ASSOTELECOMUNICAZIONI
ASSTEL

ADERENTE A **CONFINDUSTRIA** E **CONFINDUSTRIA DIGITALE**

Audizione di Assotelecomunicazioni sul Decreto Legge "perimetro di sicurezza nazionale cibernetica" – AC 2100

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

CAMERA DEI DEPUTATI

3 ottobre 2019

Sommario

Considerazioni generali

1) La sicurezza è un obiettivo ed un interesse strategico del Paese, condiviso da tutti gli operatori della filiera delle telecomunicazioni. Tradizionalmente la sicurezza logica ha riguardato principalmente la protezione dei sistemi informatici e la tutela dei dati personali degli utilizzatori dei servizi di comunicazione. Oggi la progressiva trasformazione delle reti di telecomunicazione in sistemi, che ospitano e saranno governati da "software", impone una analoga attenzione alle infrastrutture di rete; in particolare con riferimento alle reti 5G, le quali consentiranno lo sviluppo di servizi realizzati mediante una combinazione integrata di infrastrutture e di applicativi, adottati in funzione delle esigenze del cliente finale, che contribuirà a definirli. Per tale motivo sempre più ci si riferisce alle reti del futuro quali "software defined network".

2) L'adozione di appropriati sistemi di sicurezza si basa innanzi tutto sull'analisi, anche dinamica nel tempo, dei rischi connessi ai diversi elementi di rete, caratterizzati dalla specifica funzionalità e dalle dimensioni dell'impatto di un eventuale malfunzionamento. All'analisi dei rischi si associa 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. Tale approccio consente di focalizzare le risorse laddove queste hanno il più alto valore, assicurando l'efficienza e massimizzando l'efficacia dei sistemi di sicurezza.

3) Gli operatori di telecomunicazioni ed i "vendor" di infrastrutture di rete hanno sviluppato e continuano a sviluppare importanti esperienze in tal senso, anche a livello internazionale, esperienze che rappresentano una risorsa proprio alla luce delle finalità del Decreto Legge in tema di sicurezza cibernetica. Pertanto, anche a motivo della continua evoluzione delle tecnologie, ai fini della piena funzionalità ed efficacia dell'architettura di monitoraggio e gestione dei rischi, è necessaria una collaborazione altrettanto continuativa, nonché preliminare, tra Autorità di sicurezza ed Operatori, in tutte le fasi di definizione delle regole e la loro attuazione. In un contesto di collaborazione continuativa tra imprese e amministrazioni preposte alla sicurezza nazionale, come già avviene nella collaborazione con le forze dell'ordine e le autorità di giustizia, sarà possibile assicurare un sistema realmente efficace ed anche efficiente.

Commenti ai principali aspetti del Decreto Legge in materia di sicurezza nazionale cibernetica

4) Il DL "sicurezza nazionale cibernetica" adotta un approccio sistematico, con la definizione puntuale della governance di sicurezza, del perimetro di applicazione, del ruolo dei soggetti obbligati e dei criteri di valutazione. Questo aspetto è di grandissima importanza per le imprese della filiera delle telecomunicazioni

5) Affinché ciò si realizzi appieno, occorre che siano in via generale nelle varie fasi implementative della norma, anche soddisfatti alcuni fondamentali presupposti:

   a. la partecipazione degli Operatori alla definizione dei provvedimenti attuativi, in un rapporto di collaborazione con gli organismi di sicurezza, come affermato in premessa, che sia preliminare all'adozione delle regole e – successivamente - continuativo nell'esercizio del sistema;

   b. la piena adozione, come già affermato all'art. 1, comma 6 lett.a), di un approccio orientato alla valutazione del rischio e alla proporzionalità delle misure di sicurezza sui diversi elementi di rete;

   c. la valorizzazione di standard a cui le imprese aderiscono e delle certificazioni internazionali di cui si avvalgono;

   d. l'attenzione alla definizione di tempi ristretti e di procedure semplici;

   e. La previsione di un periodo di adeguamento alle misure di sicurezza richieste dalle autorità, al fine di valutare la sostenibilità economica e di garantire la realizzabilità degli adeguamenti (infrastrutturali e non) e che richiedono decisioni di programmazione, tempi di *procurement* e di installazione/ implementazione.

