EXECUTIVE SUMMARY

La permanenza forzata dei cittadini nelle proprie abitazioni causata dal Covid-19 ha avuto effetti notevoli sul sistema nazionale di telecomunicazione, determinando un aumento esponenziale del traffico dati soprattutto per via della fruizione dei contenuti di streaming video, dell'utilizzo di piattaforme videoludiche, oltre che per il massiccio ricorso da parte delle aziende allo smart working e alla formazione a distanza per gli studenti. Se diversi studi, tra cui lo stesso monitoraggio del traffico effettuato dall'Agcom, hanno mostrato chiaramente la correlazione tra l'entrata in vigore delle disposizioni atte a limitare la mobilità dei cittadini italiani e l'aumento del traffico di rete, dal punto di vista della resilienza, la rete nazionale è comunque riuscita a gestire il sovraccarico senza recare grandi disagi all'utenza. È tuttavia necessario, anche alla luce delle recenti ricadute in termini di inondamento della curva dei contagi, non rallentare lo sforzo in termini di investimenti sulle infrastrutturazioni di rete. Questo discorso appare ancor più valido in ottica 5G. L'infrastrutturazione delle nuove reti può infatti giocare un ruolo fondamentale in un orizzonte di medio-lungo termine per la ripresa nazionale dopo il crollo dovuto al Covid-19 e alle limitazioni che ne sono conseguite e che ne potrebbero ulteriormente conseguire.

Il nuovo standard di trasmissione costituisce un'importante opportunità di sviluppo e crescita a livello planetario, in particolare per la sua capacità di abilitare applicazioni avanzate proprie dell'**Internet of Things**. GSMA stima che le reti 5G porteranno un contributo all'economia mondiale di circa $ 2,2 trilioni tra il 2024 e il 2034, una crescita trainata da utilities e manifattura (33%), servizi professionali e finanziari (30%), servizi pubblici (16%), Ict e commercio (14%). Per quanto riguarda le singole aree geografiche, le stime indicano che la crescita maggiore interesserà gli Stati Uniti (oltre $ 650 miliardi), seguiti da Europa ($ 480 miliardi) e Cina ($ 460 miliardi).

L'infrastrutturazione della rete 5G quindi, oltre ad essere un **fattore abilitante** per numerose nuove tecnologie, può rappresentare un importantissimo **volano per l'economia** anche grazie agli ingenti investimenti necessari per la sua implementazione. Una stima del fabbisogno complessivo necessario in Europa per l'ammodernamento delle reti e l'implementazione delle nuove è stata effettuato da I-Com incrociando dati della Commissione Europea e del GSMA. Dall'analisi emerge un impatto di €360 miliardi necessari per il c.d. *business as usual* (manutenzione e ammodernamento), circa €155 miliardi necessari per rispettare gli obiettivi stabiliti nel quadro

della Gigabit Society e €20-30 miliardi per l'acquisizione delle licenze 5G nell'Unione Europea. Il tema degli investimenti è legato inevitabilmente al dibattito relativo alla sicurezza delle reti e, in particolare, all'opportunità di utilizzare le tecnologie dei vendor extra-europei per quanto concerne le apparecchiature, per via del possibile impatto che eventuali restrizioni potrebbero generare sugli stessi investimenti e sulla riduzione dei benefici connessi alla diffusione del 5G. L'analisi di GSMA valuta i costi di eventuali restrizioni per l'Europa in €55 miliardi, dei quali €25 miliardi derivanti dalla riduzione della concorrenza e ulteriori €30 miliardi dovuti alla sostituzione delle apparecchiature. In totale gli investimenti necessari per l'implementazione delle reti 5G in Europa sono stimati quindi in € 535 miliardi in caso di partecipazione dei fornitori extraeuropei e in € 590 miliardi in caso di esclusione degli stessi.

