'art. 64 del regolamento. Questo fissa massimi differenziati per tipo di violazione (per le più gravi, fino a 15 milioni di euro o, se superiore, fino al 2,5% del fatturato mondiale annuo) e criteri di commisurazione, senza minimi edittali. Per le sanzioni irrogate dall'Agenzia, le modalità del procedimento sono rimesse al regolamento dell'Agenzia previsto dall'art. 17, comma 4-*quater*, del DL 82/2021, che, per quanto consta, non risulta ancora adottato, benché il termine previsto dalla norma sia da tempo decorso. Per quanto non diversamente disposto si applica, in quanto compatibile, la legge 689/1981 (art. 15, comma 6, dello schema). L'analisi di impatto dà conto della scelta di non individuare minimi edittali né una gradazione dei massimi.

Le sanzioni del regolamento si applicheranno dal dicembre 2027, ma l'assetto definito ora determinerà il quadro di riferimento delle imprese. Confartigianato e CNA segnalano tre profili.

Il primo riguarda il pagamento in misura ridotta. In assenza di un minimo edittale, la regola generale della legge 689/1981, ove applicabile, lo commisura a un terzo del massimo. Per le violazioni più gravi ciò condurrebbe a importi dell'ordine di milioni di euro, che rendono l'istituto di fatto inaccessibile a una microimpresa. Il regolamento chiede che la commisurazione tenga conto della dimensione dell'impresa (art. 64, paragrafo 5). Si chiede che il decreto chiarisca l'applicabilità dell'istituto e preveda per le micro e piccole imprese un autonomo istituto di definizione agevolata, anche in deroga all'art. 16 della legge 689/1981, che ne precisi la base di calcolo, la riduzione applicabile, commisurata anche alla dimensione dell'impresa e alla tempestiva regolarizzazione, il termine di pagamento e gli effetti sul procedimento, distinto dalla diffida di cui al profilo successivo e nel rispetto dell'effettività e della dissuasività richieste dall'art. 64, paragrafo 1.

Il secondo riguarda gli strumenti deflativi. La legge di delegazione chiede di definire il sistema sanzionatorio «apportando alla normativa vigente le necessarie modificazioni, anche al fine di introdurre misure deflative del procedimento sanzionatorio o del contenzioso» (art. 15, comma 2, lettera f), numero 3, della legge 36/2026). La relazione illustrativa ritiene attuato il criterio attraverso il rinvio al regolamento dell'Agenzia, che dovrebbe disciplinare anche misure di carattere riparatorio e, in base all'art. 7-*bis* del DL 117/2025, la possibilità di assegnare un congruo termine per adempiere. Quel termine, tuttavia, è previsto soltanto «nei casi di motivata impossibilità», e il regolamento non risulta ancora adottato, mentre la delega indicava la via della modifica della normativa vigente. Il rinvio non assicura quindi, nel decreto, i presupposti e gli effetti della regolarizzazione. In attuazione di quel criterio, le Confederazioni chiedono che il decreto preveda direttamente, per le micro e piccole imprese, una diffida ad adempiere con un termine congruo per le violazioni lievi, rimediabili, non dolose né gravemente colpose e non reiterate. In caso di ottemperanza nei termini, il decreto dovrebbe disciplinare espressamente la chiusura del procedimento senza irrogazione della sanzione pecuniaria, fermi restando gli obblighi di conformità e i poteri correttivi e restrittivi dell'autorità. Sarebbe una soluzione coerente con l'impostazione graduale che il regolamento adotta per le non conformità formali, per le quali l'autorità chiede in primo luogo al fabbricante di porvi rimedio (art. 58).

Il disallineamento descritto nella sezione 3 può riflettersi anche sul sistema sanzionatorio. Quando gli obblighi sono applicabili e un controllo accerta una non conformità alla quale corrispondono interventi già specificamente individuati in una precedente domanda di finanziamento pubblico, l'impresa si trova di fronte a un'alternativa: anticipare gli interventi, compromettendo il sostegno richiesto, oppure attendere la firma dell'accordo, prolungando la violazione e l'esposizione alle relative conseguenze. La presentazione della domanda non giustifica l'inadempimento, ma un sistema che penalizza chi si è attivato per adeguarsi rischia di premiare l'attesa anziché l'adeguamento. In un tessuto produttivo composto in larghissima parte da microimprese, la resilienza effettiva passa dal coordinamento tra sostegno e regolarizzazione.

