Prof. Antonio Teti, PhD
Responsabile del Settore Sistemi Informativi e Innovazione Tecnologica dell'Università "G. D'Annunzio" di Chieti-Pescara e docente di Data Science e Technology Intelligence
E-mail: antonio.teti@unich.it

Audizione informale avanti le Commissioni riunite I e IX della Camera dei Deputati per l'esame del disegno di legge del Governo C. 2100 volto alla conversione del decreto-legge n. 105 del 2019 recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.

Premessa

In linea di principio, l'approccio del decreto legge n.105/2019 rappresenta un significativo punto di partenza della disciplina della tutela delle infrastrutture critiche, soprattutto ove a questa affianca la tutela della sicurezza dello Stato attraverso la individuazione di soggetti – amministrazioni pubbliche, enti ed operatori nazionali pubblici e privati – da includersi nel perimetro di sicurezza nazionale cibernetica, nonché la definizione di criteri in base ai quali, pur non rientrando nel novero delle infrastrutture critiche, tali soggetti saranno chiamati all'osservanza di precisi obblighi volti all'assicurazione di elevati livelli di sicurezza in quanto esercenti di funzioni o di servizi essenziali per lo Stato.
Un esempio per tutti, quello di un aeroporto, simbolo certo di una "infrastruttura critica" anche a volerne considerare la sola interazione con la pluralità, complessità e varietà di soggetti partner nell'esercizio del servizio quotidianamente reso: in estrema sintesi si pensi ai soli fornitori ed a quanto tale categoria sia suscettibile di determinare l'insorgenza di potenziali rischi in termini di sicurezza (dai servizi di vigilanza privata a quelli che a vario titolo si esplicano mediante accesso ad aree non pubbliche o a quelli resi da soggetti che interagendo con i sistemi informatici dell'aeroporto possono virtualmente attivare delle *backdoor* per l'accesso ai sistemi *core* dell'infrastruttura).
Circa la tecnica normativa prescelta, l'approccio al Decreto Legge si manifesta molto più flessibile di quello adottato in recepimento della direttiva sulle infrastrutture critiche poiché si occupa di regolare gli *obiettivi* piuttosto che gli strumenti tecnologici utilizzati per raggiungerli, con ciò facilitando la disciplina di una materia di tipo tecnico-scientifico poiché consente una maggiore flessibilità in termini di fruibilità applicativa eliminando la necessità della emanazione di ulteriori provvedimenti in caso di future innovazioni. Aspetto, quest'ultimo, che imporrebbe passaggi istituzionali che potrebbero richiedere tempi incompatibili con le possibili urgenze imposte dagli eventi (considerazione che benché valevole in termini generali risulta ancora più significativa quando si tratta della disciplina di un settore, come quello della tutela della sicurezza dello Stato, soggetto a possibili aggressioni o eventi imprevisti inevitabilmente coinvolgenti le tecnologie dell'informazione).

Considerazioni sul Decreto Legge n. 105 del 1 settembre 2019, *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*

Le attività di cui all'art. 1 comma 3 lettera b) risultano sicuramente essenziali per una efficace applicazione del provvedimento. Si segnalano tuttavia alcune considerazioni e criticità sulle quali riflettere:

1. **Rischio di sovrapposizione con la normativa sulla protezione dei dati personali e possibili conflitti di competenza con l'Autorità garante per la protezione dei dati personali.**
   Benché la normativa sulla protezione dei dati personali non si applichi alle questioni riguardanti la sicurezza dello Stato, è necessario chiarire espressamente che l'adempimento alle misure di sicurezza dettate in attuazione del decreto in esame non è soggetta ad autorizzazioni e controlli del Garante dei dati personali. Ciò risulta fondamentale poiché gli obiettivi di sicurezza che questo decreto si prefigge sono diversi da quelli definiti dal Codice dei dati personali e dal Regolamento comunitario sulla protezione dei dati personali. Essendo gli obiettivi del decreto inequivocabilmente rilevanti per la sicurezza nazionale, è consigliabile prevedere norme tecniche dirette finalizzate all'innalzamento della componente "prevenzione" suscettibile di tradursi, pressoché inevitabilmente, in un incremento delle attività istituzionali di sorveglianza.