Per quanto concerne lo **stato di diffusione delle infrastrutture di rete mobile** nelle principali economie avanzate globali, si osserva come la Cina sia il Paese che nel 2019 ha fatto registrare la quota maggiore di infrastrutture 4G sul totale delle reti. Per quanto riguarda l'Europa, più della metà delle infrastrutture di rete mobile continentale è 4G, anche se resiste ancora una quota rilevante di connettività 2G (14%). Nello studio, GSMA effettua anche una proiezione del mix tecnologico mobile al 2025, da cui emerge come l'Europa, con il 34% di copertura 5G, sarebbe notevolmente indietro rispetto a Nord America (48%) e Cina (47%), che viaggeranno quasi di pari passo, in termini di copertura della rete di quinta generazione.

Relativamente all'attuale diffusione del 5G, I-Com ha stimato il **numero di utenti attivi** nelle principali aree sviluppate del globo. Dall'analisi emerge che il Paese che può vantare la maggior diffusione dei servizi di quinta generazione in relazione alla popolazione è la Corea del Sud (16.744 ogni 100 mila abitanti), seguita a breve distanza dalla Cina (12.790). Stati Uniti ed Europa risultano notevolmente indietro, rispettivamente con appena 2.313 e 779 utenti 5G ogni 100.000 abitanti. Lo stato attuale e la possibile evoluzione del mercato dei servizi 5G mostra quindi la necessità per l'Europa di accelerare in termini di infrastrutturazione e di offerta di servizi attrattivi per gli utenti, incrementando e favorendo gli investimenti nelle reti anche per mezzo di politiche che agevolino le attività degli operatori di settore.

Allo stesso tempo, è importante notare come il *roll-out* delle reti 5G, che risulta quanto più strategico in considerazione del potenziale spostamento, da parte di molteplici settori industriali, di una quota crescente delle proprie attività su reti di nuova generazione, stia avvenendo in un contesto in cui la **c.d. "minaccia cibernetica"** mostra una relativa stabilizzazione. I dati forniti dal

Clusit sull'evoluzione degli attacchi informatici negli ultimi sei anni, sebbene complessivamente in crescita (nel 2019 +7,6% sul 2018), in particolare per via del *Cybercrime* (i crimini informatici), presentano una sensibile diminuzione per quanto concerne la *Cyber Warfare*. A tal proposito, anche la relazione sulla politica dell'informazione per la sicurezza 2019[1], pur non fornendo i dati in termini assoluti per ragioni di riservatezza, indica come le manifestazioni "critiche" del fenomeno evidenzino un numero complessivo di azioni "ostili" quasi dimezzato rispetto al 2018, dopo il picco registrato tra il 2017 e il 2018.

Nel corso degli ultimi due anni, il dibattito relativo alla sicurezza nazionale si è focalizzato sull'opportunità o meno di utilizzare componentistica proveniente dagli operatori extra europei ed in particolare cinesi. A livello italiano, tale possibile discriminazione è ulteriormente complicata dall'**alto grado di internazionalizzazione** che si riscontra anche tra i **network providers**, in gran parte a capitale estero. Nel dettaglio, nel mercato italiano sono presenti americani e francesi tra i principali azionisti dell'ex incumbent Tim (al momento al centro della possibile transizione verso la rete unica), ancora americani in Linkem, francesi in Iliad, britannici in Vodafone, cinesi in Wind Tre e svizzeri in Fastweb.

Inoltre, per quanto concerne specificamente la **componentistica per il 5G**, si osserva come il perimetro relativo alle imprese che producono tali apparecchiature sia piuttosto ristretto, comprendendo prevalentemente Ericsson (Svezia), Nokia (Finlandia), Huawei (Cina), Samsung (Corea del Sud) e ZTE (Cina), che insieme compongono circa il 75% del mercato della fornitura di apparecchiature di rete. Tale concentrazione rende quindi piuttosto complicato attuare una discriminazione per nazionalità di provenienza dei fornitori, a fronte della previsione di misure specifiche per mitigare i rischi a 360 gradi.

