Commissione riunite Affari Costituzionali e Trasporti
Camera dei Deputati

Eni SpA

Memoria sul disegno di legge di conversione del decreto legge n. 105/2019 concernente disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica (AC 2010)

Eni desidera ringraziare le Commissioni riunite Affari Costituzionali e Trasporti della Camera dei Deputati per l'opportunità di presentare un proprio contributo nell'ambito dell'esame parlamentare del disegno di legge di conversione del decreto legge sul perimetro di sicurezza nazionale cibernetica.
Eni giudica positivamente la crescente e condivisa sensibilità su una materia di rilevanza strategica per il Paese e il sistema produttivo e ritiene condivisibile l'impianto complessivo del provvedimento che ha lo scopo di elevare il livello di sicurezza delle reti, di sistemi informativi e servizi informatici necessari allo svolgimento di funzioni o alla prestazione di servizi dalla cui discontinuità possa derivare un pregiudizio alla sicurezza nazionale.

Considerazioni generali

Volendo offrire alle Commissioni riunite elementi puntuali, con l'auspicio che possano essere utili per un esame di dettaglio, di seguito evidenziamo alcuni punti di attenzione, corredati da proposte e osservazioni. In generale, una prima area di attenzione riguarda le norme che intervengono in materia di *procurement*. Infatti, è auspicabile che la normativa sia opportunamente adeguata alla specificità di aziende, come Eni, che per dimensione, eterogeneità di business e presenza internazionale, devono avvalersi di servizi e know-how specialistico che può essere ottenuto in maniera efficace solo attraverso un insieme di prodotti e servizi di fornitori anche esteri. Pertanto, nel regolamento attuativo del decreto dovrebbe essere chiarito l'ambito di applicazione della norma che impone di comunicare al Centro di Valutazione e Certificazione Nazionale (CVCN) l'affidamento di forniture di beni, sistemi e servizi ICT (art. 1 c. 6). In particolare, dovrebbe essere meglio evidenziato se la comunicazione si renda necessaria nei casi in cui la fornitura sia riferita ai fornitori italiani, oppure anche quando sia riferita a fornitori stranieri. In ogni caso, tale disposizione avrebbe un impatto

elevato sui tempi di approvvigionamento, cui si potrebbe ovviare definendo preventivamente una **white list** di servizi, prodotti e aziende affidabili, in modo da non rendere necessaria la comunicazione al MiSE.
Un utile ausilio di adeguamento alla normativa potrebbe essere richiedere all'operatore l'adozione di un ***framework risk based*** di cyber security che copra le aree di sicurezza indicate nel DL (all'art. 1 c. 3b).
Ulteriore aspetto migliorativo potrebbe consistere nell'ampliare la norma ad altri paradigmi tecnologici, in modo particolare ai **servizi *Cloud***, che estendono l'azienda oltre i confini geografici e che sono vitali ai processi di business.

Osservazioni e proposte Eni

Nel prosieguo sono riportate, secondo l'ordine dell'articolato, osservazioni che riteniamo possano agevolare l'applicazione del provvedimento ai contesti organizzativi che costituiranno il perimetro di sicurezza nazionale cibernetica.

Art. 1, c. 1

Viene istituito il **perimetro di sicurezza cibernetica nazionale** che vedrà coinvolti diversi attori, pubblici e privati, da individuare sulla base dei seguenti criteri:

- esercizio di una funzione essenziale dello Stato, ovvero di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato;
- l'esercizio di tale funzione o la prestazione di tale servizio deve dipendere da reti, sistemi informativi e servizi informatici dal cui "*malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio*", possa derivare un pregiudizio per la sicurezza nazionale.

___

Si osserva che i concetti di "malfunzionamento, interruzione o utilizzo improprio" appaiono generici e dovrebbero, quindi, essere meglio precisati, facendo riferimento a quelli di "violazione della riservatezza, integrità e disponibilità".

Art. 1, c. 2

Viene demandata ad un DPCM, da adottare su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR), l'individuazione dei soggetti che saranno inclusi nel perimetro di sicurezza nazionale cibernetica. Con tale DPCM dovranno anche essere definiti i criteri sulla base dei quali tali soggetti dovranno predisporre un elenco delle

reti, dei sistemi informativi e dei servizi informatici di rilevanza per la sicurezza nazionale.
Viene, inoltre, imposto agli operatori di fornire al MiSE informazioni su sistema, servizi e relative architetture e componentistica e che tale elenco debba essere aggiornato con cadenza almeno annuale.

___

Allo scopo di minimizzare gli oneri per gli operatori, appare opportuno che nel DPCM sia specificato il livello di dettaglio delle informazioni richieste e siano esplicitate le modalità di applicabilità ai contesti in cui le reti abbiano estensione geografica extra nazionale.
Inoltre, a vantaggio dell'efficacia e dell'efficienza della comunicazione, potrebbe essere imposto all'operatore di tenere l'elenco aggiornato (specificandone i criteri) da rendere disponibile al MiSE su richiesta.

Art. 1, c. 3

Viene demandata a un DPCM la definizione delle procedure in base alle quali dovranno essere notificati gli **incidenti** con impatti su reti, sistemi informativi e servizi informatici inclusi nel perimetro di sicurezza nazionale cibernetica, e delle misure volte a garantirne **elevati** livelli di sicurezza.

