CONFINDUSTRIA

# Schema di decreto legislativo recante recepimento della Direttiva (UE) 2022/2555 (c.d. NIS 2)

# PRIME OSSERVAZIONI

luglio 2024

La sicurezza informatica è un obiettivo fondamentale dell'Unione europea, che sta proseguendo la sua azione per elevare il livello di cybersecurity nel suo complesso.

Il coordinamento tra Paesi, organizzazioni e soggetti economici, contribuisce a potenziare la resilienza, a migliorare la vigilanza e a rafforzare la nostra risposta collettiva agli attacchi informatici ed è fondamentale per garantire il regolare funzionamento del mercato europeo e assicurare la continuità nell'erogazione dei servizi essenziali forniti dai soggetti che operano nei settori critici.

L'UE sta proseguendo, e intensificando, un percorso normativo a sostegno della sicurezza comune, adottando una serie di misure per ridurre le vulnerabilità e aumentare la resilienza dei soggetti critici, sia per quanto riguarda i rischi informatici che quelli non informatici. In particolare, sono state adottate importanti misure per sviluppare mezzi e capacità di prevenzione, individuazione e risposta rapida alle sempre più numerose minacce cyber e per favorire la sinergia tra gli operatori del settore pubblico e privato in un'azione condivisa verso un obiettivo comune.

In questo contesto si inserisce il processo di revisione della Direttiva sulla sicurezza delle reti e dei sistemi informativi – la c.d. Direttiva NIS (Direttiva UE 2016/1148, recepita nel nostro ordinamento con il d.lgs. 18 maggio 2018, n. 65) – avviato con l'adozione della direttiva (UE) 2022/2555 – c.d. Direttiva NIS 2 – e in fase di recepimento nei singoli Paesi con i vari regolamenti nazionali.

Confindustria, grazie ad un'azione coordinata a livello di Sistema Associativo e all'attività di lobby svolta attraverso la nostra Delegazione a Bruxelles, ha seguito l'iter di approvazione della Direttiva NIS 2, contribuendo attivamente alla sua definizione.

Il nuovo impianto della Direttiva NIS 2 supera e rafforza quanto già previsto dalla precedente direttiva NIS, ampliando anzitutto i settori di applicazione e i soggetti rientranti nel perimetro. La NIS 2, inoltre, appare più funzionale ad assicurare un utilizzo sicuro delle reti e dei sistemi informativi, specialmente riguardo all'operatività delle infrastrutture essenziali del Sistema Paese, siano esse gestite da soggetti pubblici o privati.

**Confindustria condivide l'attuale impostazione dello Schema di Decreto Legislativo di recepimento della Direttiva NIS 2**, approvato in via preliminare dal Consiglio dei ministri il 10 giugno 2024, così come ne condivide i principi che ne sono alla base e sui quali l'Agenzia per la Cybersicurezza Nazionale (ACN) ha fondato l'impianto normativo.

Come riportato nella "Analisi dell'Impatto della Regolamentazione" allegato allo Schema di D.lgs. di recepimento della NIS 2, al fine di una adeguata predisposizione del decreto stesso e per favorirne una corretta attuazione da parte delle organizzazioni, Confindustria ha tempestivamente avviato una proficua interlocuzione con l'ACN per attivare un dialogo tra le imprese ricadenti nei settori NIS 2 e l'ACN stessa, per far emergere eventuali criticità ed elementi da valutare di cui tenerne conto nello svolgimento dell'attività regolamentare.

Confindustria condivide il **criterio di individuazione dei soggetti NIS 2** su base dimensionale (cd. Size-cap rule), che coinvolge tutte le medie e grandi imprese che operano nei settori altamente critici e critici e le piccole e microimprese identificate in base a precisi parametri definiti nello Schema di Decreto di recepimento.

Positivo, inoltre, **l'allargamento del campo di applicazione alle pubbliche amministrazioni**, centrali e locali, di cui agli allegati III e IV allo Schema di decreto.

Si esprime apprezzamento per **il ponderato** utilizzo da parte dell'ACN del **circoscritto "margine di discrezionalità"** nel processo di recepimento della Direttiva; in particolare, si **condivide la piena applicazione** dei **criteri di proporzionalità e di gradualità** degli obblighi, degli adempimenti e delle eventuali sanzioni a carico delle organizzazioni, in base alla dimensione dei soggetti, alla criticità del settore di appartenenza, alle violazioni commesse e al grado di maturità delle organizzazioni sui temi della sicurezza.