6) Relativamente ai criteri con cui verrà definito l'ambito oggettivo di applicazione oggetto di uno specifico DPCM, la cui emanazione è prevista entro 4 mesi dall'entrata in vigore della legge, si osserva che è di grande importanza esplicitare quale siano le circostanze che possono – in ipotesi - concretizzare un effettivo pregiudizio per la sicurezza nazionale, così da mettere i soggetti obbligati in grado di focalizzare correttamente gli elementi tecnologici ed i servizi rilevanti ai fini della

sicurezza; questo chiarimento è evidentemente importante per attuare il principio di proporzionalità rispetto al rischio specifico associato a ciascun elemento e definire le priorità di intervento ai fini della sicurezza.

7) La definizione di misure volte a garantire elevati livelli di sicurezza è un punto fondamentale per garantire l'efficacia della normativa, ma anche per gli effetti che l'imposizione di tali misure può avere sui soggetti obbligati. Al fine di attuare un sistema realmente adeguato si raccomanda di:

   a. considerare gli standard di sicurezza già adottati dalle imprese quale punto di partenza, eventualmente soggetto – laddove opportuno – ad ulteriori miglioramenti;

   b. ispirare i livelli di sicurezza ai criteri ed agli standard definiti a livello internazionale, a cui le imprese si riferiscono per la configurazione delle reti. Al riguardo, senza ritenere opportuno un riferimento puntuale nel testo della legge, si citano per memoria gli standard ISO 27001 (Sistema di gestione Information Security), ISO28000 (Specifiche per il sistema di gestione sicurezza per la Supply Chain), ISO30111 (Information technology, tecniche di sicurezza, gestione delle Vulnerabilità), SECAM, ecc. e si rammenta anche l'esistenza di un nuovo framework di sicurezza c.d. "Network Equipment Security Assurance Scheme" (NESAS) definito congiuntamente da 3GPP e GSMA come uno schema volontario per l'industria Mobile[1] in via di rilascio per la fine del 2019.

   c. **prevedere una sede istituzionalizzata di consultazione tra amministrazioni preposte alla sicurezza e le imprese fornitrici ed esercenti reti e servizi di telecomunicazioni, sia in fase preventiva, durante il processo di scrittura dei regolamenti, sia in generale per l'esercizio del sistema di sicurezza previsto dalla normativa;** i processi di consultazione, con spirito pienamente contributivo e collaborativo, possono utilmente prevedere anche il coinvolgimento dei laboratori delle imprese di Ricerca e Sviluppo sui sistemi di sicurezza, nonché delle Università e dei centri di ricerca italiani, accreditati secondo opportuni criteri.

[1] cfr. https://www.gsma.com/security/network-equipment-security-assurance-scheme/

d. Prevedere, come anticipato nelle premesse generali, un periodo di adeguamento compatibile con la programmazione tecnico-economica aziendale.

8) Si sottolinea l'esigenza di fare riferimento a iniziative, norme e standard che verranno definite a livello comunitario, al fine di assicurare una base comune di sicurezza cibernetica tra gli Stati Membri. È quindi importante sottolineare che tanto più i requisiti sono conformi a standard internazionali, tanto più le operazioni a garanzia della sicurezza saranno efficienti ed efficaci ed eviteranno quindi aggravi non necessari a carico degli attori privati.

9) Il ruolo del CVCN appare uno snodo fondamentale dell'architettura procedurale complessiva, essendo il luogo in cui operare una valutazione del rischio. La valutazione del CVCN avverrà in relazione all'ambito di impiego dei singoli elementi di rete e in un'ottica di gradualità, condizioni che declinano un approccio correttamente orientato ad un principio di proporzionalità dell'intervento del CVCN. L'attenzione al CVCN appare estremamente condivisibile: essendo la sicurezza un processo continuativo ed essendo il CVCN l'organismo chiamato a definire e aggiornare criteri e certificazioni di sicurezza il suo ruolo sarà fondamentale e questo lo rende il luogo più adatto a sviluppare una interlocuzione continua – anche di natura tecnica – tra autorità di sicurezza e soggetti obbligati. Condivisibile il termine di 30 giorni entro cui il CVCN è richiesto di imporre condizioni e test di hardware e software; si segnala che risulta necessario prevedere una disciplina in caso di mancata risposta del CVCN entro il termine indicato, equiparando il silenzio ad assenso.

