CONFINDUSTRIA DIGITALE

Audizione della Federazione Confindustria Digitale sul Decreto Legge recante norme in materia di "Perimetro di sicurezza nazionale cibernetica" – AC 2100

IX Commissione Trasporti, Poste e Telecomunicazioni
e
I Commissione Affari costituzionali

CAMERA DEI DEPUTATI

7 ottobre 2019

Premessa

Il DL 105/2019 al fine di assicurare il massimo livello di sicurezza delle reti, dei sistemi informativi e dei servizi informatici di interesse collettivo, istituisce il c.d. "*Perimetro di Sicurezza Nazionale Cibernetica*".

Nell'ambito del perimetro di SNC, entro 4 mesi dalla legge di conversione, è prevista la predisposizione di un elenco di soggetti, "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 per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale".

Il DL 105/2019 stabilisce che tali soggetti, saranno tenuti al rispetto di una serie articolata di obblighi informativi e procedimentali, oltre ad essere sottoposti all'attività di ispezione e vigilanza della Presidenza del Consiglio dei Ministri, in caso di enti pubblici e pubblici economici, ovvero del Ministero dello Sviluppo Economico, laddove si tratti di soggetti di natura privatistica.

Sono previste anche delle regole particolari in materia di appalti pubblici, per i soggetti che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati su reti o sistemi informativi particolarmente a rischio, oltre che per l'espletamento di alcuni servizi informatici.

Il DL raccorda esplicitamente il sistema di sicurezza nazionale cibernetica con quanto previsto dal decreto legislativo di recepimento della direttiva sulla sicurezza di reti e sistemi informativi (c.d. NIS) e dal Codice delle Comunicazioni Elettroniche in materia di sicurezza; pertanto gli obblighi di notifica derivanti dal DL assolvono anche gli obblighi emergenti dalla NIS e dal CCE.

Il DL reca inoltre una disciplina esplicita di raccordo con la normativa del c.d. "Golden Power".

Il rispetto di tali prescrizioni e dell'attività ispettiva e di vigilanza della Presidenza del CdM e del MISE, verrà assicurato dal sistema sanzionatorio di carattere amministrativo, e da una doppia fattispecie di reato di tipo commissivo (dichiarazioni non rispondenti al vero) e di tipo omissivo (chiunque ometta di

comunicare tali informazioni, entro il termine prescritto dal Decreto) previsto e punito dal comma 11, art. 1 DL 105/2019).
Inoltre, sempre nell'ambito dello stesso art 11 del Decreto, il legislatore ha ritenuto di estendere, direttamente dal corpo di questa nuova fattispecie, la rilevanza del reato ai fini della responsabilità amministrativa degli enti ex D. Lgs.231/2001.

Considerazioni generali

L'industria delle tecnologie e dei servizi ICT rappresentata da Confindustria Digitale ha accolto positivamente l'emanazione del DL 105/2019 in quanto l'individuazione di un perimetro nazionale di cyber security è estremamente importante per il nostro Paese; la sicurezza è un obiettivo strategico del Paese condiviso da tutte le imprese operanti nel comparto dell'ICT.
E' altrettanto importante che attraverso il DL 105/2019 la cyber security diventi parte integrante delle richieste contrattuali, così come consideriamo molto positivamente l'attivazione di una filiera nazionale certificata.
E' parimenti condivisibile e apprezzabile lo sforzo fatto dal Legislatore per raccordare questa nuova disciplina con la normativa esistente in materia di "Golden Power" e con le disposizioni derivanti dalla direttiva NIS e dal Codice delle Comunicazioni Elettroniche, evitando il rischio di una duplicazione di oneri per le imprese.
Anche la circostanza che vede il nostro Paese essere tra i primi in Europa a disporre di una legislazione nazionale specifica sul tema non può che essere registrata molto positivamente dal comparto industriale dell'ICT e confidiamo che questo progresso normativo possa fungere da stimolo per incrementare il livello di investimenti che invece vede oggi il nostro Paese in posizioni di retroguardia rispetto ai principali Paesi UE.
Fermo restando il giudizio positivo appena espresso, il DL 105/2019 contiene una serie di prescrizioni che necessitano di chiarimenti e specificazioni ai fini di consentirne un'applicazione certa e univoca.

