Ministero dello Sviluppo Economico

UFFICIO LEGISLATIVO

AUDIZIONE DELLA SOTTOSEGRETARIA DI STATO PER LO SVILUPPO ECONOMICO, MIRELLA LIUZZI, NELL'AMBITO DELL'ESAME DEL DISEGNO DI LEGGE C. 2100, DI CONVERSIONE DEL DECRETO–LEGGE 21 SETTEMBRE 2019, N. 105, RECANTE "DISPOSIZIONI URGENTI IN MATERIA DI PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA"

Buongiorno a tutti,

ringrazio il Presidente Brescia e il Presidente Morelli per il cortese invito che mi dà l'opportunità di illustrare la strategia messa in campo dal Governo nel delicato ambito della sicurezza cibernetica nazionale, sul quale il Ministero che rappresento assume un ruolo chiave in qualità di Autorità NIS per i settori energia, infrastrutture e servizi digitali.

Con il **decreto-legge 21 settembre 2019, n. 105**, oggetto della presente conversione in atto , sono state inserite disposizioni urgenti per affrontare con la massima efficacia e tempestività situazioni di emergenza in ambito cibernetico, delineando per le finalità di sicurezza nazionale un sistema di organi, procedure e misure, che consenta una efficace valutazione sotto il profilo tecnico della sicurezza degli apparati e dei prodotti, in conformità alle più elevate e aggiornate misure di sicurezza adottate a livello internazionale, a fronte della realizzazione in corso di importanti e strategiche infrastrutture tecnologiche.

All'articolo 1, in particolare, si istituisce il cd. **Perimetro di sicurezza nazionale cibernetica**, con l'obiettivo di assicurare un elevato standard di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali e dal cui malfunzionamento, interruzione ovvero utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale.

L'individuazione dei soggetti pubblici e privati da includere nel predetto perimetro è demandata ai criteri che verranno determinati con successivo DPCM. A riguardo, si rileva che il Ministero dello sviluppo economico sarà l'Amministrazione di riferimento per il settore privato, mentre il settore pubblico sarà di competenza della Presidenza del Consiglio.

Entrando più nel dettaglio, evidenzio che l'inclusione di un soggetto all'interno del perimetro di sicurezza cibernetica comporterà in capo a quest'ultimo il rispetto di una serie di prescrizioni, tra cui:

1) **predisporre e aggiornare**, con cadenza almeno annuale, l'elenco delle reti, dei sistemi informativi e dei servizi informatici rilevanti;
2) **notificare** gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici al Gruppo di intervento per la sicurezza informatica italiano (CSIRT);
3) **adottare misure** volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici rientranti nel perimetro di sicurezza nazionale cibernetica.

L'articolo 1 prevede anche disposizioni per sviluppare un public **procurement** più sicuro per i soggetti inclusi nel perimetro, nel caso in cui questi ultimi procedano all'affidamento di forniture di beni e servizi ICT destinati ad essere impiegati su reti, sistemi e servizi di particolare rilevanza.
Le attività di verifica obbligatorie su tali appalti saranno condotte dal **Centro di valutazione e certificazione nazionale (CVCN)**, istituito con decreto del Ministro dello sviluppo economico del 15 febbraio 2019 presso l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI) del Ministero dello sviluppo economico, il quale si aggiunge ai già attivi OCSI (Organismo di certificazione della sicurezza informatica) e CE.VA. (Centro di valutazione della sicurezza informatica di prodotti e sistemi destinati a gestire dati coperti dal segreto di Stato o di vietata divulgazione), operativi sempre presso il MiSE da più di 10 anni.

Il Centro ha il compito di effettuare la valutazione e certificazione (CVCN) della sicurezza informatica (software, firmware e hardware) di prodotti, apparati e sistemi ICT destinati ad infrastrutture critiche e strategiche (ICS) nazionali. Nell'ambito delle competenze attribuite dal decreto legge in esame, il CVCN, sulla base di una valutazione del rischio, potrà imporre condizioni e test di *hardware* e *software* sui beni e servizi oggetto di gara*;* conseguentemente, anche sulla base delle risultanze dei test effettuati, il CVCN potrà integrare i bandi o i contratti con clausole che condizionano, sospensivamente ovvero risolutivamente, l'aggiudicazione o il contratto al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN.

È evidente che, anche alla luce delle funzioni attribuite dal decreto legge in esame, **il CVCN rappresenta un tassello fondamentale per la sicurezza cibernetica del Paese e la garanzia della sua piena operatività costituisce una priorità strategica nell'azione del Ministero che ho l'onore di rappresentare.**

Per far fronte a tale complessa attività che riguarda anche la sicurezza delle reti di tecnologia 5G, **l'articolo 2** del decreto legge in esame prevede l'assunzione con concorso pubblico di 77 unità presso il MiSE, **di cui 67 di area terza e 10 di area seconda, nel limite di spesa di circa 3 milioni di euro annui a decorrere dal 2020.**

Mi è doveroso segnalare che il numero di funzionari assegnati dalla legge al CVCN, sebbene rappresenti un contingente numericamente importante in questa fase di startup, potrebbe risultare insufficiente quando il meccanismo di controllo entrerà pienamente in vigore. Pertanto, per il futuro ritengo auspicabile che si provveda all'aumento delle unità da destinare al CVCN, specie considerando che, sulla base di stime effettuate dai competenti uffici del MiSE, per far fronte alle richieste che dovranno essere gestite dal CVCN a pieno regime, servirebbe circa il doppio delle unità oggi autorizzate.

