Il nuovo Cybersecurity Act (CSA2)
Position paper di Confartigianato Imprese

Confartigianato Imprese accoglie l'obiettivo della Commissione europea di rafforzare le norme di cui al Cybersecurity Act - Regolamento (EU) 2019/881- soprattutto in tema di *governance* e attuazione degli strumenti ivi previsti.
In linea con gli obiettivi specifici della proposta per un "secondo" Cybersecurity Act (CSA2), si riconosce infatti la necessità di **rivedere il quadro normativo** soprattutto per ridurne la **frammentazione** e **aumentare l'effettività del Quadro europeo per la certificazione della cibersicurezza**. Inoltre, la revisione sarà altresì fondamentale per **adattare le regole alle concrete esigenze degli operatori economici**, rappresentando così una cruciale opportunità per allinearle alle **esigenze delle micro e PMI (MPMI)**, coinvolte nella catena del valore.
Accanto alla necessità di alcuni aggiustamenti strutturali, riscontrata anche in altre normative in materia digitale, occorre infatti che il CSA2 sia finalmente in grado di avvicinare le MPMI alle questioni di cibersicurezza, attraverso **regole più coerenti e proporzionate,** capaci di incentivarle ad affrontare tali sfide e contribuire così ad elevati livelli di protezione delle imprese e dei cittadini in Europa.

1. Le MPMI nelle catene del valore: il c.d. *liability dumping*

Così come già sottolineato nell'ambito dei lavori sul c.d. Omnibus digitale[1], Confartigianato Imprese evidenzia la sempre più preoccupante tendenza da parte delle grandi imprese di trasferire obblighi di *compliance* di cui alla normativa digitale europea (non solo in materia di cibersicurezza) sui fornitori più piccoli. La clausola '*as (it) is*' ne è la dimostrazione: inserita nei contratti di licenza per i software, essa esonera di fatto il fornitore dalle responsabilità connesse alla vulnerabilità del prodotto, il quale viene venduto appunto '*così com'è*'.
Il c.d. *liability dumping* mette a rischio la sostenibilità giuridico-economica delle MPMI, sobbarcandole di oneri che esulano dalla loro posizione nella catena del valore e dunque dalle loro effettive capacità di intervento. Coerentemente con il principio secondo cui le responsabilità devono seguire il controllo, servono pertanto disposizioni che limitino l'indebito trasferimento di responsabilità, soprattutto in relazione a prodotti digitali critici. In tal senso, un buon punto di partenza sarebbe l'adozione di alcune misure di salvaguardia già nel futuro CSA2, in particolare nel Titolo IV della proposta, dedicato alla sicurezza delle catene di approvvigionamento ICT. Ad esempio, auspichiamo che tra le misure di cui all'art. 103 della proposta (v. par. 2, lett. e), si possa includere anche un divieto di clausole del tipo '*as (it) is*' per i contratti aventi ad oggetto processi, servizi o prodotti ICT con un rischio

[1] Osservazioni di Confartigianato Imprese sul c.d. Pacchetto Digitale, 22 gennaio 2026 (link).

classificato – ai sensi dell'art. 82 - come alto o sostanziale. Più in generale, si potrebbe affidare il compito di monitorare le pratiche di *liability dumping* alle autorità di contrasto che gli Stati membri dovranno designare in virtù dell'art. 112.

2. Gli schemi di certificazione: necessità di maggiore proporzionalità

Allo stato, il Quadro europeo per la certificazione della cibersicurezza (ECCF) si ispira ad un approccio '*one size fits all'*, rendendolo di fatto inaccessibile agli operatori più piccoli. Assoggettare tutte le imprese allo stesso livello di oneri per la certificazione di cibersicurezza costituisce anzitutto un rischio per l'effettività dello stesso ECCF: costi elevati scoraggiano le MPMI dalla certificazione, compromettendo in generale gli elevati livelli di tutela che la normativa in questione intende raggiungere. A differenza degli standard internazionali, anch'essi ancorati ad un approccio unitario per tutti i tipi di operatori economici (es. ISO/IEC 27001), l'ECCF dovrebbe includere schemi proporzionali, modellati rispetto alle dimensioni aziendali e alle variabili di rischio di cui all'art. 82, nonché interoperabili, in grado cioè di certificare la *compliance* rispetto alle diverse normative di settore.

Oltre a quanto già previsto nella proposta (ad es. artt. 78 e 83), al fine di creare uno schema di certificazione realmente accessibile alle MPMI, si potrebbe prevedere l'individuazione di un elenco di componenti software – inclusi componenti open source – che la Commissione europea o ENISA, previo audit, riconosce come "*trusted*". L'utilizzo di tali componenti da parte delle MPMI potrebbe comportare una presunzione di conformità rispetto ad alcuni requisiti tecnici previsti dagli schemi di certificazione europei. Ciò consentirebbe alle piccole imprese che integrano tali componenti nei propri prodotti, processi o servizi ICT classificati a rischio "*basic*" di accedere a procedure di certificazione semplificate, riducendo gli oneri amministrativi e di valutazione.