2. **Valutazione della opportunità di bilanciamento delle scelte tecniche di natura preventiva con la funzione del Comitato parlamentare per la sicurezza della Repubblica (Copasir).**
   Per un migliore bilanciamento delle esigenze tecnico-operative con quelle di controllo democratico, sarebbe da valutarsi l'introduzione di una specifica potestà del Copasir di accesso e verifica delle modalità di attuazione ed esecuzione delle misure tecniche in questione, oltre che un dovere dei soggetti individuati dal decreto di riferire al Copasir, almeno su base annuale, sulle modalità di applicazione delle misure tecniche adottate.

3. **Valutazione dell'opportunità di prevedere qualifiche di sicurezza per i fornitori non soggetti al Nulla Osta Sicurezza (NOS).**
   La struttura a "scatole cinesi" del mercato tecnologico mondiale ha prodotto una prassi diffusa: quando i servizi sono erogati a soggetti pubblici si fa spesso ricorso al subappalto (anche se nella forma del raggruppamento temporaneo di imprese o di altri analoghi strumenti giuridici). La conseguenza, è che non possedendo le necessarie competenze, il capofila o l'aggiudicatario della gara, le reperisca sul mercato in funzione delle esigenze del momento. Per quanto non contrario alle previsioni del Codice degli appalti, sarebbe consigliabile

prevedere una forma di qualificazione di sicurezza (una sorta di sub-NOS) cui assoggettare i titolari delle persone giuridiche e le persone fisiche (siano esse singoli professionisti o dipendenti finanche distaccati da altre organizzazioni) che assumano funzioni e servizi critici nell'ambito della sicurezza.

4. **Richiesta di adeguate garanzie ai produttori di tecnologie utilizzate dai soggetti erogatori di servizi connessi all'esercizio di funzioni essenziali.**
   Nell'ambito delle tecnologie impiegate nella gestione delle funzioni e dei servizi essenziali indicati dal decreto, permane la problematicità derivante dalle effettive garanzie di sicurezza sui software e hardware utilizzati dalle aziende operanti nel settore ICT (Information and Communication Technology). La normativa sulla proprietà industriale e intellettuale, difatti, impedisce ai fornitori che utilizzano tecnologie prodotte da terzi di eseguire le adeguate verifiche di sicurezza. L'esperienza comune accumulata in materia di software, fornisce inoltre un chiaro ed inequivocabile scenario di *security vulnerabilities* che impone ai fruitori continui aggiornamenti di sistema forniti dai rispettivi produttori. È vero che l'art. 1 comma 6 lettera a) condiziona la fornitura di beni e servizi alle conformità agli standard definiti dal Centro di valutazione e certificazione nazionale (CVCN), ma potrebbero sorgere problematiche derivanti dalle limitazioni che la normativa sul diritto d'autore e sui brevetti impone sui collaudi e le verifiche di conformità dettate dal CVCN. Sarebbe pertanto consigliabile prevedere la non applicabilità dei diritti di cui al Codice della proprietà intellettuale e industriale e dalla Legge sul diritto d'autore in materia di tutela del segreto e dell'accesso al codice sorgente di software, oltre all'imposizione di una precisa assunzione di responsabilità in capo ai produttori circa l'effettivo livello di sicurezza dei prodotti hardware e software che dovranno essere utilizzati in ambito istituzionale.