A livello tecnico, sono in fase di sviluppo una **serie di misure per innalzare la sicurezza delle reti 5G**. Dall'analisi condotta emerge che due fattori, in particolare, diventeranno sempre più critici nelle evoluzioni future: **velocità e automazione**. Se è verosimile che la velocità di identificazione delle nuove minacce verrà progressivamente migliorata, la creazione di difese automatizzate per garantire la più rapida risposta possibile in caso di attacco potrebbe diventare addirittura indispensabile. Inoltre, poiché il 5G incorporerà progressivamente servizi che riguardano

[1] Sistema di Informazione per la Sicurezza nella Repubblica, "Relazione sulla politica dell'informazione per la sicurezza 2019", febbraio 2020

direttamente la vita e il benessere dei cittadini, come la sanità e l'automotive, la sicurezza delle sue reti travalicherà il valore economico, pertanto le sue metriche trascenderanno quelle che tradizionalmente fanno capo alla sicurezza dei sistemi IT. Per tali ragioni, la sicurezza di tali reti è divenuta e diverrà sempre più una questione di interesse governativo, e potrà essere complicata dal fatto che molteplici autorità (altre nazioni, enti internazionali) vorranno imporre una serie di requisiti diversificati a diversi livelli e/o in diverse parti del mondo. Pertanto la sicurezza del 5G, in quanto standard globale, rischia di dover sottostare, oltre che ad una lunga serie di funzioni e parametri tecnici, ad un complesso e diversificato ambiente normativo.

Anche per fronteggiare la possibile tendenza alla balcanizzazione delle normative sulla sicurezza delle reti, gli operatori, già consorziati a livello mondiale dai tempi della diffusione del GSM, hanno proseguito le proprie operazioni di **standardizzazione internazionale** anche con il 3G ed il 4G, e sono al lavoro per trovare procedure comuni anche il 5G. Il 3GPP (*3rd Generation Partnership Project*), che già aveva condotto un'operazione di portata globale sul 3G, assicurando una completa interoperabilità tra le reti dei diversi operatori e nei diversi Paesi, ha introdotto la **SECAM (Security Assurance Methodology)**, un processo usato per misurare le caratteristiche relative alla sicurezza dei prodotti di rete, definendo attività e ruoli dei diversi soggetti. Il processo di valutazione SECAM comprende sia l'analisi dei processi con cui i fornitori delle apparecchiature di rete sviluppano i propri prodotti, sia la valutazione della gestione del loro ciclo di vita. A ciò si aggiunge la creazione di requisiti di sicurezza e specifiche per i test, denominate *Security Assurance Specifications* (SCAS).

Parte dei compiti di valutazione e accreditamento sono stati assegnati alla principale associazione a livello mondiale che raggruppa gli operatori di rete e i vendor, la GSM Association (GSMA). Per svolgere questi compiti, GSMA ha definito un proprio schema, il ***Network Equipment Security Assurance Scheme*** **(NESAS)**, che consiste in un insieme comune di requisiti a garanzia della sicurezza, finalizzati ad introdurre una base comune a tutti i prodotti, indipendentemente dai requisiti individuali del singolo Stato. Tali requisiti e l'intero processo di certificazione sono pensati per essere utilizzati a livello globale, lasciando che i fornitori di apparecchiature si concentrino sulla creazione e sul miglioramento del prodotto. Tra i vantaggi del NESAS si osservano la possibilità di evitare la moltiplicazione dei requisiti di sicurezza cui i fornitori dovrebbero conformare le proprie apparecchiature, il venir meno della necessità per gli operatori di rete di sviluppare specifici requisiti di sicurezza e, per i governi e le autorità nazionali, l'universale applicabilità del sistema di sicurezza e la possibilità di farlo interfacciare con le certificazioni nazionali. In questo contesto,

GSMA ha preparato una proposta da sottoporre alla Commissione europea per rendere il NESAS uno schema candidato per la certificazione del 5G.

