icom
istituto per la competitività

POLICY PAPER
Lo sviluppo del 5G in Italia tra competitività e sicurezza nazionale

1. La rivoluzione del 5G: use cases e impatto economico

Le reti 5G rappresentano una straordinaria opportunità di sviluppo e crescita a livello planetario. Si tratta, infatti, di un'evoluzione tecnologica in grado di garantire una velocità di trasferimento dei dati fino a 100 volte più veloce, ridurre fortemente la latenza avvicinandola allo zero, consentire di gestire un milione di dispositivi in 1 km^2, assicurare una maggiore longevità della batteria dei dispositivi e consentire di utilizzare diverse frequenze da 400 MHz a 100 GHz abilitando lo sviluppo di nuovi servizi e generando enormi benefici socio-economici. Siamo di fronte ad una tecnologia altamente performante ed innovativa che ridisegnerà dal profondo i servizi di connettività di tipo fisso (*wireless last mile* ad altissima capacità) e di tipo mobile (altissimi volumi di dati), abilitando la diffusione pervasiva di oggetti che avranno la capacità di interagire tra di loro e con l'uomo condividendo le conoscenze acquisite.
Il 5G svolgerà il ruolo di acceleratore per la trasformazione digitale delle aziende, abilitando lo sviluppo di nuovi servizi avanzati tra cui l'**IoT (*Massive Machine-type* e *Critical Machine-type*)** nonché ***l'Enhanced Mobile Broadband*** (e-MBB), che rappresenteranno i cluster applicativi in cui sarà più evidente l'impatto di tale tecnologia.
Nel cluster degli use-case *IoT Massive Machine-type*, in particolare, rientrano tutte le reti di sensori, contatori intelligenti, sensori per il monitoraggio remoto di asset strategici e strutture, con requisiti chiave in termini di durata della batteria superiore a 10 anni, densità di connessione supportata superiore al milione di unità per chilometro quadrato, affidabilità del servizio pari al 99,99%, ma senza SLA particolarmente sfidanti in termini di latenza e mobilità.
Negli use-case *IoT Mission Critical Machine-Type*, invece, si annoverano tutte quelle applicazioni che necessitano di performance particolarmente elevate in termini di affidabilità del servizio (99,99%), di latenza (~ inferiore ai 10ms) e di mobilità (anche superiore ai 500Km/h). Si pensi, ad esempio, al telecontrollo remoto di smart grid con requisiti di 8ms di latenza oppure, servizi IoT per treni ad alta velocità, con requisiti di mobilità di + 500 Km/h e latenza inferiore a 10 millisecondi, fino a servizi sanitari avanzati come la chirurgia da remoto ed il monitoraggio a distanza dello stato di salute dei pazienti (meno di 1ms di latenza e affidabilità stimata del 99,999%).

Tra i servizi avanzati appartenenti alla categoria dell'*Enhanced Mobile Broadband*, infine, rientrano tutte quelle applicazioni che prevedono tipicamente come requisiti chiave di supportare un throughput estremamente elevato (anche +10Gbps) e una latenza inferiore ai 5 millisecondi, fornendo al tempo stesso servizi affidabili, di qualità e altamente efficienti (si tratta, in particolare, di servizi legati all'offerta di esperienze avanzate di intrattenimento, video e automazione domestica come esperienze immersive di gaming, e-learning e remote-training etc.).

Da quanto esposto è chiaro che la piena espressione delle potenzialità dei *cluster IoT Critical Machine-type* e dei servizi in *Enhanced Mobile Broadband* esigono lo sviluppo delle piattaforme 5G che abiliteranno i requisiti essenziali per la loro applicazione in termini di latenza, user throughput, mobilità, densità di traffico, affidabilità del servizio e sicurezza.

L'evoluzione tecnologica del 5G consentirà lo sviluppo di applicazioni e servizi altamente innovativi in molteplici settori, tra i quali l'automotive, i trasporti, l'energia, la sanità e la manifattura.