5. **Rischio di ridotta efficacia degli obblighi dei "test di hardware e software" (art. 1 comma 6 lettera a) e possibilità di introduzione dell'utilizzo di standard "aperti".**
   I produttori di hardware e software - essenzialmente stranieri – rappresentano i maggiori fornitori di prodotti tecnologici dello Stato. In ambito software/firmware sarebbe opportuno intraprendere la medesima strada adottata dal Dipartimento della Difesa statunitense in occasione della creazione del protocollo TCP/IP (Transmission Control Protocol/Internet Protocol) che è alla base del funzionamento della rete Internet: rendere i codici di "pubblico dominio", cioè privi di diritti d'autore esclusivi o, quantomeno prevederne la accessibilità alle istituzioni governative del comparto sicurezza. In alternativa, in sostituzione dei cosiddetti "standard di mercato", valutare la possibilità che le norme attuative previste dal decreto dettino ai propri fornitori di tecnologie degli standard "ad hoc". Il vantaggio

consisterebbe nel pieno controllo delle istituzioni sulle tecnologie utilizzate nelle infrastrutture critiche.

6. **Evitare il ricorso ai soli standard di processo (certificazioni).**
   Benché questa sia materia per i provvedimenti attuativi indicati dal decreto, va evidenziato che il possesso delle aziende di certificazioni di processo in materia di sicurezza - come nel caso dello Standard ISO/IEC 27000 - non è di per sé sufficiente a garantire gli obiettivi previsti dal decreto. Queste certificazioni, infatti, si limitano ad attestare l'esistenza di determinate procedure in essere all'interno dell'organizzazione, ma non sono esaustive nel merito della loro concreta efficacia tecnologica. A tal proposito, le prassi registrate sul mercato (soprattutto nazionale) evidenziano la semplicità dell'ottenimento delle certificazioni in questione anche per parziali settori tecnici interni. In altri termini, il potenziale fornitore di prodotti/servizi negli ambiti individuati dal decreto potrebbe possedere una certificazione per un "ramo" dell'azienda ma non per tutti gli altri.

7. **Valutazione di impatto sui costi.**
   Benché le indicazioni di cui al precedente punto 4 siano - dal punto di vista delle *best practices* di sicurezza - certamente importanti, va evidenziata la criticità derivante dall'incremento dei costi per gli utilizzatori di tali tecnologie. Il rischio, dunque, è che si trovino delle "scappatoie" per certificare solo formalmente il possesso dei requisiti normativamente imposti. In particolare, per quanto riguarda le previsioni di cui all'art. 1 comma 3 lettera b) sarebbe opportuno prevedere che i costi di adeguamento di prodotti hardware/software finalizzati al rispetto dei livelli di sicurezza siano sostenuti direttamente dai produttori e non dagli utilizzatori. In alternativa, il produttore dovrebbe sviluppare i propri prodotti in ossequio ai principi della "progettazione sicura" (per esempio, adozione di uno standard come OWASP - Open Web Application Security Project - per le applicazioni software).

8. **Ruolo degli operatori di telecomunicazioni e dei fornitori di servizi di comunicazione elettronica.**
   Gli operatori di telecomunicazioni e Internet Provider rivestono un ruolo essenziale nel garantire la sicurezza del perimetro cibernetico. Quelli italiani sono già soggetti, ai sensi del Codice della comunicazione elettronica, all'obbligo di garantire la sicurezza delle reti pubbliche di comunicazione. Tale obbligo, tuttavia, non è mai stato dettagliato e sarebbe opportuno che il decreto indicasse specifiche misure di sicurezza (e relative responsabilità anche penali) al riguardo. Anche se l'art. 1 comma 8 del decreto si occupa del tema, necessita di un approfondimento per la parte relativa alle indicazioni

per la garanzia della tutela della sicurezza nazionale, in termini di misure di sicurezza da adottarsi. Sarebbe preferibile esplicitare i requisiti onde consentire una maggiore facilità di implementazione a fronte di limiti normativi come il Regolamento sulla protezione dei dati personali.

Conclusioni

L'impianto del decreto legge n. 105/2019 è sicuramente solido da un punto di vista dell'architettura, ma necessita – specie nell'indicazione degli atti normativi da emanare successivamente – chiarimenti aggiuntivi finalizzati all'eliminazione di possibili sovrapposizioni e contrasti con la normativa esistente, finanche in ambiti di competenza di altre Autorità indipendenti.