A livello internazionale, osservando l'evoluzione delle scelte degli operatori di rete dei maggiori Paesi europei relative alla scelta dei fornitori di apparecchiature di rete 5G, si osserva come questi si stiano adeguando ai nuovi scenari complessivi del mercato. Infatti, se l'upgrade al 5G è oramai considerato un *must-have* che nessun operatore, se vuole rimanere competitivo, può permettersi di non avere, la regolamentazione europea e in particolare nazionale rappresenta un elemento che influisce sempre più nelle loro scelte.
Le posizioni di mercato sono infatti direttamente collegate alla compatibilità delle apparecchiature, ed elementi di decisiva importanza sono altresì dati dai rapporti internazionali che, in molti casi, risultano determinanti nella scelta e nel numero di fornitori ammessi in ciascun Paese. Dalla prolungata **analisi condotta sulle scelte degli operatori di rete nei 4 maggiori Paesi europei, oltre all'Italia**, si è inizialmente osservata la generale tendenza ad investire in upgrade della rete al 5G attraverso aggiornamenti delle apparecchiature preesistenti e rinnovi degli accordi con i fornitori precedenti. Tuttavia, in particolare negli ultimi mesi, in molti casi i rinnovi sono stati resi impraticabili da ragioni regolamentari, con Paesi che hanno optato per l'esclusione ex-ante dei *vendor* extra-europei per ragioni legate alla sicurezza cibernetica. Il Regno Unito, ad esempio, ha disposto la rimozione delle antenne Huawei entro il 2027, nonostante le forti perplessità degli operatori di rete nazionali, mentre in Germania il Governo ha stabilito regole più severe per tutti i *vendor* extra-UE, creando iter burocratici con criteri di sicurezza particolarmente stringenti. Una posizione simile è stata assunta anche dalla Francia che, sebbene abbia negato esclusioni ex-ante, si è riservata la possibilità di valutare autorizzazioni caso per caso per i fornitori extra-europei. Il governo spagnolo, invece, allo stato attuale non prevede l'esclusione di nessun operatore dal mercato, dando maggiore peso al raggiungimento dell'obiettivo di realizzare la copertura 5G per il 75% del territorio nazionale entro tempi molto brevi.
Dalle tendenze e dai risultati relativi alla sottoscrizione degli accordi a livello mondiale, si rileva comunque come il mercato si mantenga piuttosto ristretto con appena 4-5 fornitori che si contendono il 75% del mercato europeo. OIn tale contesto, appare certo che l'esclusione a priori di fornitori extra-europei rischi di produrre esiti problematici a livello di fornitura, con inevitabili ritardi nelle operazioni di installazione, di costi di implementazione e infine di innovazione complessiva del sistema.

Se dal punto di vista tecnologico e di mercato il tema della sicurezza appare particolarmente complesso, non meno articolato e difficoltoso l'**iter normativo che sta accompagnando il settore sia a livello comunitario che nazionale**.

Con questa consapevolezza, a livello di **Unione Europea**, l'attenzione per lo sviluppo del 5G e la creazione di un ecosistema sicuro è massima e lo dimostra l'ampia serie di iniziative messe in campo dalla Commissione negli ultimi anni. Ed infatti, il 2016 ha visto l'adozione della **direttiva NIS** (della quale è stata avviata l'attività di revisione mediante il lancio di una consultazione pubblica la cui prima fase si è conclusa il 13 agosto scorso) con la quale per la prima volta è stato definito un quadro organico della materia, affrontando le sfide in materia di cyber sicurezza e rivoluzionando la resilienza e la cooperazione in Europa, mentre il "Cybersecurity Act" del 2019 (Regolamento n. 881/2019) ha disciplinato il ruolo ed i poteri dell'ENISA, ha fissato un quadro per l'introduzione di sistemi europei di certificazione della cybersecurity ed ha istituito il Gruppo europeo per la certificazione della cybersecurity.