Attualmente automotive e più in generale i trasporti sono i casi maggiormente citati, probabilmente per via della rivoluzione che comporterebbe la diffusione su larga scala di veicoli a guida (completamente) autonoma sia a livello di confort sia a livello di efficienza e produttività. Queste innovazioni, oltre a dispensare le persone da una attività quotidiana che può risultare faticosa, porterebbero a una gestione intelligente del traffico e a una drastica riduzione degli incidenti stradali. La SAE (*Society of Automotive Engineers*) ha classificato l'automazione delle auto secondo 6 tipologie, da quelle in cui il pilota svolge tutte le funzioni (livello 0) a quelle con qualche funzione automatizzata (livello 1) passando per le auto a guida semi autonoma (livello 2, come la Tesla S e la Mercedes Classe E,) fino a identificare 3 ulteriori tipologie di guida autonoma che variano per la necessità di supervisione umana in caso di imprevisto, le condizioni in cui sono in grado di gestire le operazioni (livello 4) fino all'automazione totale (livello 5) che identifica veicoli in grado di guidare in ogni situazione, indipendentemente da fattori quali la tipologia di strada e le condizioni climatiche.

Secondo uno studio Pwc, dal 2025 tutte le auto di nuova immatricolazione saranno "connesse", e tra queste le auto a guida semi-autonoma, cioè in grado di guidare da sole in determinate condizioni, saranno 33 milioni a livello globale. Le auto a guida completamente autonoma (livello 5) saranno disponibili solo dopo il 2025, e potrebbero raggiungere quota 12 milioni di unità vendute già nel 2030.

Lo studio supportato dalla Commissione Europea, "*Identification and quantification of key socio-economic data to support strategic planning for the introduction of 5G in Europe*", prevede che la diffusione del 5G determinerà benefici sostanziali nel settore dell'automotive a livello strategico, operativo, amministrativo e per i consumatori. Stimando una diffusione di 168 milioni di veicoli connessi nel 2025 e di 274 milioni nel 2030, si ipotizzano benefici strategici che arriveranno a € 20 miliardi l'anno nel 2030, benefici operativi (ovvero relativi alla produzione) per circa € 1,8 miliardi, benefici per i consumatori (assistenza ed entertainment) per € 22,7 miliardi e benefici amministrativi (es. sicurezza e

pronto intervento, riorganizzazione del traffico in caso di incidenti) per € 22,3 miliardi. In totale quindi, l'impatto potrebbe arrivare a quota € 42,2 miliardi nel 2025 e € 67,6 miliardi l'anno nel 2030.

Per quanto concerne il **settore energetico** la crescente complessità delle reti, generata dalla moltiplicazione degli attori, dalla decentralizzazione e dalla disintermediazione, richiede un incremento delle capacità di calcolo e degli algoritmi di elaborazione e necessita che le operazioni avvengano in tempo reale. Tale dinamica determina una crescente interdipendenza dalle reti di telecomunicazione, rendendo il 5G uno dei principali fattori abilitanti della "smartificazione" delle reti energetiche in direzione delle smart grid. Ciò porterà a cambiamenti fondamentali sia nel campo della produzione che della distribuzione e del consumo di energia. I sistemi volgeranno all'automatizzazione, includendo variabili quali la valutazione dei comportamenti dei prosumer rispetto a offerte, l'andamento del mercato dei prezzi energetici, anche a livello internazionale, e le esigenze strutturali della rete. In tal modo sarà possibile effettuare previsioni sempre più accurate sull'utilizzo e la produzione di elettricità da parte degli utenti e questo permetterà ai gestori delle reti di allocare in maniera sempre più "intelligente" l'energia disponibile. Sarà più semplice gestire efficacemente i picchi della domanda e scongiurare il rischio di collassi della rete tenendo conto di tutte le immissioni e i consumi di energia. Secondo la Commissione europea, l'introduzione degli smart meter - la cui diffusione in Europa potrebbe raggiungere quasi 280 milioni di unità nel 2025 e si avvicinerà a quota 320 milioni nel 2030 - determinerà benefici economici sostanziali a livello strategico, operativo e per i consumatori. Riguardo al primo aspetto, un miglior uso dell'informazione reso possibilità da meter con connettività 5G, genererebbe risparmi quantificati in circa € 2,75 per ogni device, producendo benefici per € 775 milioni l'anno dal 2025 e di € 877 milioni dal 2030. A livello operativo, i risparmi sono identificati nel miglioramento dei canali di comunicazione tra imprese e consumatori (minori costi derivanti da call center, gestione di pratiche e reclami, fatturazioni e lettura digitale dei contatori), che ammonterebbero a € 2,7 miliardi nel 2025 e € 3,1 miliardi nel 2030. L'uso crescente di contatori smart sempre connessi tenderà a migliorare anche le abitudini energetiche dei consumatori, producendo minori consumi stimati in € 107 l'anno per device. Secondo la Commissione, l'uso di device con capacità IoT supportate dal 5G aumenterà tali benefici nell'ordine di almeno il 10%, totalizzando ulteriori € 3 miliardi di risparmi nel 2025 e € 3,4 miliardi nel 2030. Nel complesso, dunque, la diffusione degli smart meters con capacità 5G porterebbe risparmi per quasi € 6,5 miliardi l'anno dal 2025 e di quasi € 7,4 miliardi dal 2030.