10) La rilevanza del ruolo del CVCN è ulteriormente evidenziata dal disposto dell'art. 3 del DL, il quale prevede un opportuno ed esplicito raccordo con la disciplina del Golden Power vigente, chiarendo che il sistema di sicurezza nazionale cibernetica si applica anche nei casi in cui sia previsto l'obbligo di notifica richiesto dal Golden Power (ad ovvia eccezione delle norme sulle procedure di notifica delle operazioni di acquisto soggette a Golden Power). Viene, infatti, esplicitamente indicato che, a partire dall'entrata in vigore dei Regolamenti attuativi, i poteri di Golden Power vengono esercitati "previa valutazione" da parte del CVCN e del Centro di Valutazione della Difesa "degli elementi indicanti la presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano". In un periodo stimabile attorno all'anno, vengono così ricondotti ad unitarietà i criteri di valutazione del Golden Power e quelli di certificazione del CVCN, su cui si basa il sistema di sicurezza nazionale cibernetica,

con il vantaggio di delineare a regime un sistema coerente, necessario alla luce di quanto osservato in apertura sulla rilevanza – ai fini della sicurezza – non solo degli elementi di rete, ma anche delle interrelazioni che caratterizzano le reti 5G rispetto a programmi e applicativi degli utenti.

11) Con riguardo specificatamente alle norme del Golden Power, per quanto riguarda le procedure di notifica delle operazioni di acquisto, è importante osservare che il DL integra opportunamente alcuni aspetti non presenti nella disciplina del Golden Power introdotta nel marzo 2019, relativamente all'ambito oggettivo di applicazione ed ai criteri di valutazione delle operazioni notificate; tale integrazione ha aumentato la chiarezza e l'agibilità per gli operatori di rete del quadro normativo applicabile ai processi di acquisto degli elementi di rete. A questo riguardo si sottolineano due esigenze particolarmente sentite da parte delle imprese: in primo luogo, si sottolinea l'importanza di non modificare le tempistiche previste nella norma Golden Power vigente, che sono di cruciale importanza per rendere la disciplina compatibile con uno svolgimento "fisiologico" delle attività di realizzazione dei programmi di investimento infrastrutturali. In secondo luogo, ma non meno importante, è dare completa attuazione alla norma contenuta del DL Brexit, con riferimento alla possibilità di apportare semplificazioni alle procedure amministrative ordinarie attualmente utilizzate per l'ottemperanza, dando seguito alla consultazione pubblica avviata nel luglio del corrente anno, al fine di prevenire in via generale insorgere di duplicazioni di oneri aventi la medesima finalità.

12) Si evidenzia altresì che 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. In particolare, si prevede che l'obbligo di notifica derivante dal DL assolva anche gli obblighi emergenti dalla NIS e dal CCE e che le misure di sicurezza già previste restino in vigore, con eventuali integrazioni per garantire i livelli elevati di sicurezza.

13) La previsione di una disciplina esplicita di raccordo delle disposizioni del DL con il Golden Power, da un lato, e con le disposizioni derivanti dalla direttiva NIS e dal Codice delle Comunicazioni Elettroniche, dall'altro, appare altamente apprezzabile e risolve nella direzione della semplificazione una criticità potenzialmente molto rilevante.

14) Sotto il profilo dei procedimenti di valutazione, si evidenzia che i soggetti obbligati dovranno confrontarsi con tre modalità differenziate, in relazione a:

   a. operazioni "ordinarie", o

   b. rilevanti per il Ministero della Difesa, o

   c. per l'accertamento dei reati.

   Tale articolazione, pur comprensibile alla luce delle diverse competenze dei diversi pubblici poteri, rischia di comportare una complessità di difficile gestione per i soggetti obbligati, quindi è auspicabile che le diverse procedure siano mantenute quanto più possibile similari ed omogenee nel loro svolgimento, pur nel rispetto delle differenti esigenze, connesse al diverso livello di criticità o di urgenza delle relative circostanze.