Si chiede pertanto che, nell'ambito della diffida per le micro e piccole imprese, il decreto imponga all'autorità di valutare espressamente e motivatamente la possibilità di coordinare il termine di regolarizzazione con un progetto oggetto di domanda completa, presentata con data certa prima dell'avvio del controllo. Il coordinamento dovrebbe riguardare soltanto le non conformità formali o prive di rischio significativo per gli utilizzatori, e i soli adempimenti per i quali il regolamento consente l'assegnazione di un termine; non potrebbe differire gli obblighi di intervento immediato

o tempestivo del fabbricante né le misure di attenuazione necessarie. L'impresa dovrebbe documentare la corrispondenza degli interventi alla violazione, il vincolo di ammissibilità delle spese e un cronoprogramma attuabile. Il coordinamento dovrebbe operare entro un termine massimo fissato dal decreto, con verifiche intermedie e senza proroghe automatiche in caso di ritardo o di diniego del finanziamento. Restano esclusi gli obblighi di segnalazione e restano integri i poteri correttivi e restrittivi dell'autorità. Nella determinazione dell'eventuale sanzione dovrebbero comunque essere valutate, ai sensi dell'art. 64, paragrafi 1 e 5, del regolamento e dell'art. 11 della legge 689/1981, in quanto compatibile, le misure concrete, tempestive e documentate effettivamente adottate per rimediare alla violazione e limitarne le conseguenze, indipendentemente dalla fonte del loro finanziamento.

Il terzo profilo riguarda il coordinamento con le altre discipline di cibersicurezza. La legge di delegazione chiede di coordinare il sistema sanzionatorio con quanto previsto dalla disciplina NIS2 e dal Perimetro di sicurezza nazionale cibernetica. Lo schema non esercita questo criterio, ritenendo autonome le diverse discipline. Fatti connessi, ad esempio una vulnerabilità sfruttata in un prodotto del quale un fornitore di servizi gestiti soggetto alla disciplina NIS2 sia anche fabbricante, possono tuttavia dare luogo a più procedimenti davanti alla stessa Agenzia. Si chiede che il decreto preveda il coordinamento dell'istruttoria dei procedimenti relativi a fatti connessi e, per le sanzioni riferibili alla medesima condotta dello stesso soggetto, la valutazione del cumulo e della proporzionalità complessiva, fermi gli obblighi autonomi previsti da ciascuna disciplina.

Sul piano della vigilanza, un'esigenza di coordinamento analoga riguarda i prodotti classificati come sistemi di intelligenza artificiale ad alto rischio, per i quali lo schema individua più autorità di vigilanza del mercato (art. 9, comma 2). Si chiede che gli accordi dell'art. 12, comma 1, siano adottati entro un termine definito e resi pubblici, rendendo conoscibili i criteri di individuazione dell'autorità competente e le modalità di raccordo nei rapporti con gli istituti finanziari vigilati e con i loro fornitori. Gli accordi dovrebbero coordinare le istruttorie e favorire il riutilizzo della documentazione già acquisita, evitando richieste ripetitive alle imprese, ferme le competenze e le esigenze istruttorie di ciascuna autorità.

Si segnala infine che il regolamento esclude sanzioni pecuniarie a carico delle micro e piccole imprese per il mancato rispetto del termine di 24 ore del preallarme, e a carico dei gestori di *software open source* per qualsiasi violazione (art. 64, paragrafo 10, nel testo rettificato). Il considerando 120 chiarisce che, negli stessi casi, non dovrebbero applicarsi neppure altri tipi di sanzioni di natura pecuniaria. Si chiede che l'art. 15 precisi che, per le medesime violazioni del

regolamento, non si applichino neppure sanzioni nazionali di altra natura a carattere pecuniario. Quanto al regolamento sanzionatorio dell'Agenzia, che ha portata generale e il cui termine di adozione è scaduto, si chiede che il parere impegni il Governo a trasmetterne senza ulteriore indugio lo schema alle Commissioni parlamentari, assicurando la consultazione delle associazioni di categoria.

5. Sperimentazione regolamentare

L'art. 19 istituisce uno spazio di sperimentazione normativa per i prodotti innovativi prima della loro immissione sul mercato, in coerenza con l'art. 33, paragrafo 2, del regolamento, e riconosce alle micro e piccole imprese un accesso prioritario. L'attuazione è però rinviata a un decreto senza termine e, secondo la relazione tecnica, senza nuovi oneri.

