FEDERAZIONE AZIENDE ITALIANE PER L'AEROSPAZIO, LA DIFESA E LA SICUREZZA

Position Paper sul Decreto Legislativo di recepimento della Direttiva NIS2 (AG 164)

AIAD – Federazione Industrie Aerospazio Difesa e Sicurezza

Comitato Cyber

Premessa

Aiad, Federazione Industrie Aerospazio Difesa e Sicurezza, raccoglie al suo interno 37 aziende su un totale di 212 associati, che sono impegnate nell'ambito della cybersecurity, sia come produttori di tecnologia proprietaria che come detentori di competenze su tecnologie altrui che consentono di erogare attività di servizi a vantaggio di terzi. Queste aziende danno vita ad un apposito "Comitato Cyber" che ha lo scopo di aumentare il livello di dibattito e raccordo in tema di cyber all'interno dell'associazione e di rappresentare all'esterno, in raccordo e condivisione con la Presidenza e la Segreteria Generale, le posizione della Federazione sul tema della Cybersecurity a 360 gradi. Sebbene AIAD aggreghi principalmente aziende del comparto Difesa, è necessario sottolineare come la gran parte dell'offerta di beni e servizi nel mercato civile provenga proprio dall'insieme delle aziende che aderiscono al Comitato Cyber di AIAD. Ciò posiziona AIAD come realtà maggiormente rappresentativa dell'industria nazionale della sicurezza informatica.

In questa ottica AIAD sostiene l'attuazione della direttiva NIS2 e ritiene positivo l'elevato grado di normazione sul tema da parte dell'Unione Europea e delle istituzioni degli stati membri, promuove politiche di sostegno all'impresa e ribadisce la volontà di contribuire all'autonomia strategica e tecnologica del Paese e dell'Unione Europea, ribadendo la validità degli intendimenti condivisi dagli Stati Membri nel documento "Bussola Strategica".

1) **Tavolo per l'attuazione della Direttiva NIS (art. 12) –** E' necessario prevedere, anche in una configurazione apposita e distinta del tavolo, la partecipazione allo stesso del comparto industriale fornitore di prodotti e servizi atti all'implementazione delle misure di sicurezza di cui all'articolo 24 (Articolo 21 comma 2 della Direttiva). Tale coinvolgimento potrà avvenire attraverso la partecipazione al tavolo delle associazioni datoriali maggiormente rappresentative dei soggetti che forniscono ai soggetti essenziali e importanti soluzioni e prodotti necessari a rendere operative le misure di sicurezza previste nella direttiva. La presenza dei soggetti industriali all'interno del tavolo è utile al fine di attivare uno scambio continuo di informazioni tra l'autorità NIS ed i soggetti che sono chiamati a fornire soluzioni ai soggetti essenziali ed importanti. Attraverso il confronto con l'industria dei fornitori, infatti, sarà possibile monitorare l'effettivo andamento applicativo della normativa, osservare l'impatto che essa ha nel mercato della cybersecurity in Italia ed acquisire informazioni sia sotto il profilo della risposta che i soggetti NIS daranno alle norme in relazione all'aumento delle capacità di investimento sia sotto il profilo delle potenziali azioni di miglioramento e resilienza che i soggetti attuatori potranno assumere per correggere eventuali criticità che dovessero manifestarsi.

Proposta di condizione per il parere:

All'articolo 12 si preveda la partecipazione dell'industria al Tavolo per l'attuazione della Direttiva NIS, attraverso il coinvolgimento delle associazioni datoriali maggiormente rappresentative delle imprese che producono beni e forniscono servizi di cybersicurezza.