Osservazioni di merito sulle norme contenute nel DL

1. Un primo aspetto di criticità riguarda l'individuazione puntuale della platea dei soggetti ricadenti nel perimetro di SNC. Sarà estremamente importante dettagliare, in sede di emanazione del DPCM di attuazione, il criterio che porterà ad individuare i soggetti dell'elenco (pubblici e privati) obbligati al rispetto delle prescrizioni. Infatti non si può non osservare come attualmente il testo del decreto fissi criteri particolarmente inclusivi che potrebbero far rientrare nel perimetro praticamente tutte le società impegnate, a qualunque titolo, nell'erogazione di prestazioni essenziali e/o strategiche per lo Stato, quali l'energia e i trasporti, ma anche la progettazione e l'esecuzione di infrastrutture.

2. Un secondo elemento di criticità è rappresentato dal criterio guida a cui deve essere ispirata l'adozione di misure atte a prevenire i rischi per la sicurezza. L'adozione di appropriati sistemi di sicurezza si basa innanzi tutto sull'analisi, anche dinamica nel tempo, dei rischi connessi al funzionamento di reti, sistemi, apparati, e all'analisi dei rischi si deve associare la definizione di misure atte a mitigare gli impatti attesi, nel caso il rischio si materializzasse. Le contromisure adottate sono dunque caratterizzate dal principio di proporzionalità rispetto ai rischi identificati. Occorre quindi adottare un principio di proporzionalità che consenta di focalizzare le risorse laddove queste hanno il più alto valore, assicurando l'efficienza e massimizzando l'efficacia dei sistemi di sicurezza.

Le imprese del settore ICT continuano a sviluppare esperienze in questo campo, anche a livello internazionale, esperienze che rappresentano una fondamentale risorsa alla luce della continua evoluzione delle tecnologie, è quindi altamente auspicabile che si istauri una collaborazione continuativa, tra Autorità di sicurezza e operatori, in tutte le fasi di definizione delle regole e la loro attuazione.

3. Il decreto introduce un'attività di verifica da parte del Centro di Valutazione e Certificazione Nazionale (CVCN) che non è chiaro se debba essere assolto prima o dopo una procedura di selezione del fornitore. Non è chiaro se il CVCN agirà *ex ante*, anche divulgando linee guida per gli approvvigionamenti, o se opererà in una logica *ex post.* In quest'ultima ipotesi appare chiaro che l'aggravio temporale sull'implementazione delle forniture rischia di essere notevole. Nel caso di