Si chiede di fissare un termine per il decreto attuativo, da adottare sentite le associazioni di categoria, e di chiarire che possono accedervi, qualora presentino profili di innovazione, anche i prodotti sviluppati su commessa e le nuove versioni destinate all'immissione sul mercato, comprese quelle sviluppate a partire da prodotti già commercializzati. Per i prodotti già sul mercato, che restano fuori dal perimetro della sperimentazione, sarebbe utile prevedere nell'ambito degli accordi dell'art. 18 un servizio di supporto alle prove di conformità.

6. Indicazioni operative dell'Agenzia

Secondo la valutazione delle scriventi Confederazioni, gli orientamenti pubblicati dalla Commissione europea nel 2026, che non sono vincolanti, affrontano solo in termini generali alcuni temi decisivi per le imprese che rappresentiamo: il *software* sviluppato su commessa, le personalizzazioni realizzate dagli integratori, la rivendita di prodotti con il proprio marchio. L'art. 3 dello schema consente alle autorità nazionali di adottare linee guida nei limiti e per le finalità del regolamento.

Si chiede che l'Agenzia adotti, previa consultazione pubblica e in coerenza con gli orientamenti europei, indicazioni operative per le micro e piccole imprese, con esempi concreti relativi ai gestionali, ai sistemi di gestione dei contenuti, agli impianti e alle configurazioni. Sarebbe utile chiarire, in particolare, che l'impiego delle estensioni e delle configurazioni previste e documentate dal fabbricante originario costituisce un elemento rilevante nella valutazione circa la natura sostanziale della modifica.

Un'esigenza analoga riguarda i rivenditori e i fornitori di servizi gestiti che commercializzano apparati o *software* realizzati da altri. Servirebbero esempi che distinguano tre ipotesi: l'immissione sul mercato con il proprio nome o marchio, che comporta gli obblighi del fabbricante indipendentemente da modifiche tecniche; la semplice personalizzazione senza modifica

sostanziale; la modifica sostanziale, che comporta gli obblighi del fabbricante secondo le regole degli artt. 21 e 22 del regolamento. Esempi operativi su queste fattispecie consentirebbero alle imprese di valutare consapevolmente i propri modelli commerciali.

Per i profili di sicurezza comuni al regolamento e alla disciplina sulla protezione dei dati personali, le indicazioni dovrebbero essere elaborate in raccordo con il Garante per la protezione dei dati personali, nelle rispettive competenze, valorizzando la collaborazione prevista dall'art. 52, paragrafo 7, del regolamento e dall'art. 13 dello schema. Sarebbe utile chiarire quali evidenze già disponibili sulle misure di sicurezza adottate ai sensi degli articoli 25 e 32 del regolamento (UE) 2016/679 possano essere riutilizzate nella documentazione tecnica, se pertinenti al prodotto, e quali integrazioni siano necessarie, senza modificare i requisiti né le procedure di valutazione della conformità. Tali indicazioni dovrebbero essere rese disponibili anche attraverso il canale dedicato dell'art. 18.

Analoghe indicazioni potrebbero accompagnare la transizione dei requisiti di cibersicurezza delle apparecchiature radio verso il nuovo regime e il raccordo tra il regolamento e la disciplina delle macchine, che continuano ad applicarsi congiuntamente, favorendo il riutilizzo della documentazione già predisposta. Potrebbero infine orientare le stazioni appaltanti verso un'applicazione proporzionata dei requisiti del regolamento negli appalti pubblici.

7. Attuazione, consultazione e monitoraggio

Dall'analisi di impatto risulta che non si è svolta una consultazione pubblica e che sono stati utilizzati dati già nella disponibilità dell'Agenzia. L'analisi non contiene stime del numero delle imprese italiane interessate né dei costi di adeguamento. Lo schema rinvia inoltre a numerosi atti attuativi, per la maggior parte privi di termine.

Si chiede che il parere preveda un cronoprogramma degli atti attuativi e una consultazione pubblica, con termini definiti, sugli atti generali che incidono direttamente su obblighi, costi, accesso ai servizi e procedure delle imprese, assicurando la partecipazione delle associazioni di categoria. Si propone altresì che la relazione annuale dell'Agenzia al Parlamento contenga una sezione dedicata alle micro e piccole imprese, con dati sui servizi di assistenza resi, sulle notifiche ricevute e sulle sanzioni irrogate.

