

**Audizione nelle Commissioni IX Trasporti, Poste e telecomunicazioni e I Affari Costituzionali del Gruppo Ferrovie dello Stato sull'esame del DdL C. 2100 di conversione del Dl n. 105 del 2019, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.**

Illustri Presidenti, Illustri Onorevoli,

desidero anzitutto ringraziarVi personalmente e per conto dell'Amministratore Delegato del Gruppo FS per l'opportunità che abbiamo oggi di fornire il nostro punto di vista in merito al decreto-legge sulla sicurezza nazionale cibernetica, un tema senza dubbio prioritario e centrale nello scenario tecnologico attuale.

Il Gruppo Ferrovie dello Stato Italiane è una delle più grandi realtà industriali del Paese, che conta circa 83mila dipendenti attivi nelle diverse società controllate che operano in quattro settori:

- ✓ **Trasporto:** include le società che svolgono attività di trasporto passeggeri e/o merci su ferro, strada o via mare;
- ✓ **Infrastruttura:** comprende le società che curano la manutenzione, la gestione e lo sviluppo dell'infrastruttura ferroviaria e stradale, nonché i servizi di collegamento via mare con le maggiori isole;
- ✓ **Servizi immobiliari:** comprende le società che gestiscono i principali scali ferroviari e che si occupano della gestione e valorizzazione del patrimonio immobiliare del Gruppo;
- ✓ **Altri servizi:** comprende le società che gestiscono attività non direttamente connesse all'esercizio ferroviario (gestione amministrativa, building e facility management, leasing, factoring, certificazione sistemi trasporto, ecc.).

Il nostro principale obiettivo è cercare di garantire sempre la migliore qualità del servizio in termini di presenza capillare sull'intero territorio nazionale, nel rispetto dei più alti standard qualitativi nazionali ed internazionali di sicurezza di reti, sistemi e servizi attraverso l'impiego di un ampio e diversificato panorama tecnologico.



Rilevo preliminarmente che il decreto legge 21 settembre 2019, n. 105, oggetto di conversione, istituisce il perimetro di sicurezza nazionale cibernetica con l'obiettivo di:

- ✓ disporre, di un sistema di organi, procedure e misure, che consenta una efficace valutazione sotto il profilo tecnico della sicurezza degli apparati e dei prodotti;
- ✓ prevedere il raccordo con le disposizioni in materia di valutazione della presenza di fattori di vulnerabilità che potrebbero compromettere integrità e sicurezza delle reti 5G e dei dati che vi transitano;
- ✓ disporre anche dei più idonei strumenti d'immediato intervento che consentano di affrontare con la massima efficacia e tempestività eventuali situazioni di emergenza in ambito cibernetico.

Ciò posto, il Gruppo Ferrovie dello Stato Italiane quindi condivide e supporta l'azione del legislatore al fine di innalzare il livello di sicurezza dei sistemi ricadenti nel Perimetro cibernetico. Auspica tuttavia che il testo possa essere opportunamente modificato, pur conservandone ratio, contenuti e finalità.

Nel ringraziare quindi per l'opportunità che oggi ci viene data, forniamo alcune osservazioni.

**Una prima osservazione di carattere generale, riguarda l'auspicabile costituzione di uno specifico Cloud Service Provider Nazionale per l'erogazione dei servizi identificati nel Perimetro di Sicurezza Nazionale.** In tal modo si potrebbe evitare di ricorrere alle attuali soluzioni tecnologie "in Cloud" fornite attraverso data center localizzati anche fuori dal territorio nazionale.

**Quanto all'ambito di applicazione,** con il DPCM previsto al **comma 2 dell'articolo 1**, è previsto che si proceda all'individuazione dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica. Le reti, i sistemi informativi ed i servizi informatici presenti sul territorio possono variare molto da soggetto a soggetto a seconda delle funzioni e delle attività svolte, che possono essere più o meno sensibili sotto il profilo della sicurezza. **Sarebbe pertanto opportuno inserire la possibilità per il soggetto attuatore di poter distinguere tra i vari**



**soggetti obbligati al rispetto della normativa in questione, in modo da regolare in maniera proporzionale e ragionevole l'applicazione della disciplina sulla cyber security e prevedere, se del caso, anche deroghe espresse a tale applicazione.**

Per quanto di competenza si rileva, tra l'altro, come il settore ferroviario sia caratterizzato da standard e requisiti di sicurezza definiti attraverso una dettagliata disciplina europea e nazionale e, nel suo ambito, da una molteplicità di situazioni. **Sarebbe pertanto auspicabile una definizione selettiva dei criteri di assoggettamento al perimetro cibernetico** con riferimento quindi non a tutte le società del Gruppo FS o alle società che lo compongono nella loro interezza, ma ai singoli sistemi di cui le stesse dispongono.

**Quanto all'elenco delle reti, dei sistemi informativi e dei servizi informatici di cui all'art. 1, comma 2, lett. b) del decreto, comprendere nello stesso anche i relativi aspetti architeturali e componentistici di dettaglio rischia di trasformarsi in un adempimento di difficile realizzazione da parte dei soggetti obbligati e probabilmente sproporzionato rispetto all'obiettivo di tutela della sicurezza nazionale.** Sarebbe pertanto utile e auspicabile **adeguare le informazioni da fornire alle specificità dei settori interessati.**

**Con riferimento a quanto previsto dall'art. 1, comma 3, si ritiene auspicabile che le procedure di notifica degli incidenti e che le misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici siano stabilite in coerenza con quanto disposto dal quadro normativo europeo in materia di *Cyber Security*, e che siano ispirati al rispetto dei requisiti definiti negli standard internazionali maggiormente accreditati (es. ISO, IEC, NIS).**

A tale proposito è da tener presente che **la sostituzione di apparati o prodotti, quindi l'ipotesi di intervenire su impianti e sistemi in esercizio**, secondo standard attualmente non previsti a livello europeo, considerati i possibili impatti sulle società del Gruppo Ferrovie dello Stato Italiane in termini di numerosità di impianti, richiederebbero ingenti risorse finanziarie e adeguati tempi di implementazione.



**Quanto all'elaborazione delle misure di intervento previste dall'art. 1, comma 4, come abbiamo già avuto modo di sottolineare in apertura, il settore dei trasporti è ampiamente disciplinato sia a livello nazionale che europeo. Sarebbe pertanto auspicabile che il Ministero delle infrastrutture e dei trasporti partecipasse alla fase di redazione delle misure di intervento.**

**Venendo infine alle modalità di affidamento delle forniture - disciplinate dall'art. 1, comma 6, lett. a) – osserviamo come la norma preveda un potere di imposizione di condizioni e test sui sistemi informativi da parte del CVCN che potrebbe addirittura arrivare a portare al non affidamento del contratto di tali prestazioni. Questa disposizione introdurrebbe una forte incertezza sulle tempistiche di affidamento, anche in contrasto con altre normative. È pertanto auspicabile che il CVCN fornisca indicazioni per la redazione dei bandi di gara rinviando la fase di verifica al momento della realizzazione e del collaudo dei sistemi.**

Ringraziando ancora per l'opportunità offertaci, resto a disposizione insieme ai colleghi oggi presenti per rispondere alle Vostre eventuali domande.