Audizione Fastweb nell'ambito dell'analisi del Decreto Legge recante Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica

Camera dei Deputati – Commissioni riunite I (Affari Costituzionali) e IX (Trasporti, Poste e Telecomunicazioni)

Onorevole Presidente, Illustri Deputati,

Vi ringrazio per averci offerto la possibilità di esprimere la nostra opinione in merito ad un tema centrale sia per lo sviluppo del settore delle Telecomunicazioni che per il Paese, come quello della sicurezza delle reti. Siamo convinti che adottare un quadro coerente in relazione alle misure da implementare per garantire l'integrità delle reti e sicurezza dei dati ivi trasmessi sia di primaria importanza nello scenario tecnologico presente e, ancor più, in quello futuro.

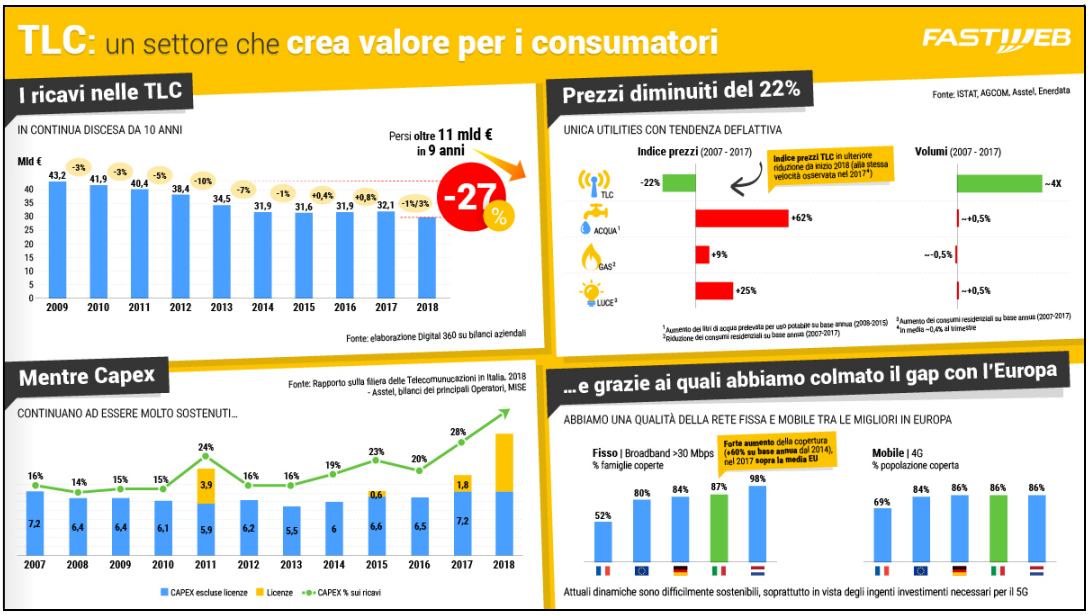
Fastweb condivide, pertanto, l'attenzione che il decisore pubblico, in questa fase, sta dedicando a tale tema ed è lieta di poter fornire il proprio contributo in questa sede.

Crediamo sia utile prima di entrare nel merito degli aspetti legati al Decreto Legge in esame, fare una rapida introduzione per rappresentare alcune criticità relative al nostro settore – di cui necessariamente si dovrà tenere conto – e per rappresentare come la sicurezza delle reti sia già oggi una priorità assoluta di aziende come Fastweb.

Quello delle Telecomunicazioni è un settore che ha dato tanto al Paese non solo in termini occupazionali, ma anche di investimento e di sviluppo tecnologico. Con l'avvento delle reti 5G l'apporto del nostro settore a beneficio dello sviluppo economico e sociale del Paese sarà sempre crescente (pensiamo ad esempio alla possibilità di monitorare da remoto i pazienti attraverso apparecchiature collegate all'ospedale in 5G, con un significativo miglioramento della vita dei pazienti ed un notevole risparmio per le aziende ospedaliere che riescono così a ridurre i tempi di degenza in ospedale o al monitoraggio degli edifici di interesse storico-artistico attraverso l'utilizzo di sensori per controllare in tempo reale lo "stato di salute" degli edifici di interesse storico-artistico consentendo di intervenire in misura preventiva evitando rischi di stabilità strutturale).

