NT+ Diritto
Norme & Tributi Plus

Il Sole 24 ORE

Comunitario e Internazionale

Con la direttiva Nis2 ruolo centrale all'Agenzia per la cybersicurezza

Lo schema conferma sostanzialmente la strategia nazionale per la cybersecurity e disciplina gli obblighi di condivisione tra Stati membri delle informazioni

di Oreste Pollicino e Flavia Scarpellini
08 Agosto 2024

Lo schema di decreto legislativo attualmente in discussione per attuare la **direttiva Ue 2555/2022** (cosiddetta Nis2) pone interessanti sfide sia agli operatori, sia alle istituzioni per elevare (e di molto) il livello di cybersecurity nei paesi dell'Unione europea, come da disegno comunitario.

Si tratta di un provvedimento corposo (44 articoli, suddivisi in 6 capi), con qualche rinvio a una ravvicinata normazione di secondo livello (con dpcm o determinazioni dell'autorità), che pone al centro l'Agenzia per la cybersicurezza nazionale (Acn) ai fini della verifica dell'attuazione della Nis2 e della vigilanza (anche sanzionatoria), ferme restando le competenze delle autorità di settore.

A livello di scenario generale, lo schema conferma sostanzialmente la strategia nazionale per la cybersecurity e disciplina gli obblighi di condivisione tra Stati membri delle informazioni sulla cybersicurezza. Quanto ai destinatari, si contraddistingue per il rigore (sanzioni molto elevate e responsabilità degli organi gestori delle imprese) - come da principi Nis2 -, contemperato dalla rilevanza data alla cooperazione (tra imprese, oltre che tra istituzioni) e al "supporto" di guida ai destinatari fornito dall'Acn, entrambi voluti dal legislatore nazionale. Si è data, verosimilmente, rilevanza allo sforzo richiesto, soprattutto alla Pubblica amministrazione e alle piccole-medie imprese, privilegiando la fase di apprendimento.

Resta da interrogarsi, tuttavia, sulla effettiva possibilità per le istituzioni preposte di fare fronte a un'attività di produzione normativa, coordinamento (nazionale e internazionale), vigilanza, supporto, formazione e repressione che forse richiederebbe altri stanziamenti finanziari per potersi dotare delle risorse tecniche e umane necessariamente al top. Del pari, le Pa locali e gli enti pubblici territoriali (già destinatari della, per certi versi, anticipatoria legge 90/2024 che non appare, a oggi, espressamente coordinata con lo schema) potrebbero trovarsi in una situazione analoga.

Lo schema individua l'ambito di applicazione del decreto in primis con riferimento all'attività esercitata, principio che trova il suo temperamento nella dimensione dell'impresa. Infatti, vi rientrano i soggetti, pubblici o privati, dei settori individuati in quattro allegati al decreto.

Per i primi due allegati assume rilevanza (ma vi sono notevoli eccezioni) anche la dimensione dell'impresa (in breve, oltre 50 dipendenti e un fatturato annuo superiore a 10 milioni di euro o un totale bilancio annuo superiore a 43 milioni di euro). Lo schema, tuttavia, introduce un temperamento "tecnico" a tale criterio dimensionale con riferimento ai gruppi di società al fine di escluderne, in determinati casi, l'aggregazione di valori (cosiddetta clausola di salvaguardia, i cui criteri di applicazione saranno individuati con dpcm). Per i restanti due allegati (che includono le categorie di Pa e le ulteriori tipologie di soggetti) non vi è un criterio dimensionale.

Rientrano, inoltre, tra i destinatari della bozza di decreto, indipendentemente dalle loro dimensioni, anche una serie di soggetti (come previsto dalla Nis2) che ricomprendono, si segnala, anche: (a) gli enti che potranno essere identificati dall'Acn, su proposta delle Autorità di settore, nonché (b) le imprese collegate (e questa è una novità) a un soggetto essenziale o importante, ove soddisfino determinati requisiti.

Lo schema riprende poi la distinzione della Nis2 tra soggetti «essenziali» e soggetti «importanti» all'interno dei destinatari del provvedimento, definendo per esclusione quelli importanti.

Tra le sanzioni, notevole è la facoltà dell'Acn di disporre nei confronti delle persone fisiche, ivi inclusi i ceo o il legale rappresentante dei soggetti essenziali e importanti, l'incapacità a svolgere temporaneamente funzioni dirigenziali all'interno dell'ente finché non vengano adottate le misure richieste.

Anche le sanzioni amministrative pecuniarie massime sono molto rilevanti e già di per sé dovrebbero indurre a un'attenta attuazione della normativa da parte dei destinatari. Per la mancata osservanza degli obblighi (i) imposti dall'articolo 23 agli organi di amministrazione e agli organi direttivi (qui potrebbe non sempre risultare agevole

distinguere i diversi organi o aversi un cumulo di responsabilità), nonché (ii) relativi alla gestione del rischio per la sicurezza informatica e alla notifica degli incidenti (articoli 24 e 25), troviamo per i soggetti essenziali (escluse le Pa) sanzioni fino a 10 milioni di euro o al 2% del totale del fatturato annuo su scala mondiale, se tale importo è superiore. Per i soggetti importanti (escluse le Pa), sanzioni fino a 7 milioni di euro o all'1,4% del totale del fatturato annuo su scala mondiale. Per fortuna è stato previsto il mancato cumulo con la sanzione irrogata, per la medesima condotta, dal Garante per la privacy!

Infine, secondo lo schema in esame, l'Acn stabilirà obblighi proporzionati per i destinatari del decreto, tenuto conto del grado di esposizione ai rischi, delle dimensioni dei soggetti e della probabilità che si verifichino incidenti, nonché della loro gravità.

ISSN 2499-1589 - Norme & Tributi Plus Diritto [https://ntplusdiritto.ilsole24ore.com]