____

Appare opportuno che le procedure di notifica degli incidenti specifichino: modi, tempi e metodi di notifica, dandone una classificazione e richiedendone una segnalazione solo nei casi di particolare rilevanza.
Relativamente alle misure di sicurezza, si osserva che il DPCM debba basarsi su un approccio al rischio, consentendo una flessibilità tale da essere applicabile a contesti eterogenei ed internazionali, ciò in analogia con il criterio sino ad ora seguito dalle vigenti normative Ue (es. direttiva Ue 2016/1148 - NIS, regolamento 2016/679 - GDPR) che pongono a carico degli operatori la responsabilità di valutare ed individuare le misure "adeguate e proporzionate alla gestione dei rischi posti alla sicurezza dei sistemi".
Inoltre, nel definire eventuali tempi di adeguamento, è necessario considerare elementi di flessibilità in ordine alle dimensioni dell'azienda e, nel caso specifico dei contesti industriali, al ciclo di vita e di manutenzione degli impianti.

Art. 1, c. 5

Si prevede che i DPCM che dovranno dettare le misure di sicurezza cui gli operatori dovranno adeguarsi debbano essere aggiornati con cadenza biennale.

———

Allo scopo di evitare un eccessivo appesantimento degli oneri per gli operatori, si auspica che l'intervallo di aggiornamento dei DPCM preveda di considerare elementi di flessibilità in ordine alle dimensioni dell'azienda e dei contesti industriali in cui essa opera.

Art. 1, c. 6

Viene **disciplinato il processo aziendale di approvvigionamento dei servizi e sistemi ICT**. Si demanda a un regolamento l'adozione delle procedure, modalità e termini da rispettare nell'affidamento di forniture di beni, sistemi e servizi ICT destinati ad essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici. Con tale regolamento potranno essere disposte deroghe a tali procedure per i casi in cui sia indispensabile procedere in sede estera.

Delle operazioni di approvvigionamento dovrà essere data comunicazione al Centro di valutazione e certificazione nazionale (CVNV), istituito presso il MiSE, che potrà **imporre condizioni e test di *hardware* e *software***. In tal caso, i bandi di gara e i relativi contratti di affidamento dovranno essere integrati con specifiche clausole sospensive o risolutive.

Inoltre, **si demanda al MiSE la competenza ad effettuare attività di ispezione e verifica** sulle misure di prevenzione dei rischi adottate dai soggetti privati in attuazione della presente normativa.

———

Si evidenzia che la norma introduce disposizioni che avrebbero impatto diretto sui tempi di approvvigionamento dei beni e servizi ICT che in talune circostanze potrebbero portare a un forte rallentamento delle forniture, bloccando l'erogazione di servizi prestati dagli operatori.

Oltre a quanto sottolineato nelle considerazioni generali, è auspicabile l'applicazione di tali casistiche solo a beni e servizi ICT di particolari categorie di operatori che erogando specifici servizi impiegano tecnologie ad alto rischio.

Pertanto, nel regolamento attuativo dovrebbe essere imposta la comunicazione al CVCN solo nei casi di approvvigionamento di specifiche forniture ad alto rischio

(opportunamente definite) e meglio specificata la tipologia di servizi (es. sviluppo/manutenzione di applicativi).
Infine, in coerenza con le finalità di prevenzione della norma, in ottica collaborativa, si propone che siano previste attività di audit sulle misure applicate dagli operatori, precedute da idoneo preavviso (es. 30 giorni) oltre alle eventuali ispezioni previste dalla norma.

Art. 5, c. 1

Viene definita una **procedura d'urgenza in caso di crisi cibernetica**, ossia in presenza di rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi e servizi. Il Presidente del Consiglio dei Ministri, su deliberazione del Comitato interministeriale per la sicurezza della Repubblica, potrà decidere – per il tempo strettamente necessario all'eliminazione dello specifico fattore di rischio - **la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati**.

_____

Tale misura può comportare un significativo impatto sull'erogazione dei servizi operativi dei gruppi societari internazionali che offrono servizi per le proprie società controllate/partecipate in tutto il mondo. Inoltre, sarebbe opportuno considerare il rischio introdotto da vulnerabilità dei sistemi e servizi dell'operatore che, anche se fisicamente dislocati in territorio extra nazionale, quindi di diversa giurisdizione, hanno impatti diretti sull'infrastruttura nazionale.

Conclusioni

Eni crede fermamente nel valore della cooperazione e della collaborazione fra istituzioni e aziende, che risulta fondamentale in un contesto di evoluzione tecnologica e digitalizzazione. Nell'ottica di perseguire e fortificare la cooperazione tra il settore pubblico e quello privato per addivenire a una regolamentazione della materia che sia efficace ed efficiente, Eni apprezza l'opportunità di fornire il proprio contributo, lavorando per realizzare un ecosistema informatico sostenibile e affidabile, continuando e intensificando il costruttivo dialogo con le Istituzioni e con tutti gli *stakeholder*, dialogo che auspichiamo perduri anche nella fase di attuazione del provvedimento.