2) **Specifiche tecniche tecnologiche (artt. 24, 31, 40) –** La LEGGE 21 febbraio 2024, n. 15 Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2022-2023**,** individua – tra i principi direttivi cui il Governo deve attenersi per l'emanazione della legislazione – uno specifico punto all'art. 3, comma 1 lettera h*): in relazione alle misure di cui all'articolo 21, paragrafo 2, della direttiva (UE) 2022/2555, prevedere l'individuazione, attraverso l'utilizzo di strumenti flessibili atti a corrispondere al rapido sviluppo tecnologico, delle tecnologie necessarie ad assicurare l'effettiva attivazione delle misure stesse. L'autorità amministrativa individuata come responsabile di tale procedimento provvede altresì all'aggiornamento degli strumenti adottati*. Tale principio direttivo è recepito in maniera poco chiara nel testo del DLGS di recepimento. All'art.28, si stabilisce che l'ACN "promuove" l'armonizzazione delle misure di sicurezza "senza imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia" attraverso un "elenco" (comma 3) che avrà carattere "non vincolante e non esaustivo". Tale formulazione appare troppo morbida ed è ritenuta poco incisiva nell'indicare chiaramente ai soggetti NIS2 cosa debbano fare e di cosa debbano dotarsi affinché si ritenga adempiuta ciascuna delle misure di sicurezza di cui all'articolo 24. Comprendiamo la volontà dell'Agenzia di adottare il principio della "neutralità tecnologica" e di evitare che una disposizione possa essere interpretata come una lesione della libera concorrenza. Tuttavia riteniamo che la previsione normativa possa essere migliorata, senza per questo urtare con i principi di fairness del mercato. In particolare sarebbe opportuno evitare l'utilizzo del termine "promuove" (che risulta ambiguo, interpretabile ad esempio come mera "possibilità" e non come azione che certamente deve essere messa in campo da ACN) da sostituirsi con una espressione più netta (ad esempio "adotta un provvedimento"). E' inoltre necessario specificare che si tratta di un provvedimento che sarà senza meno adottato e che non rimane invece come eventualità (ad esempio disponendo che il provvedimento è adottato in sede di prima applicazione "entro" un termine perentorio). E' infine indispensabile specificare che, sebbene il provvedimento sia "non esaustivo" o "non vincolante", l'adeguamento dei soggetti NIS2 delle tecnologie / pratiche / soluzioni, individuate nello stesso assicura la compliance con la direttiva. Ciò, pur non escludendo che la compliance possa essere conseguita in altri modi, fornisce almeno un quadro di riferimento di certezza minima ai soggetti che devono adeguarsi chiarendo ciò che - sicuramente- conduce alla compliance.

Sul tema intervengono poi anche le norme di cui all'articolo 31, commi 1, 4 e 5 e all'articolo 32. In particolare si stabilisce che l'ACN stabilisce obblighi di varia natura e con diverse finalità. Non è però chiaro se l'ACN avrà una mera "facoltà" di stabilire tali obblighi oppure se è da attendersi che con certezza arriverà una disposizione in tal senso. In particolare, nei casi di linee guida e raccomandazioni di cui ai commi 4 e 5 dell'articolo 31 è chiaramente specificato che si tratta di una possibilità e non di qualcosa che con certezza avverrà.

A tal fine riteniamo che sia più appropriato ricondurre tutte le attività di indicazione di specifiche tecnologie "abilitanti" a provvedimenti che l'ACN dovrà certamente adottare e non a quelli che rimangono nel campo dell'eventualità, cosa che potrebbe far rimanere i soggetti NIS2 nell'ambito dell'incertezza.
Riteniamo che una scelta di questo tipo sia maggiormente aderente al principio legislativo di delega e ne soddisfi al meglio lo spirito, fornendo ai soggetti che devono adeguarsi un quadro più certo degli adempimenti ed alle industrie fornitrici di beni e servizi un quadro più efficiente per la propria programmazione degli investimenti.