Nel **settore manifatturiero** l'azione combinata di *Enhanced Mobile Broadband* (eMBB), *Massive Machine Type Communications* (mMTC) e *Ultra-Reliable Low Latency Communications* (URLLC) consentirà la diffusione della c.d. "fabbrica del futuro". Questa sarà basata sulla flessibilità e sulla versatilità di produzione e logistica, che verranno calibrate sulla base del consumo e dell'approvvigionamento, così come sulla sicurezza, sull'ottimizzazione delle risorse e sull'aumento della qualità. I classici sistemi di produzione statici e sequenziali verranno progressivamente sostituiti da sistemi produttivi flessibili e modulari, che necessiteranno di connettività wireless in grado di offrire il

massimo in termini di mobilità, versatilità ed ergonomia. Secondo il 3GPP (3rd Generation Partnership Project), le aree di applicazione di 5G e IoT nel settore manifatturiero riguarderanno l'automazione delle fabbriche e dei processi, il monitoraggio degli stessi processi e degli asset, la gestione della logistica e dei magazzini, la manutenzione e lo sviluppo di interfacce di uomo-macchina, ad esempio in direzione della realtà aumentata. Il rapporto della Commissione stima benefici derivanti dal c.d. *smart workplace* nell'ordine di € 30 miliardi l'anno dal 2025, grazie a miglioramenti nella produttività (€ 14 miliardi) e nello smaltimento dei rifiuti (€ 16 miliardi).

Nel complesso, i benefici economici derivanti dai 4 principali verticals (automotive, sanità, trasporti ed energia), insieme a quelli ambientali (corrispondenti a benefici diffusi per città, aree suburbane, case e aziende) sono stimati fino a € 113 miliardi di euro l'anno già dal 2025[1].

Tab. 1: Benefici annui derivanti da 5G al 2025 (mld €)

Benefici da verticals per anno al 2025	**mld €**
Automotive	42,2
Salute	5,5
Trasporti	8,3
Utilities	6,5
Subtotale benefici da verticals	62,5
Benefici derivanti da evoluzioni "ambientali" per anno al 2025	**mld €**
Smart cities	8,1
Aree non-urbane	10,5
Smart homes	1,3
Smart workplaces (uffici e aziende)	30,6
Subtotale benefici "ambientali"	50,6
Benefici annuali totali	**113,1**

Fonte: Trinity College, Tech4i2, Real Wireless and InterDigital, "Identification and quantification of key socio-economic data to support strategic planning for the introduction of 5G in Europe).

La diffusione del 5G avrà quindi un considerevole impatto economico nei prossimi anni. Per tali ragioni, appare fondamentale garantire la sicurezza delle reti mantenendo nello stesso aperto il mercato e garantendo il deployment delle reti nei tempi previsti. A tal proposito, gli operatori di telecomunicazione che operano nel **Regno Unito** hanno prodotto nei mesi scorsi un **rapporto contenente delle previsioni sulle tempistiche necessarie allo sviluppo delle reti e sull'impatto che l'esclusione di soggetti extra europei nella fornitura di componentistica 5G potrebbe avere a livello economico** dovuto ai ritardi nell'implementazione delle reti.

[1] Come riportato nel documento della Commissione, non è possibile effettuare una stima complessiva al 2030 perché i dati non sono presenti per tutti i verticals.

Il rapporto, riprendendo le stime del Governo relative ai benefici del 5G per l'economia del paese, quantificate nell'ordine di £ 164 miliardi complessivi fino al 2030 (Tab. 2), calcola il costo del ritardo dell'implementazione del 5G tra £ 4,5 miliardi e £ 6,8 miliardi nel triennio 2020-2022 (Tab. 2), in relazione alla tipologia di restrizione della concorrenza e al conseguente lag temporale.