Ma il 5G è solo l'ultima puntata di una storia di sviluppo ed innovazione. Per dare una dimensione di quanto le Telecomunicazioni abbiano contribuito allo sviluppo del nostro Paese, riportiamo di seguito una figura dalla quale emerge chiaramente quanto valore abbia creato il nostro Settore. I dati riportati in

figura evidenziano come a fronte di reti sempre più performanti, grazie alla robusta dinamica concorrenziale i prezzi dei servizi di telecomunicazione, in dieci anni, siano addirittura diminuiti del 22%, al contrario di quanto invece è successo in altri settori in cui i prezzi hanno avuto una dinamica assolutamente opposta.



Una diminuzione costante dei prezzi che ha generato a sua volta una netta contrazione dei ricavi: negli ultimi 10 anni i ricavi sono diminuiti di ben il 27%. Si tratta di 11 miliardi a cui il settore ha rinunciato e che corrispondono ad un beneficio diretto per le famiglie. Il tutto in un contesto in cui, invece, gli investimenti continuano ad essere più che sostenuti, creando valore due volte: le prestazioni per i consumatori aumentano e il settore genera un indotto rilevantissimo, contribuendo a PIL e ad occupazione.

Si stimano nel settore investimenti annui di circa 7 miliardi di euro, una percentuale pari a circa il 20% dei ricavi, che aumentano considerevolmente in corrispondenza delle aste per le frequenze.

Fastweb fa più che la sua parte, reinvestendo annualmente circa il 30% dei propri ricavi in infrastrutture. Grazie a tali investimenti, la rete telefonica italiana, sia mobile sia fissa, è notevolmente migliorata in termini qualitativi vedendo pressoché colmato il divario rispetto ai principali Paesi europei in termini di copertura (30 Mega per l'87% delle famiglie italiane e l'86% di popolazione coperta in 4G).

Se questo vuol dire che abbiamo garantito a famiglie ed imprese servizi sempre più performanti a prezzi più bassi, c'è un lato negativo della medaglia: con ricavi e margini in continua contrazione a fronte di investimenti sempre più consistenti, il settore ha una sostenibilità critica.

Ci auguriamo dunque che, proprio in virtù del contributo rilevantissimo dato dal Settore all'innovazione e della difficoltà che esso attraversa, sui temi che discutiamo oggi, **si riesca a raggiungere una soluzione equilibrata in modo da garantire la sicurezza ma anche la possibilità di continuare a innovare e a sviluppare servizi per le famiglie e per le imprese.**

Appare doveroso sottolineare come la sicurezza delle reti non nasce certo con il 5G ma è un tema di cui le aziende come la nostra e Fastweb in particolare si preoccupano in modo costante da sempre. Per un operatore di Telecomunicazioni è infatti, fondamentale, garantire la sicurezza e l'inviolabilità delle comunicazioni e dei dati dei nostri utenti nonché la robustezza e resilienza delle reti, alla luce del fatto che la connessione ad Internet è sempre più pervasiva, in tutti i settori.

Fastweb, che oltre a fornire servizi di accesso ai clienti residenziali, è tra i principali fornitori di servizi al mondo della Pubblica Amministrazione e delle grandi aziende, ha da tempo adottato meccanismi e procedure all'avanguardia che garantiscono la sicurezza delle proprie reti: siamo stati il primo operatore italiano a ricevere, nel 2007, la certificazione internazionale di sicurezza ISO 27001 per **il proprio sistema di gestione della sicurezza a protezione dell'intera rete e dell'erogazione dei servizi.**

Abbiamo un'unità organizzativa molto consistente che si occupa di Sicurezza e che risponde, per la delicatezza e strategicità di tale compito, direttamente al CEO definendo gli standard tecnici di sicurezza e le procedure da seguire in tutte le fasi di vita della rete: dalla fase di progettazione (in cui applichiamo il principio della *"security by design")* alla fase di procurement (nella quale abbiamo controlli stringenti per garantire la qualità e sicurezza dei prodotti e servizi che acquistiamo dai partner), di realizzazione e infine di esercizio della rete stessa.