Ad ogni modo, per far fronte alle esigenze del CVCN in pendenza dei concorsi per l'assunzione delle predette unità, il MISE potrà avvalersi di un contingente di personale non dirigenziale appartenente alle pubbliche amministrazioni per un massimo del 40 per cento delle unità di personale autorizzato. Confidiamo nel supporto che il Ministero della Funzione Pubblica potrà fornirci a riguardo per poter avviare le procedure concorsuali tempestivamente e garantire al MiSE l'assunzione di personale altamente qualificato. Si rappresenta inoltre che sono attualmente in corso le interlocuzioni con Università, laboratori e centri di ricerca per procedere quanto prima a rendere operativo il Centro di valutazione e certificazione nazionale.

Con l'**articolo 3** vengono introdotte disposizioni di raccordo tra il decreto in esame e la normativa in materia di esercizio dei poteri speciali governativi sui servizi di comunicazione a banda larga basati sulla tecnologia 5G.

Come noto, il 26 marzo scorso la Commissione europea ha raccomandato una serie di azioni e misure operative volte a rivedere e rafforzare le vigenti norme di sicurezza in questo settore per assicurare che riflettano l'importanza strategica delle reti 5G, nonché l'evoluzione delle minacce.

Considerati i rischi che potrebbero derivare dalla nuova tecnologia, nell'ordinamento nazionale è già operativa la normativa sull'esercizio dei poteri speciali del Governo (decreto legge 15 marzo 2012, n. 21, convertito con modificazioni dalla L. 11 maggio 2012, n. 56) cd. GOLDEN POWER, volta a tutelare interessi essenziali della difesa e della sicurezza nazionale nonché gli interessi pubblici relativi alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti nei settori dell'energia, dei trasporti e delle comunicazioni.

Con il decreto legge in esame, è stato pertanto precisato che le disposizioni relative al perimetro di sicurezza cibernetica si applicano anche ai soggetti inclusi nel perimetro di sicurezza nazionale, per i contratti o gli accordi, ove conclusi con **soggetti esterni all'Unione europea**, aventi ad oggetto l'acquisto di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti inerenti i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, ovvero l'acquisizione di componenti ad alta intensità tecnologica funzionali alla predetta realizzazione o gestione, rispetto ai quali l'articolo 1-bis del Decreto Legge 21/2012 prevede un obbligo di notifica alla Presidenza del Consiglio dei Ministri ai fini dell'eventuale esercizio del potere di veto o dell'imposizione di specifiche prescrizioni o condizioni.

Viene inoltre prevista la possibilità che, nei confronti dei soggetti inclusi nel perimetro di sicurezza nazionale, le condizioni o le prescrizioni relative ai beni e servizi acquistati con contratti già autorizzati con decreti del Presidente del Consiglio dei Ministri e adottati sulla base della normativa sui poteri speciali previgente **possano essere modificate o integrate con misure aggiuntive**, al fine di assicurare livelli di sicurezza equivalenti a quelli previsti dal presente decreto legge, anche prescrivendo, ove necessario, la sostituzione di apparati o prodotti che risultino **gravemente inadeguati** sul piano della sicurezza.

Infine, **all'articolo 4,** si introduce una modifica all'articolo 2, comma 1-ter del citato DL 21/2012**,** relativo ai settori ad alta intensità tecnologica, specificando che, nell'ambito della verifica sulla sussistenza di un pericolo per la sicurezza e l'ordine pubblico, è compreso anche il possibile pregiudizio alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti.

Nelle more dell'adozione del regolamento di cui al comma 1-ter - le cui bozze sono peraltro in uno stato avanzato di definizione - l'articolo 4, comma 2 inserisce una disciplina transitoria in base alla quale è soggetto a notifica l'acquisto a qualsiasi titolo, d**a parte di un soggetto esterno all'Unione europea**, di partecipazioni societarie di rilevanza tale da determinare l'insediamento stabile dell'acquirente in società che detengono beni e rapporti nei **settori di cui all'art. 4, paragrafo 1, lettere a) e b), del regolamento (UE) n. 2019/452, ovverosia:**

a) infrastrutture critiche, siano esse fisiche o virtuali, tra cui **l'energia,** i trasporti, l'acqua, la salute, **le comunicazioni**, i media, il trattamento o l'archiviazione di dati, **le infrastrutture aerospaziali**, di difesa, elettorali o finanziarie, e le strutture sensibili, nonché gli investimenti in terreni e immobili fondamentali per l'utilizzo di tali infrastrutture,

b) **tecnologie critiche e prodotti a duplice uso, tra cui l'intelligenza artificiale, la robotica, i semiconduttori, la cibersicurezza, le tecnologie aerospaziali, di difesa, di stoccaggio dell'energia, quantistica e nucleare, nonché le nanotecnologie e le biotecnologie.**

In conclusione, è del tutto evidente il massimo impegno profuso dal MISE, quale Ministero guida sul fronte della sicurezza cibernetica; tengo però a sottolineare che l'approccio che caratterizzerà l'azione del Ministero sarà incentrata sull'assicurare la salvaguardia dei nostri interessi nazionali, in coordinamento e in sinergia con gli altri organismi competenti, previa adeguata ponderazione degli interessi di natura commerciale degli operatori e delle imprese che quotidianamente si interfacciano con la nostra Amministrazione.