È sempre del 2019 la **Raccomandazione n. 2019/534 sulla cybersecurity delle reti 5G** con la quale la Commissione ha evidenziato i rischi di cybersecurity rispetto a tali reti e presentato orientamenti sulle opportune misure di analisi e gestione dei rischi a livello nazionale, sullo sviluppo di una valutazione dei rischi coordinata a livello europeo e sulla definizione di un processo per lo sviluppo di un insieme di strumenti comuni volti a garantire la migliore gestione dei rischi.

In attuazione di quanto previsto da tale raccomandazione, il 9 ottobre 2019 è stata pubblicata dal gruppo di cooperazione NIS una **relazione sulla valutazione coordinata a livello di UE dei rischi per la cibersicurezza delle reti di quinta generazione** la quale, partendo dai risultati delle valutazioni nazionali dei rischi per la cibersicurezza, effettuate da tutti gli Stati membri dell'UE, ha individuato le minacce più rilevanti e i principali autori di tali minacce, le risorse più sensibili e le principali vulnerabilità (di natura tecnica e di altro tipo), nonché diversi rischi strategici. Ad integrazione di tale rapporto degli Stati membri, il 21 novembre 2019, l'ENISA ha pubblicato un Threat Landscape for 5G Networks, in cui, sulla base anche del contributo offerto da gruppi e organismi di standardizzazione 5G e stakeholder 5G come operatori, fornitori, organizzazioni nazionali e internazionali, sono state individuate le sfide e le possibili minacce nella sicurezza delle reti 5G, è stato definito un diagramma degli asset, formulata una tassonomia delle minacce, identificata l'esposizione dei diversi asset e valutate le motivazioni dell'agente di minaccia.

Il 2020 si è aperto invece con la pubblicazione, il 29 gennaio, della Comunicazione della Commissione "***Dispiegamento del 5G sicuro - Attuazione del pacchetto di strumenti dell'UE***" e del pacchetto di strumenti dell'UE (**Toolbox sul 5G**) da parte del gruppo di cooperazione NIS comprendente misure di attenuazione dei rischi, che tratta tutti i rischi individuati nella relazione coordinata sulla valutazione dei rischi individuando e descrivendo una otto misure strategiche ed undici tecniche, nonché di corrispondenti azioni di sostegno volte a rafforzare la loro efficacia, che possono essere attuate per attenuare i rischi individuati. Il 24 luglio il gruppo di cooperazione NIS, con il sostegno della Commissione e dell'ENISA, ha pubblicato una relazione sui progressi degli Stati membri nell'attuazione del *Toolbox* sulla sicurezza 5G nella quale si fa il punto sul livello di maturità raggiunto dai vari paesi nell'implementazione delle misure contenute nel *Toolbox*. Evidenziando come tre principali rischi individuati siano quello dell'errata configurazione delle reti, della mancanza di controllo all'accesso e di interferenze statali attraverso la catena di fornitura 5G.

Il quadro normativo che si sta passo dopo passo componendo a livello comunitario è chiaramente orientato a sostenere lo sviluppo e la sicurezza delle reti 5G. Tuttavia, per garantire all'Unione la capacità di competere e giocare un ruolo da protagonista a livello globale nello sviluppo del 5G, è cruciale, da un lato, che gli Stati membri rispettino quanto più possibile la roadmap tracciata già nel 2016 dalla Commissione con l'Action Plan e, dall'altro, che a livello più generale, l'Europa persegua obiettivi di armonizzazione ambiziosi, soprattutto in materia di standard e certificazioni, che assicurino quella semplificazione e quella chiarezza indispensabili a creare un ecosistema favorevole agli investimenti ed agevolare l'operato delle aziende operanti in diversi Stati membri.

