ASSOTELECOMUNICAZIONI
ASSTEL

ADERENTE A CONFINDUSTRIA

AUDIZIONE DI ASSOTELECOMUNICAZIONI-ASSTEL

Dott.ssa Marzia Minozzi

su Recepimento della Direttiva NIS 2

---

presso

I Commissione (Affari costituzionali), e IX Commissione (Trasporti, poste e telecomunicazioni)

15 luglio 2024

Asstel è l'associazione aderente a Confindustria che rappresenta la filiera delle telecomunicazioni.

E' costituita dalle imprese delle diverse aree merceologiche che appartengono a tale filiera, tra cui le imprese che gestiscono reti di telecomunicazioni fisse e radio-mobili e servizi digitali accessori, i produttori ed i fornitori di terminali-utente, i produttori ed i fornitori di infrastrutture di rete, di apparati e di servizi software per le telecomunicazioni, i gestori di servizi e di infrastrutture di rete, anche esternalizzati, i gestori di servizi di Customer Relationship Management e di Business Process Outsourcing.

Asstel ha la missione di favorire e promuovere lo sviluppo e la crescita della Filiera, nell'interesse generale del sistema economico-produttivo nazionale, curando la tutela degli interessi delle Imprese associate presso le sedi istituzionali, politiche ed economiche, pubbliche e private e la rappresentanza in materia sindacale e del lavoro delle imprese associate che applicano il CCNL TLC e/o l'Accordo Outbound, supportandole nella gestione delle questioni d'interesse, ivi inclusi il rinnovo e l'applicazione dei relativi contratti collettivi nazionali, curando a livello nazionale l'assistenza e la tutela dei loro interessi in tutti i problemi sindacali e del lavoro che direttamente o indirettamente le riguardano.

Asstel ha quindi fra i suoi associati gli operatori di telecomunicazioni che sono in prima linea per quanto riguarda il ruolo svolto in relazione alla salvaguardia dei requisiti di sicurezza nel contesto emergente con l'estensiva azione di trasformazione digitale di tutti i settori economici e sociali.

Fin dal 2020 Asstel ha un gruppo di lavoro focalizzato sul monitoraggio delle normative emergenti finalizzate al perseguimento della cybersicurezza con impatto sugli obblighi degli operatori di telecomunicazioni.

Il settore delle telecomunicazioni, per il suo ruolo chiave nell'impianto generale dell'economia e della società digitale, è da sempre molto attento a perseguire obiettivi di cybersicurezza per naturali finalità legate alla qualità e alla continuità del servizio offerto ai clienti residenziali, aziende e pubblica amministrazione.

Inoltre, gli operatori di telecomunicazioni sono da tempo soggetti ad obblighi relativi alle misure per la cybersicurezza introdotti da una sequenza di dispositivi normativi europei e

nazionali (inclusi i recepimenti delle Direttive), con impatti sulle aziende e sulla loro supply chain.

Si ricordano:

- Decreto Telco - Decreto 12 dicembre 2018 “Misure di sicurezza ed integrità delle reti di comunicazione elettronica e notifica degli incidenti significativi”
- Golden Power - Decreto Legge 15 marzo 2012, n. 21 “Norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni.”
- PSNC – Perimetro di Sicurezza Nazionale Cibernetica (per i soggetti che vi rientrano per i servizi essenziali) - Decreto Legge 21 settembre 2019, n. 105 “Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.”
- DORA – Regolamento UE 2022/2544 “Digital Operational Resilience Act”
- CER (per i soggetti a cui è applicabile) – Direttiva UE 2022/2557 “Critical Entities Resilience”

Il recepimento della Direttiva NIS 2 si inserisce in un quadro di misure ed adempimenti in essere con l’obiettivo di creare una condizione di resilienza orizzontale omogeneo per l’ambito territoriale dei paesi aderenti all’UE.

Il perseguimento di obiettivi di cybersicurezza si concretizza in una combinazione di misure (necessariamente dinamici e soggetti ad aggiornamento) di natura organizzativa, processiva, tecnica che sono guidate dagli standard internazionali (utilizzati come riferimento dalle aziende e dagli enti normativi) che si fondano su metodiche e processi di analisi e gestione dei rischi e principi di proporzionalità.

I programmi di recepimento di nuove normative critiche che si sviluppano in periodi relativamente brevi, quali quelle relative alla cybersicurezza, debbono essere in grado di inserirsi e di perseguire le finalità attese nella dimensione, nella distribuzione geografica e nella complessità delle strutture che sono realizzate ed esercite dagli operatori di telecomunicazioni, che devono avere un quadro evolutivo certo e compatibile con le dinamiche di mercato.