In ogni caso, Confartigianato Imprese apprezza la clausola di riconoscimento automatico di cui all'art. 71, par. 4, in quanto previene la frammentazione all'interno del mercato unico (v. anche *infra*).

3. Un quadro europeo sulle competenze di cibersicurezza: un'opportunità per la mobilità dei talenti

La capillare presenza di MPMI nelle catene del valore di riferimento rende centrale la questione del consolidamento delle loro competenze in materia di cibersicurezza. In questo contesto, il rafforzamento del quadro previsto dalla proposta di CSA2 e il ruolo dell'ENISA offrono un'opportunità per sviluppare ulteriormente un riferimento comune sulle competenze nel settore a livello europeo.

Partendo da ciò che già esiste, vale a dire l'*e-Competence Framework* (e-CF), occorre implementare norme tecniche adeguate e aggiornate rispetto alle esigenze delle imprese e al livello di specializzazione nel mercato del lavoro. In Italia, infatti, dal Quadro europeo citato è stata sviluppata la norma multiparte UNI 11621: in particolare, la norma UNI 11621-1 contiene la metodologia su *come* costruire profili professionali basati su e-CF; coerentemente, le norme UNI 11621-2,3,4, 5, 6, 7 descrivono rispettivamente i profili ICT generali, i profili Web, i profili sulla sicurezza informativa, i profili di informatica geografica, i profili legati alle misurazioni IT e, infine, i profili per la transizione digitale. Tra queste ultime, la norma UNI 11621-4 è appunto dedicata ai ruoli della c*ybersecurity* (16 profili), come il *Chief information security officer (C*ISO) o *l'Incident Manager*.

A nostro avviso, tale norma dovrebbe costituire il punto di riferimento per effettuare lo stesso esercizio a livello europeo: serve infatti maggiore concretezza nella descrizione delle competenze legate alla cibersicurezza, per incoraggiare la mobilità dei talenti e agevolare l'accesso ai mercati e ai programmi europei.
Affinché l'iniziativa sia efficace, è tuttavia importante che segua un approccio realmente armonizzatore, in linea con le esigenze dei portatori di interesse (che andranno necessariamente consultati sul punto: v. anche *infra*). Il confronto con gli Stati membri di cui all'art. 20, par. 5, della proposta di CSA2 deve garantire l'uniformità e la comparabilità delle competenze. Esperienze precedenti[2] mostrano infatti che adattamenti nazionali possono ridurre sensibilmente l'effettiva armonizzazione, compromettendone gli impatti positivi sul mercato unico.

4. Una *governance* semplice e inclusiva per le MPMI

Le MPMI rappresentano la stragrande maggioranza delle imprese europee e sono al contempo tra gli attori più vulnerabili di fronte alle minacce informatiche, pur essendo spesso utenti chiave di *software* e servizi digitali certificati. Per questo motivo, è essenziale garantire un pieno ed effettivo coinvolgimento delle MPMI nella – complessa - *governance* di ENISA, in modo da far emergere le specifiche esigenze di queste imprese nella definizione di schemi di certificazione, linee guida operative e supporto tecnico. In questo senso, apprezziamo il riferimento alle MPMI all'art. 35 (*Advisory Board*) e art. 69 (Cooperazione con i portatori di interesse) della proposta.
L'inclusione delle MPMI andrebbe poi assicurata anche nella definizione di quegli strumenti che l'ENISA dovrà adottare per l'attuazione della normativa. In particolare, nell'elaborazione delle specifiche tecniche comuni o nell'attività di supporto agli enti normatori di cui al Regolamento UE 1025/2012 (v. art. 18 della proposta), i procedimenti dell'Agenzia dovranno sistematicamente coinvolgere i rilevanti *stakeholder*, scongiurando in particolare il pericolo che le norme tecniche siano adattate esclusivamente alle esigenze delle grandi imprese. In questo contesto, occorrerà prevedere appositi meccanismi di rimborso per gli esperti di norme tecniche per le MPMI, nonché ogni altro strumento utile a rendere effettiva la possibilità per i rappresentanti delle piccole imprese di prendere parte ai lavori legati alla normazione.

19 marzo 2026

[2] La *European Digital Competence Framework* (DigComp), ad esempio, è ancora insufficiente per uniformare i livelli di competenze digitali e garantire quindi una più intensa circolazione di lavoratori specializzati all'interno del mercato unico europeo. In Italia esistono le Linee guida per le competenze digitali dell'Agenzia per l'Italia Digitale (link), che però non sono necessariamente sovrapponibili a quelle degli altri Stati membri europei.