Anche l'**Italia** si trova a giocare la propria partita nello sviluppo del 5G. Se dal punto di vista della roadmap tracciata dall'Action Plan il nostro Paese si posiziona tra i primi in Europa per aver già completato le procedure di assegnazione delle frequenze destinate al 5G, più complesso e farraginoso si sta, invece, rivelando il processo di composizione del quadro normativo a garanzia della sicurezza delle reti 5G. Ed infatti, dopo che il D.L. 25 marzo 2019, n. 22 (c.d. "**Decreto Brexit**"), convertito con modificazioni dalla Legge 20 maggio 2019, n. 41, ha esteso l'ambito applicativo dei poteri speciali (il c.d. "golden power") alle reti 5G, prevedendo l'applicazione del meccanismo di tutela dello Stato anche alle forniture di materiali e servizi, prevedendo l'obbligo di notifica in relazione a contratti o accordi aventi a oggetto l'acquisto di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti 5G che vedano coinvolti soggetti esterni all'Unione europea, il 21 settembre 2019 è stato varato il **decreto legge n. 105/2019**, convertito con la legge n. 133/2019, con il quale è stato istituito il **perimetro di sicurezza nazionale**

cibernetica. Si tratta di un decreto che delinea un percorso attuativo frazionato con scadenze temporali diversificate attraverso quattro decreti del Presidente del Consiglio dei ministri ed un regolamento attraverso i quali definire, tra l'altro, le modalità e i criteri procedurali di individuazione dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica e che, pertanto, saranno tenuti al rispetto delle misure e degli obblighi previsti dal decreto-legge, declinare i criteri con i quali i soggetti inclusi nel perimetro predispongono e aggiornano l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica, disciplinare le procedure di notifica degli incidenti, l'attività del CVCN e le attività di ispezione e verifica di MISE e Presidenza del Consiglio.

Il **primo DPCM (il n. 131 del 30 luglio 2020)**, dopo ampio dibattito, e dopo aver ricevuto, come da procedura delineata dal decreto legge, il parere del Consiglio di Stato e delle Camere, è stato pubblicato sulla Gazzetta Ufficiale del 21 ottobre, con ritardo rispetto alla tabella di marcia definita del decreto stesso complice, evidentemente, anche l'emergenza sanitaria in atto. Tale decreto ha individuato i criteri e le modalità per l'individuazione dei soggetti inclusi nel perimetro, ha declinato i concetti di funzione e servizio essenziale, ha selezionato i settori di attività in cui operano i soggetti da inserire nel perimetro, ha disposto l'istituzione di un Tavolo interministeriale per l'attuazione del perimetro ed ha fissato i criteri per la predisposizione e l'aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici.

Medio tempore, è stato proposto uno **schema di regolamento** (al vaglio del Consiglio dei Ministri), indispensabile ai fini dell'operatività del CVCN, che in attuazione del decreto istitutivo del perimetro, definisce le procedure, le modalità ed i termini da seguire ai fini delle valutazioni da parte dello stesso CVCN e dei centri di valutazione del Ministero dell'interno e del Ministero della difesa (CV), ciascuno nell'ambito delle rispettive competenze, in ordine all'acquisizione, da parte dei soggetti inclusi nel perimetro, di oggetti di fornitura rientranti nelle categorie individuate sulla base dei criteri dallo stesso indicati, i criteri di natura tecnica per l'individuazione delle categorie a cui si applica la procedura di valutazione delineata, le procedure, le modalità ed i termini con cui le Autorità competenti effettuano le attività di verifica e ispezione ai fini dell'accertamento del rispetto degli obblighi stabiliti nel decreto-legge e nei decreti attuativi.

Se il primo decreto è stato pubblicato con un ritardo di circa 7 mesi, complice, senza dubbio, anche l'emergenza sanitaria ancora in atto, e lo schema di regolamento sull'attività di CVCN e CV è ancora in fase embrionale e certamente genererà, per l'importanza delle questioni che disciplina, un ampio

dibattito, è prioritario accelerare per scongiurare il rischio che si generi un clima di generale incertezza in grado di impattare negativamente sugli investimenti e lo sviluppo delle reti 5G e di mettere a repentaglio la posizione d'avanguardia faticosamente guadagnata negli anni scorsi dal nostro Paese.