procedure ad evidenza pubblica è legittimo domandarsi se la fase di valutazione si svolga prima dell'indizione della gara stessa o invece nella fase di aggiudicazione.
E' legittimo anche domandarsi quale possa essere il livello di approfondimento delle verifiche.
La delicatezza di questa tema risulta evidente nel caso di approvvigionamenti che riguardino un sistema: si certifica il sistema o i suoi componenti? E se un componente è richiesto dal committente fino a che livello se ne deve conoscere la struttura? Il problema è di tutta evidenza quando si tratti di chipset inseriti in sistemi.
Di chi è responsabilità se un determinato componente in futuro rivela una vulnerabilità, magari quando inserito in un sistema? Del fornitore che lo ha prodotto, oppure del committente che lo ha specificamente richiesto, oppure del system integrator che lo ha inserito nel sistema, o ancora del centro di verifica e certificazione?
La definizione del livello delle attività di verifica ha implicazioni molto rilevanti: in primo luogo per la mole di lavoro che rischia di essere demandata al CVCN, con ovvie conseguenze in tema di strutturazione del CVCN e di investimenti necessari per reperire personale con competenze adeguate, competenze che oggi le imprese del settore faticano a trovare nel mercato del lavoro.
Ma il livello delle attività di verifica ha rilevantissime implicazioni anche dal punto di vista della tutela della proprietà intellettuale e industriale: si pensi alla criticità per una impresa del settore di dover rivelare a una terza parte dettagli di soluzioni tecniche, che qualora il CVCN dovesse operare ex ante verrebbero rivelati in fase di offerta in procedure di gara.
Vi è anche la necessità di capire se il CVCN nell'ambito delle attività di verifica renderà pubbliche o comunque disponibili alle imprese i criteri di certificazioni e le check list.
E' essenziale che i livelli di sicurezza siano ispirati ai criteri e agli standard definiti a livello internazionale, che sia riconosciuto valore alle certificazioni internazionali di cui le imprese si avvalgono a livello globale, e che le procedure di verifica siano semplici e abbiano tempi certi e contingentati.

4. Il tema delle forniture agli enti pubblici è particolarmente delicato e al riguardo andrebbe chiarito ed ulteriormente soppesato l'impatto sulle modalità di affidamento e di acquisizione di tecnologie ed i controlli richiesti. Come noto, le PA e organismi partecipati acquisiscono beni e servizi nel rispetto del codice dei contratti pubblici con le relative tempistiche. È vero che il decreto prevede espressamente che "*i relativi bandi di gara e contratti sono integrati con clausole che condizionano, sospensivamente ovvero risolutivamente, l'affidamento ovvero il contratto al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN*", tuttavia ci si domanda se il Legislatore abbia adeguatamente soppesato l'incidenza di tale previsione sui processi di approvvigionamento.
Ulteriore aspetto con riguardo alle forniture agli enti pubblici che merita di essere approfondito è quello relativo all'aggravio di attività e di costi che rischia di abbattersi sulle imprese fornitrici di sistemi, soluzioni e apparati, aggravio che potenzialmente rischia di pesare in maniera particolare sulle PMI, di fatto limitandone fortemente la capacità di partecipazione alle gare pubbliche per forniture che rientrino nel perimetro di sicurezza cibernetica nazionale.

5. Considerata l'elevata entità delle sanzioni amministrative pecuniarie previste, ci si domanda se sia stata attentamente valutata la necessaria proporzionalità tra sanzioni e comportamenti considerati illeciti ai sensi del DL.
Inoltre le disposizioni contenuti nei commi da 9 a 14 prevedono esclusivamente sanzioni amministrative e pecuniarie che scattano quando sia verificata una vulnerabilità delle reti; sarebbe quantomeno opportuno prevedere un meccanismo che, anziché comminare una sanzione in maniera automatica, preveda invece una richiesta di azioni correttive mandatorie, eventualmente con un "grace period" per risolvere le criticità riscontrare, prima di comminare una sanzione e/o imporre una disattivazione del servizio.
A quest'ultimo riguardo si deve segnalare una ulteriore criticità rappresentata dalla norma contenuta nell'art.3, comma 3, che prevede che le condizioni e prescrizioni definite nelle autorizzazioni già rilasciate possano essere riviste ed integrate in un periodo successivo entro 60 giorni dall'entrata in vigore del DPCM, che stabilirà le "misure volte a garantire elevati livelli di sicurezza anche prevedendo, ove necessario, la sostituzione di apparati o prodotti che risultino gravemente

inadeguati sul piano della sicurezza." Tale previsione di fatto introduce elementi di forte incertezza per quei soggetti che, pur avendo avuto l'autorizzazione per le operazioni effettuate e agendo nel pieno rispetto delle prescrizioni ed obblighi precedentemente adempiuti, si troverebbero a dover modificare le proprie reti e sistemi con gravi difficoltà operative e significativi costi incrementali.