15) Un elemento che deve essere oggetto di una accurata e approfondita analisi, per le potenziali implicazioni ad esso connesse, è rappresentato dalla previsione dell'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 – nella prospettiva della gestione aziendale di processi pluriennali di investimento - non può essere condivisa, in quanto introduce elementi di 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, con gravi difficoltà operative, significativi costi incrementali a cui sarebbero associati ritardi o riduzioni dei piani di investimento.

   Va evidenziato infatti che il processo autorizzativo comprensivo dell'ottemperanza degli obblighi e delle prescrizioni ricevute, vede il coinvolgimento e la piena visibilità di tutte le azioni volte a garantire gli standard di sicurezza richiesti. In questo quadro risulterebbe di difficile comprensione il fatto che, dopo aver adempiuto a tutti gli obblighi, un soggetto possa trovarsi nuovamente ad una condizione ante notifica. Per queste ragioni si ritiene che limitatamente a tale aspetto l'attuale formulazione debba essere superata.

Considerazioni conclusive

16) La sicurezza è un obiettivo strategico del Paese, condiviso dalle imprese della filiera delle telecomunicazioni. Le imprese già hanno sistemi di sicurezza e funzioni di Ricerca e Sviluppo in questo campo, le cui competenze possono fornire un utile contributo alla realizzazione del sistema di sicurezza nazionale cibernetica oggetto del provvedimento in esame.

17) L'approccio alla sicurezza deve essere basato sulla valutazione del rischio e su misure proporzionate a tale valutazione, con attenzione a mantenere tempi di esercizio delle attività operative dei soggetti obbligati compatibili con la programmazione aziendale e procedure snelle.

18) Il sistema delineato nel DL può creare un quadro normativo certo, purché sia caratterizzato con:

   a. la partecipazione degli Operatori alla definizione dei provvedimenti attuativi, in un rapporto di collaborazione con gli organismi di sicurezza che sia preliminare all'adozione delle regole e continuativo nell'esercizio del sistema,

   b. la valorizzazione di standard e certificazioni internazionali,

   c. l'attenzione alla definizione di tempi ristretti e procedure semplici, che non impattino in modo negativo sullo sviluppo delle reti di telecomunicazione.

19) Il sistema di sicurezza nazionale cibernetica adotta un approccio sistematico di medio-lungo periodo, integrando positivamente anche la disciplina del Golden Power vigente per le reti 5G, con cui è operato un raccordo esplicito. Entro un periodo orientativamente valutabile nell'ordine dell'anno i criteri di valutazione e quelli di certificazione su cui si basa la sicurezza saranno ricondotti ad unitarietà, con evidenti benefici in termini di coerenza del sistema, anche alla luce di quanto premesso in relazione al ruolo delle dotazioni di utente nelle reti 5G.

20) Importante dare stabilità al sistema, adottando nei tempi previsti i provvedimenti attuativi e non modificando le tempistiche previste nella disciplina Golden Power, rispetto alla quale l'intervento da fare può eventualmente essere quello di semplificazione delle procedure, già previsto dalla norma.

21) Il ruolo del CVCN sarà di snodo fondamentale del sistema e dati i compiti affidatigli dal DL potrebbe essere il luogo più adatto per sviluppare una collaborazione di tipo

tecnico con il settore privato ed i soggetti obbligati, anche attraverso la gestione del sistema di laboratori di ricerca accreditati.

22) Si apprezza il raccordo con le procedure di notifica dei perimetri applicativi della direttiva NIS e delle norme di sicurezza contenute nel Codice delle Comunicazioni Elettroniche.

23) Si riscontra un elemento di seria criticità in relazione alla possibilità di modificare le autorizzazioni rilasciate sino a 60 giorni dall'emanazione del DPCM contenente le misure che garantiscono gli "elevati livelli di sicurezza": tale disposizione introduce una significativa incertezza per le aziende, nonostante queste abbiano adempiuto agli obblighi ed alle prescrizioni già ricevute in seguito alla notifica. Al riguardo si ravvisa la necessità di un approfondimento congiunto e di una conseguente riformulazione al fine di rendere compatibile, in una prospettiva dinamica e di sostenibilità, le imprescindibili esigenze di sicurezza con il regolare esercizio dei piani di realizzazione delle infrastrutture 5G.