Proposta di condizione per il parere:

Al fine di una più facile comprensione delle misure da adottare da parte dei soggetti inclusi nel perimetro della Direttiva, i poteri dell'ACN di cui agli articoli 28, 31 commi 1, 4 e 5, 32, devono essere ricondotti ad un unico provvedimento; è necessario che sia stabilito il termine entro cui l'ACN emani detto provvedimento in sede di prima applicazione, ferma restando la possibilità di modificarlo, aggiornarlo ed adeguarlo ogni qual volta lo si ritenga necessario. Il provvedimento, pur mantenendo il principio di neutralità tecnologica, deve indicare con chiarezza le soluzioni minime di cui i soggetti devono dotarsi al fine di essere considerati compliant alle misure di sicurezza, ciò al fine di rendere il Decreto Legislativo maggiormente aderente al principio di delega di cui all'articolo 3 comma 1 lettera h) della Legge di Delegazione Europea che, con l'attuale formulazione legislativa proposta, non è adeguatamente recepito.

3) **Autonomia strategica –** Anche alla luce delle disposizioni di cui al DDL Cybersicurezza che ha disposto un indistinto criterio di premialità per le tecnologie italiane, UE, dei Paesi aderenti alla NATO e dei Paesi che hanno un accordo in materia di Cybersicurezza con UE e NATO, che finisce per penalizzare le industrie nazionali che investono su tecnologia proprietaria, è necessario più che mai un intervento che sostenga l'ambizione al conseguimento della autonomia strategica e tecnologica nazionale ed europea. In particolare è necessario contrastare la minaccia della "Supply Chain Compromise of Software depencency", che l'ENISA ha censito al primo posto tra le Foresight Cybersecurity Threats 2030, in particolare per quanto riguarda la resilienza cibernetica delle entità critiche individuate ai sensi della Direttiva UE 2557. In particolare riteniamo che, fermo restando la libertà di concorrenza ed il principio di non discriminazione ed il rispetto dei principi dell'UE e dei trattati del WTO, sia assolutamente necessario individuare un sistema che assicuri la sovranità sulla tecnologia di sicurezza che presidiano alla resilienza delle entità critiche. In questa ottica proponiamo che si stabilisca una norma di "backup sovrano", prevedendo che – per l'attuazione delle misure di sicurezza di cui all'articolo 24 – i soggetti di cui alla direttiva CER che adottano tecnologia o servizi forniti da soggetti extra UE, acquisiscano anche la disponibilità di una tecnologia o di un servizio fornito da entità che hanno la sede legale, il management e gli asset all'interno dell'UE e che non siano soggetti a giurisdizioni di Paesi extra UE nell'ambito di quanto attiene alla fornitura di beni o servizi, anche in cloud, che assicurano la sicurezza cibernetica di entità critiche.

Proposta di condizione per il parere:

All' articolo 24 si aggiunga un ulteriore comma che preveda che, almeno i soggetti altamente critici e comunque quelli di cui alla direttiva 2022/2557, nel caso adempiano alle misure di sicurezza previste dall'articolo 21 della Direttiva 2022/2555 attraverso l'utilizzo di tecnologie di proprietà di entità extra UE o servizi gestiti da aziende extra UE, si dotino anche di una analoga tecnologia, che siano certificati nell'ambito dei sistemi europei di certificazione della cybersicurezza di cui all'articolo 49 del regolamento (UE) 2019/881, di proprietà di entità UE non controllata da una entità extra UE ovvero di analogo servizio gestito da entità UE non controllata da una entità extra UE, al fine di assicurare la sicurezza della supply chain e di rispondere alla minaccia individuata alla Priorità 1 di cui al paragrafo 4 del Foresight Cybersecurity Treaths for 2030 Update 2024 dell'European Network Information Security Agency (*Supply Chain Compromise of Software Dependencies).*