L’armonizzazione e l’omogeneizzazione delle disposizioni emergenti nel contesto già avviato sono una necessità al fine di corroborare ed aggiornare la postura di presidio della cybersicurezza ed evitare inefficienti sprechi di energie (con duplicazioni o dispersione di sforzi senza incremento o peggio con riduzione del livello di difesa).

Il dialogo continuo e collaborativo (nel rispetto delle disposizioni di riservatezza, ove opportune) con gli enti deputati a redigere la normativa in materia di sicurezza ed a curarne l'applicazione, in particolare con l'ACN, è ritenuto da ASSTEL e dai suoi associati uno strumento essenziale per agevolare il processo di costruzione di un assetto di salvaguardia di cybersicurezza che massimizzi gli obiettivi di sistema paese e comunitari.

Dall'analisi della bozza di testo di recepimento della Direttiva NIS 2 nel gruppo di lavoro per la cybersicurezza di ASSTEL sono emerse le seguenti osservazioni:

- All'art. 3 comma 14 è prevista un'esenzione dall'applicazione della NIS2 per tutti i soggetti che ricadono nel perimetro applicativo del regolamento DORA: in tal modo verrebbero esclusi anche tutti i soggetti che operano come istituti di pagamento in ambito "negative scope" della direttiva sui servizi di pagamento: sembra che tale esenzione sia troppo ampia e andrebbe ricondotta alle "attività" soggette a DORA piuttosto che tout court ai "soggetti" come è attualmente scritto.
- All'art. 8 si prevede la garanzia di trattamento dei dati personali conformemente al GDPR e al decreto legislativo di recepimento; si richiama l'esistenza del REGOLAMENTO (UE) 2018/1725 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 ottobre 2018 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, che sembra altrettanto rilevante ai fini delle attività disciplinate dallo (schema di) decreto legislativo e che quindi forse andrebbe anch'esso citato.
- All'art. 23 dello schema si introducono i termini "organi di amministrazione" e "organi direttivi" di cui si richiede una definizione più dettagliata che evidenzi la differenza tra i due.
- All'allegato 4 si fa riferimento all'attività di ricerca come elemento rilevante per l'applicazione di una serie di disposizioni agli istituti di istruzione: alla luce dell'estrema varietà delle attività classificate come attività di ricerca nel panorama degli istituti di istruzione, potrebbe essere utile specificare le caratteristiche delle attività di ricerca che le rendono rilevanti ai fini della sicurezza.
- In generale, si ritiene utile chiarire il concetto di soggetto essenziale e importante in relazione al servizio. In particolare, chi opera in diversi segmenti di business potrebbe rientrare nella NIS 2 come soggetto essenziale o importante sia per il servizio che rappresenta il core business che per altri sotto-servizi (che potrebbero non essere critici). Questo approccio potrebbe avere implicazioni importanti (oneri aggiuntivi) non strettamente necessarie, anche in relazione all'obiettivo della Direttiva stessa. A questo proposito si potrebbero prevedere delle soglie entro cui il

soggetto possa essere escluso da settori che non rappresentano il suo core business. Va chiarito se il soggetto possa rientrare nella categoria essenziale o importante per ciascuna tipologia di servizio offerto. Questa discriminazione del ruolo del soggetto in relazione al singolo servizio porterebbe già ad una differenziazione degli obblighi per servizio.

Al netto delle osservazioni sopra riportate, lo schema di decreto legislativo in valutazione non solleva particolari criticità o preoccupazioni, che sono semmai rivolte all'armonizzazione dei provvedimenti attuativi che saranno adottati a seguito della direttiva NIS 2 a livello europeo con le disposizioni già vigenti a livello nazionale.

Infatti, la consultazione UE aperta sulla bozza di Regolamento attuativo "Cybersecurity risk management & reporting obligations for digital infrastructure, providers and ICT service managers", sebbene diretta a regolamentare gli obblighi di notifica a carico di fornitori di servizi digitali (*DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers)* propone un approccio "per soglie" all'imposizione di obblighi di notifica che non è immediatamente coerente con quello "qualitativo" (che valorizza l'essenzialità del servizio in questione) adottato dal Perimetro di Sicurezza Nazionale Cibernetica e che, se fosse adottato anche per le attività più direttamente connesse alla fornitura di reti e servizi di comunicazione, potrebbe rischiare – in relazione alle soglie che sarebbero adottate – di ingenerare incertezza e duplicazioni di attività a carico degli Operatori.

Siamo a conoscenza che ACN è consapevole e attiva su questo aspetto e Asstel parteciperà alla Consultazione pubblica per rinforzare la posizione nazionale in merito.