Tab. 2: Stima benefici economici del 5G in UK (£ mln)

	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Totale	0	2.190	4.625	7.309	10.262	13.745	17.915	23.883	28.442	30.456	34.392
Per mese	0	183	385	609	855	1.145	1.493	1.990	2.370	2.538	2.866

Fonte: Assembly, DCMS (2019)

Secondo gli operatori, gli effetti di una restrizione del mercato ai vendor europei si riverserebbero non solo sui consumatori ma anche sugli stessi operatori di rete, per via dei costi aggiuntivi necessari a sostituire la componentistica 5G e per il possibile collo di bottiglia che verrebbe generato dal poter contare esclusivamente su due vendor (Ericsson e Nokia).
Nel dettaglio, il report commissionato dal DCMS (*Department for Digital, Culture, Media & Sport*) del Governo britannico stima per il solo settore delle comunicazioni mobili dei benefici derivanti dal 5G nell'ordine di £ 29 miliardi l'anno entro il 2020 e £ 51 miliardi l'anno entro il 2030.
Secondo lo studio, stilato dalla società di consulenza Assembly per conto degli operatori tlc britannici, una parziale restrizione della componentistica 5G genererebbe un ritardo di 18 mesi nell'implementazione delle reti tra il 2020 e il 2022, determinando una perdita di circa £ 4,5 miliardi. Una restrizione totale determinerebbe un ritardo nell'implementazione delle reti 5G nell'ordine di 24 mesi, i cui effetti sono stimati in una perdita di potenziali benefici di circa £ 6,8 miliardi.

Tab. 3: Stima riduzione dei benefici economici del 5G in UK causata da restrizioni e conseguenti ritardi nell'implementazione

Ritardo di 1 anno	**2020**	**2021**	**2022**
Riduzione dei benefici (m £)	0	2.190	2.190
Ritardo di 1,5 anni	**2020**	**2021**	**2022**
Riduzione dei benefici (m £)	2.190	2.313	4.503
Ritardo di 2 anni	**2020**	**2021**	**2022**
Riduzione dei benefici (m £)	2.190	4.625	6.815

Fonte: Assembly, DCMS (2019)

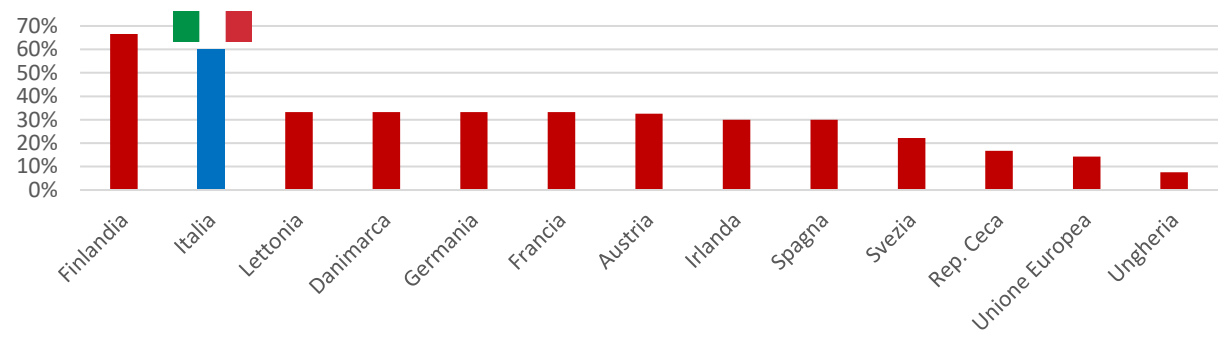
Per quanto concerne più specificamente l'**Italia**, il Paese si trova in una prospettiva di relativo vantaggio rispetto agli Stati europei. **L'indice DESI, prodotto annualmente dalla Commissione europea, che nella**

release 2019, pubblicata poche settimane fa, ci posiziona solo al 24° posto complessivo in Europa per digitalizzazione dell'economia e della società, ci vede al 2º posto proprio in relazione allo stato di avanzamento della diffusione del 5G. In particolare l'indice DESI relativo alla "*5G readiness*" è composto da 5 indicatori, ovvero l'adozione di strategie o roadmap per l'implementazione del 5G, i trials 5G, l'assegnazione effettiva dello spettro, le città in 5G (in cui è stato annunciato il lancio di servizi commerciali o dove si stanno effettuate sperimentazioni finalizzate al lancio di tali servizi) e i corridoi internazionali 5G (dove sono in fase di test i sistemi 5G applicati a soluzioni di mobilità connessa e sostenibile).