Nel regolamento previsto dall'art. 10, comma 3 per le attività dell'Agenzia e, per le autorità del settore finanziario, nei protocolli dell'art. 11, si chiede di precisare le modalità di coordinamento delle attività svolte con la collaborazione della Guardia di finanza, garantendo le competenze tecniche necessarie e mantenendo in capo all'autorità competente la responsabilità delle

valutazioni e dei provvedimenti di vigilanza. Il raccordo con le altre autorità dovrebbe essere assicurato attraverso gli accordi dell'art. 12, nei rispettivi ambiti. La programmazione e lo svolgimento delle verifiche dovrebbero seguire criteri basati sul rischio, con richieste documentali proporzionate all'oggetto dell'accertamento e coordinate tra i soggetti coinvolti, assicurando controlli efficaci anche sui prodotti in ingresso nel mercato dell'Unione e commercializzati *online*.

Quanto all'art. 14, si chiede che il decreto del direttore generale dell'Agenzia previsto dai commi 2 e 4 sia adottato previa consultazione e preveda, per le segnalazioni dei consumatori al CSIRT Italia di cui al comma 4, modalità coerenti con le prassi di divulgazione coordinata delle vulnerabilità, con una verifica tempestiva di attendibilità tecnica che non ritardi l'informazione del fabbricante, affinché questi possa fornire elementi utili e predisporre le misure correttive, ferme le limitazioni alla comunicazione previste dalla normativa applicabile e, per le notifiche volontarie, quanto previsto dall'art. 15, paragrafo 4, del regolamento. Per i reclami trasmessi tra autorità ai sensi del comma 3, si auspica un coordinamento istruttorio che eviti richieste duplicate alla medesima impresa.

Si chiede inoltre che l'art. 27 assicuri espressamente, fin dall'entrata in vigore del decreto, la tutela delle informazioni commerciali riservate, dei segreti commerciali e dei diritti di proprietà intellettuale, compreso il codice sorgente, in coerenza con l'art. 63 del regolamento. Gli accordi e i protocolli dovrebbero prevedere accessi commisurati alle funzioni esercitate, misure di sicurezza e tracciabilità degli scambi, ferme le comunicazioni e le divulgazioni dovute secondo la normativa applicabile.

Si segnala, infine, un profilo puntuale. L'art. 23 inserisce il regolamento tra le materie oggetto di azioni rappresentative a tutela dei consumatori senza indicarne la decorrenza, mentre il regolamento la fissa all'11 dicembre 2027 (considerando 124 e art. 71, paragrafo 2). Si suggerisce di precisare che l'inserimento produce effetti da tale data.

8. Ulteriori suggerimenti e posizioni da sostenere in sede europea

Alcune criticità non possono essere risolte dal decreto legislativo, ma richiedono un'iniziativa del Governo nelle sedi europee. Confartigianato e CNA auspicano che il parere inviti il Governo a sostenere: un trattamento specifico per il *software* realizzato su misura per clienti professionali, ulteriore rispetto alle deroghe puntuali già previste; ove non ancora intervenuta, la rapida adozione del modello semplificato di documentazione tecnica per micro e piccole imprese previsto dall'art. 33, paragrafo 5, del regolamento; l'istituzione e l'operatività dei programmi volontari di attestazione di sicurezza del *software open source* previsti dall'art. 25, e il riconoscimento di tali attestazioni

come elemento utile alla dovuta diligenza di chi integra i componenti; clausole contrattuali tipo per i rapporti relativi ai componenti di terzi integrati nei prodotti e ai servizi *cloud* da cui dipende il loro funzionamento, sui quali le piccole imprese sono chiamate a esercitare la dovuta diligenza senza disporre di potere negoziale.

Merita attenzione, infine, il *software* libero e *open source*, che molte piccole imprese sviluppano, distribuiscono o mantengono per conto dei clienti. Il regolamento lo esclude dagli obblighi quando è fornito al di fuori di un'attività commerciale e prevede un regime attenuato per i gestori di *software open source*. Pur in presenza dei criteri indicati dal regolamento, l'applicazione di questi confini resta incerta per le realtà di minori dimensioni, ad esempio quando una microimpresa o una cooperativa offre assistenza a prezzo di costo su un progetto libero. Allo stesso modo, secondo gli orientamenti europei non rientra nella nozione di *software* libero quello il cui codice sorgente è messo a disposizione dei soli clienti paganti, con effetti da valutare su modelli di distribuzione molto diffusi. Si auspica che il Governo promuova in sede europea esempi e chiarimenti su questi aspetti, perché l'incertezza non scoraggi la partecipazione delle piccole imprese all'ecosistema *open source*.