La progettazione delle reti, ad esempio, viene sempre fatta sulla base di diversi protocolli e standard specifici, quali ad esempio quello di *"segregazione e compartimentazione delle reti"*: ovvero la suddivisione della rete in diversi compartimenti con l'applicazione di regole e tecnologie (es. ACL – *Access Control List*; *firewall*) finalizzate a controllare in modo rigido la comunicazione tra i diversi compartimenti della rete (es. *segregazione*). I meccanismi di segmentazione e separazione consentono di isolare gli ambiti di azione del personale che vi opera, garantendo così che ciascuno abbia accesso esclusivamente ai componenti sui quali è chiamato ad intervenire e non all'intero sistema e bloccando quindi qualsiasi scambio di traffico non esplicitamente autorizzato.

Con riferimento, infine, all'esercizio della rete ed erogazione del servizio, fin dal 2000 **Fastweb dispone di un Network Operations Centre (NOC)**, centro operativo attivo 24 ore su 24 che ha il compito di

monitorare le prestazioni e il buon funzionamento della rete e gestire eventuali anomalie o incidenti. Dal 2009 **Fastweb ha affiancato al NOC un *Security Operations Centre* (SOC)***:* un presidio operativo attivo 24 ore su 24 interamente dedicato alla sicurezza con il compito di monitorare in tempo reale tutta la rete e tutti i sistemi informatici dell'azienda per rilevare tempestivamente tentativi di abuso o di attacco. Il SOC registra e raccoglie in tempo reale eventi da tutti i punti della rete elaborando circa 500 milioni di segnali ogni giorno e individuando tempestivamente anomalie e potenziali attacchi.

Il tema della cybersecurity insomma è fortemente presidiato perché il tema della sicurezza è fondamentale già oggi, non solo domani con il 5G. Il Security Operation Center gestisce e blocca ogni anno diverse migliaia di attacchi di cybersecurity: da quelli più comuni – ad esempio gli attacchi i ddos in grado di mandare in tilt un'azienda, o infrastrutture critiche come ospedali e aeroporti, in pochi secondi - in cui a quelli più *"innovativi"*. Più volte al giorno insomma i nostri esperti di sicurezza intercettano degli attacchi informatici, rivolti alla nostra rete, o a nostri clienti specifici, e li gestisce in modo da garantire la continuità operativa della rete nostra e dei nostri clienti così come la sicurezza dei loro dati.

I nostri esperti di sicurezza informatica interagiscono in modo costante e strutturato con le Istituzioni preposte a ciò, in modo da generare circoli virtuosi di informazione ed essere costantemente aggiornati su nuovi rischi informatici. Questo per sottolineare come il tema sia tutt'altro che limitato all'acquisto di componenti extra-europee per il 5G e la vulnerabilità eventuale prescinde da chi ha fornito un certo apparato. Il tema della sicurezza informatica dovrà essere sempre più pervasivo e gestito in modo dinamico dalle aziende. Da chiunque vengano acquisite le parti della nostra rete, adottiamo protocolli tali da garantire la massima sicurezza in tutte le fasi.

Ovviamente, in un ecosistema in rapido cambiamento come quello della cybersecurity, anche i nostri meccanismi e processi di protezione sono in continua evoluzione e miglioramento ma vogliamo comunque sottolineare che **tutti i processi e i meccanismi a difesa delle reti che abbiamo adottato fino ad oggi hanno piena validità ed efficacia non soltanto per le tecnologie di rete fissa e mobili 3G e 4G, ma anche per il 5G e addirittura per le future evoluzioni**.