4) **Risorse finanziarie per la PA, sostegno ai privati.** Come già previsto dal DDL Cybersicurezza, anche il DLGS di recepimento della Direttiva NIS2 contiene una clausola di invarianza finanziaria. In questo caso vi sono alcune attività (artt. 10, 11, 13 e 15) per i quali viene prevista una spesa aggiuntiva, ma si tratta di "metacosti", vale a dire di spese che dovranno essere fronteggiate per garantire la funzionalità delle strutture centrali preposte all'esecuzione della Direttiva. Non vi sono risorse né per le PA, né per i soggetti privati che dovranno adeguarsi alla direttiva. Sostanzialmente tutti i soggetti interessati dovranno "far da se", ritagliando le notevoli risorse necessarie agli adempimenti di cui agli articoli 24 e 25, nonché i costi di formazione, all'interno dei budget già esistenti. E' chiaro che, se la previsione verrà mantenuta così, non vi saranno particolari azioni di adeguamento nel concreto e tutti i soggetti NIS2 vivranno tale normativa con l'unico intendimento di evitare, possibilmente a costo zero, le sanzioni. Ciò tradisce lo spirito della normativa, spostando il tema dalla Cyber-Security alla Paper-Security, vale a dire alla costruzione di documentazioni atte ad attestare che le disposizioni sono state rispettate. Pur comprendendo la difficoltà dettata dalla non corrispondenza temporale tra il recepimento della NIS2 e la deliberazione della sessione di bilancio, è necessario rimarcare la necessità di addivenire sin dal prossimo anno all'attuazione di quanto previsto a pag. 12 della Strategia di Sicurezza Nazionale Cibernetica tutt'ora vigente, che prevede lo stanziamento di risorse pubbliche pari all'1,2% del totale degli investimenti pubblici lordi, per un totale che -ai dati odierni- si attesterebbe intorno ai 2.3 miliardi di euro all'anno. Ad oggi l'intero mercato della Cybersecurity si attesta ad una cifra inferiore, nonostante in tale dato convergano sia la spesa pubblica che quella dei privati. Si tratta, in sostanza, di raddoppiare il mercato con una iniezione di liquidità fortemente orientata non già a sostenere gli investimenti (che le aziende possono sobbarcarsi, in presenza di nuove opportunità di business) ma tese a stimolare la domanda. In particolare è necessario introdurre un sistema efficace di incentivo per l'acquisto di soluzioni (beni e servizi) finalizzate al rispetto delle norme di cui all'art. 24. Ad oggi e solo in minima parte, tali necessità possono trovare risposta nell'incentivo "Industria 4.0", con una serie evidente di limiti: a) l'incentivo sostiene l'acquisto principalmente di beni ICT e non di servizi; b) il credito d'imposta è minimo e con massimali molto bassi; c) la struttura del credito d'imposta non è fruibile da tutti ma solo dai soggetti che hanno contabilità basata su bilancio e costi/ricavi; d) il credito d'imposta, non oggetto di sconto in fattura, non determina una diminuzione dei costi di approvvigionamento ma solo un recupero minimo e

spalmato nel tempo di una parte delle risorse impiegate per l'acquisto e solo in presenza di costi fiscali compensabili. E' quindi necessario prendere atto che ad oggi i soggetti NIS2 non hanno a disposizione strumenti di sostegno agli acquisti e che non esiste una politica industriale mirata a stimolare la domanda. Una delle opzioni, anche al fine di evitare storture e comportamenti non in linea con le norme, potrebbe essere quella di fornire a talune categorie di soggetti, non già un incentivo, ma direttamente una tecnologia o soluzione (contrattualizzata a monte dallo Stato attraverso gli strumenti di procurement centralizzato disponibile) che sia almeno sufficiente a dichiarare adempiuta ciascuna delle misure di sicurezza di cui all'art.24.