Concordiamo con la previsione di istituire in via permanente un **Tavolo per l'attuazione del decreto legislativo di recepimento della NIS 2** con il coinvolgimento di diversi portatori di interesse, tra i cui compiti evidenziamo la possibilità di formulare proposte e pareri per l'adozione di iniziative, linee guida o atti di indirizzo. Si evidenzia inoltre che sarebbe importante prevedere la partecipazione dell'industria al suddetto Tavolo attraverso il coinvolgimento delle associazioni datoriali maggiormente rappresentative delle imprese che producono beni e forniscono servizi di cybersicurezza.

In relazione alla facoltà per ACN di promuovere nei confronti dei soggetti NIS 2 l'uso di determinate **"specifiche tecniche" e tecnologie per la mitigazione dei rischi**, è auspicabile rafforzare la previsione introducendo un termine perentorio anziché la mera possibilità per ACN di adottare tale provvedimento. Sarebbe inoltre importante che tali specifiche tecniche vengano rese note quanto prima, soprattutto a beneficio delle piccole e microimprese che, in virtù della loro bassa maturità digitale, potrebbero necessitare di tempi e risorse rilevanti per adeguarsi agli obblighi richiesti dalla normativa. Al fine di tutelare la sovranità tecnologica e di assicurare la sicurezza della supply chain, si suggerisce di prevedere che, per l'attuazione delle misure di sicurezza, i soggetti altamente critici, qualora utilizzino tecnologie di proprietà di entità extra UE o servizi gestiti da aziende extra UE, si dotino anche di una analoga tecnologia 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.

È inoltre fondamentale agevolare e supportare il **processo di autoidentificazione** delle imprese chiamate a registrarsi su apposita piattaforma resa disponibile dall'ACN, in particolare a sostegno di quelle imprese che per peculiarità produttive non sono immediatamente ascrivibili ad uno dei settori di cui agli allegati I e II allo Schema di decreto di recepimento.

Come poi evidenziato nel documento di Analisi dell'Impatto della Regolamentazione allegato allo Schema di decreto di recepimento, la **responsabilità attuativa dell'intervento**

**normativo** ricade, in via prioritaria, **sull'ACN**, che in relazione alle nuove funzioni ad essa assegnate (monitoraggio e vigilanza sugli adempimenti degli obblighi, analisi e supporto alle imprese, verifica, ispezione e adozione di misure di esecuzione e di irrogazione delle sanzioni), dovrà far fronte ad un significativo incremento della mole di lavoro. Per evitare ritardi nell'implementazione delle nuove norme sia in fase di adozione dei provvedimenti attuativi sia nell'attività di supporto in favore dei soggetti NIS2, **si auspica**, pertanto, **che le dotazioni dell'Agenzia siano adeguate a tale impatto** per fornire, come fatto sinora, il necessario sostegno al tessuto produttivo del Paese in questo ambizioso percorso di potenziamento della sua postura di cybersicurezza.

In vista dell'entrata in vigore in data 17 luglio p.v. della legge 28 giugno 2024, n. 90, recante "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*", sarebbe altresì auspicabile una armonizzazione degli obblighi e delle misure previste nella citata normativa con il Decreto legislativo di recepimento della Direttiva NIS2 anche per evitare una duplicazione/sovrapposizione degli adempimenti in capo ai soggetti vigilati e favorire una interlocuzione univoca con l'Agenzia per la più efficace implementazione delle nuove norme e l'effettivo raggiungimento di un più elevato livello di cybersicurezza del tessuto produttivo italiano.

Parimenti, considerando l'avvio dal 1° agosto 2024 del regime ordinario di qualificazione dei servizi cloud offerti da operatori privati, previsto dal nuovo Regolamento unico per le infrastrutture e i servizi cloud per la PA, sarebbe quanto mai opportuna una armonizzazione del quadro regolatorio vigente al fine di uniformare gli obblighi e le procedure in esso previsti a quanto previsto dal decreto legislativo di recepimento della Direttiva NIS2 e dai suoi successivi provvedimenti attuativi.

Infine, si coglie l'occasione per sottolineare la necessità di garantire degli incentivi alle imprese, ad esempio per l'acquisto dei beni e servizi necessari ad adempiere agli obblighi della Direttiva NIS2 al fine di stimolare la domanda e quindi rafforzare il mercato della Cybersecurity.