In tale scenario **il Decreto sul perimetro di sicurezza nazionale cibernetica, appare come un passo fondamentale** per due motivi:

- In primo luogo perché promette di **creare un contesto chiaro e trasparente** in cui gli operatori siano messi nelle condizioni di conoscere a priori i criteri che le istituzioni ritengono necessari per

garantire la sicurezza delle reti, con un approccio più di sistema che è esattamente quello che abbiamo appena descritto.

- In secondo luogo perché opera un raccordo con la disciplina della Golden Power e gli stessi criteri saranno utilizzati per la valutazione degli accordi di procurement di tutti i sevizi e prodotti 5G. La conoscenza a priori di tali criteri – cosa che ad oggi manca – consente a noi aziende di **avere una maggiore cognizione sulle condizioni da rispettare** e dunque incorporare tali requisiti già nei bandi di gara e nella negoziazione del contratto con il vendor, garantendo la massima sicurezza e al tempo stesso accelerando i tempi di sviluppo delle reti.

Per diventare pienamente operativo però il Decreto necessita di alcuni provvedimenti attuativi, in particolare dovranno essere emanati, in un periodo complessivo di circa un anno, 3 Decreti della Presidenza del Consiglio dei Ministri ed un Regolamento. Pertanto sarà proprio tale fase di stesura ed elaborazione dei suddetti provvedimenti cruciale, poiché è proprio in questo momento che si getteranno le basi per lo sviluppo di tutto il comparto nei prossimi anni. Vista la rilevanza di tale momento riteniamo che sia **fondamentale:**

a) **accelerare il più possibile la redazione di tali decreti, per eliminare al più presto quest'area di indeterminatezza;**

b) **rendere gli operatori parte attiva di questo processo: proprio alla luce delle competenze specifiche in materia di cibersicurezza che abbiamo sviluppato in questi anni, riteniamo di poter fornire un contributo fondamentale per costruire, insieme agli organismi competenti, un perimetro chiaro e definito di regole, norme, requisiti e standard da rispettare** che sia coerente da un lato con le esigenze degli operatori e dall'altro con l'obiettivo di tutela della sicurezza nazionale del Governo.

Vediamo due aree di potenziale criticità nel Decreto Legge in fase di conversione:

- In primo luogo **riteniamo fondamentale che il processo di monitoraggio e controllo da parte delle istituzioni relativo al perimetro di sicurezza sia il più possibile standardizzato e con tempistiche contenute.** La procedura di notifica per l'esercizio della Golden Power sui 5G – se dovesse essere estesa oltre i 15 giorni + 10 previsti dalla norma attuale – rischierebbe di diventare un serio ostacolo allo sviluppo delle reti. Grazie ad alcune scelte fatte in questi anni, l'Italia ha un vantaggio sul 5G, che può essere facilmente perso. Il rispetto di tempistiche accettabili (al momento la procedura di notifica allunga i tempi di circa 1 mese) è fondamentale per l'avvio della

commercializzazione e il recupero degli investimenti già messi in campo con l'asta delle frequenze. Pertanto si auspica fortemente che i **limiti procedurali previsti** sia per l'attuale processo della Golden Power (ovvero 15 giorni + 10 giorni per la richiesta di ulteriori informazioni) che per gli altri processi di valutazione tramite il CVCN (pari a 30 giorni) **non subiscano eventuali estensioni in fase di conversione del Decreto.**

- Un altro **tema che genera non poca incertezza per gli operatori riguarda la possibilità che le condizioni e le prescrizioni** definite nelle autorizzazioni rilasciate sino all'entrata a regime del Regolamento, **possano essere riviste ed integrate entro 60 giorni**, *"anche prevedendo, ove necessario, la sostituzione di apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza."* Tale previsione introduce un forte elemento di incertezza: pur avendo avuto l'autorizzazione a procedere con l'acquisto di beni e servizi relativi ad operazioni già notificate, gli operatori potrebbero improvvisamente trovarsi a dover modificare e quindi sostituire apparati già installati sulle proprie reti, con **gravi ripercussioni sull'operatività del servizio e con notevoli costi per la sostituzione degli apparati.**