Proposta di condizioni per il parere

Attraverso un articolo aggiuntivo si disponga che tutti i beni e servizi acquistati dalle imprese al fine di ottenere la compliance alla Direttiva NIS2 siano considerati, senza ulteriori o maggiori oneri per la finanza pubblica, come parte della categoria "cybersecurity" di cui all'allegato B della Legge 11 Dicembre 2016 n.232 nonché di quelli al n.19 dell'allegato al Decreto interministeriale 25 gennaio 2016 (beni strumentali – Nuova Sabatini)

Attraverso un articolo aggiuntivo si preveda la possibilità che le autorità di settore, di concerto con ACN, anche attraverso i centri di competenza di cui al decreto 12 settembre 2017, n. 214 (Regolamento sulle modalità di costituzione e sulle forme di finanziamento di centri di competenza ad alta specializzazione, nel quadro degli interventi connessi al Piano nazionale industria 4.0, in attuazione dell'articolo 1, comma 115, della legge 11 dicembre 2016, n. 232) ovvero attraverso le centrali di committenza procedano ad acquisti centralizzati di software, prodotti informatici o servizi atti a determinare la compliance con la Direttiva NIS2, da mettere a disposizione gratuitamente di specifici settori o categorie di entità particolarmente svantaggiate ovvero afflitte da scarsa propensione all'innovazione.

5) **Legittimità delle attività cyber condotte da soggetti privati.** Poiché la Legge di Delegazione Europea dispone delega ad intervenire anche in materia penale, è necessario utilizzare tale facoltà stabilendo che lo svolgimento di attività di cybersecurity finalizzate al rispetto delle misure di cui all'art.24, costituisce attività legittima e pertanto non può mai dare vita alla fattispecie di cui al novellato art. 635 del Codice Penale. Tale intervento si rende necessario poiché le modifiche apportate dal DDL Cybersecurity a detto articolo potrebbero determinare una interpretazione ambigua o non chiara della norma, dalla quale si potrebbe desumere che talune specifiche attività (threat intelligence, penetration testing, OSINT) siano ascrivibili al campo dell'illegalità o che comunque mettano in condizione le aziende private di subire un inversione dell'onere della prova a loro carico ove debbano trovarsi a dimostrare la liceità dei propri comportamenti e la non presenza di un "intentum" delittuoso nello svolgere una determinata pratica (che potrebbe aver arrecato un danno ovvero una interruzione di programma informatico ai danni del soggetto malevolo da cui ci si sta difendendo e del quale si intende prevedere la minaccia).

Proposta di condizione per il parere:

All'articolo 24 si aggiunga un ulteriore comma che specifichi che ogni attività o servizio svolti dai soggetti NIS2, ovvero da terzi che siano fornitori dei soggetti NIS2, ai sensi del comma 1, sono considerati leciti e legittimi e non danno, pertanto, corso alle fattispecie di cui all'articolo 635 quater.1 del Codice penale a carico dei soggetti NIS2 o dei loro fornitori. E' altresì considerata legittima, ai sensi del medesimo articolo 635 quater.1 la detenzione, la produzione, la riproduzione, l'importazione, la diffusione, la comunicazione, la consegna o, comunque, la messa in altro modo a disposizione e l'installazione di apparecchiature, dispositivi o programmi informatici necessari per mettere in pratica le misure di cui al comma 1. L'eventuale danno arrecato a terzi, nell'ambito dell'esercizio delle misure di sicurezza di cui al comma 1, non da luogo alla fattispecie di danneggiamento illegittimo di cui all'articolo 635 quater.1 del Codice penale.

<u>Ulteriori chiarificazioni</u>

E' necessario inserire, dopo l'articolo 3 comma 14, una ulteriore norma di coordinamento tra l'applicazione del presente decreto e l'applicazione delle disposizioni del Regolamento (UE) 2022/2554, per i settori diversi da quelli di cui ai numeri 3 e 4 dell'allegato I che rientrano nell'ambito di applicazione del Regolamento (UE) 2022/54.

E' necessario inserire una definizione chiara delle espressioni "organi amministrativi" ed "organi direttivi" di cui all'art. 23, specificando a quali organismi ci si riferisca con ciascuna di queste espressioni, al fine di circoscrivere con chiarezza l'ambito di applicazione della citata disposizione nonché di tutte le altre disposizioni che ad essa si richiamano al fine di individuare il perimetro di riferimento.

Roma, 10 luglio 2024