In quasi tutti questi segmenti l'Italia risulta all'avanguardia. Le città per le sperimentazioni 5G sono state individuate già nel 2017 nelle città di Milano, Prato, L'Aquila, Bari e Matera, con numerose sperimentazioni pre-commerciali.

Altre sperimentazioni del 5G, sulla base di accordi volontari tra gli operatori e i comuni, sono in corso a Roma, Torino, Napoli e Genova.

Fig. 1: 5G readiness dei Paesi europei



Fonte: Commissione Europea, Digital Scoreboard (giugno 2019)

Lo spettro armonizzato a livello UE per la banda larga senza fili è stato assegnato al 94%. Come noto, l'asta per l'assegnazione delle bande "pioniere" del 5G (700 MHz, 3,6 GHz e 26 GHz) si è tenuta lo scorso anno, con la banda 700 MHz che però verrà messa a disposizione entro luglio 2022 (da qui il valore che indica l'Italia pronta al 60%, che la posiziona comunque seconda in Europa). Per la banda 3,6 GHz, sulla quale si prevede la prima implementazione dei servizi 5G, sono stati registrati prezzi di assegnazione record per l'erario, ma allo stesso tempo una spesa ingente per gli operatori, che dovranno remunerare gli investimenti per la partecipazione all'asta, oltre a quelli necessari per il roll-out delle reti. Lo stesso rapporto DESI indica come il prezzo di tali assegnazioni in Italia sia risultato fino ad ora il più alto in Europa, equivalente in media a 36 centesimi di EUR/pop/MHz. Per tali ragioni, è importante garantire la rapidità nelle procedure burocratiche relative ai permessi per l'implementazione delle reti 5G, in modo che questa sia efficace, veloce e sostenibile.

2. Lo stato dell'arte europeo sulla sicurezza: Direttiva NIS, Cybersecurity Act e raccomandazione della Commissione Europea sulla cybersecurity delle reti 5G

Sin dall'adozione della Strategia europea sulla cybersecurity nel 2013, le istituzioni europee hanno pianificato azioni per migliorare la sicurezza degli utilizzatori di internet e dei servizi digitali. La strategia lanciata nel 2013, in particolare, ha fissato cinque priorità che consistevano nel rafforzamento della resilienza informatica, nella riduzione del cyber crimine, nello sviluppo di una politica europea di cybersecurity, nell'incremento di risorse industriali e tecnologiche per la sicurezza informatica e nella definizione di una politica europea sulla cybersecurity coerente a livello internazionale.
Successivamente, il 6 luglio 2016 l'Unione europea ha adottato la **direttiva 2016/1148 (la cosiddetta direttiva NIS)**, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, con la quale le istituzioni europee hanno affrontato le sfide in materia di cyber sicurezza, rivoluzionando la resilienza e la cooperazione in Europa.
Partendo dalla constatazione del ruolo vitale ricoperto dalle reti e dai sistemi e dai servizi informativi nella società, la direttiva ritiene essenziale che essi siano affidabili e sicuri per le attività economiche e sociali e in particolare ai fini del buon funzionamento del mercato interno. A tal fine, la direttiva: 1) obbliga gli Stati membri ad adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi; 2) istituisce un **gruppo di cooperazione** – con l'obiettivo di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra Stati membri e di sviluppare la fiducia tra di essi – composto da rappresentanti degli Stati membri, della Commissione e dell'ENISA, con il compito di svolgere i propri compiti sulla base di programmi di lavoro biennali; 3) crea una **rete di gruppi di intervento per la sicurezza informatica** in caso di incidente per contribuire allo sviluppo della fiducia tra Stati membri e promuovere una cooperazione operativa rapida ed efficace; 4) stabilisce **obblighi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali**; 5) obbliga gli Stati membri ad **individuare autorità nazionali competenti, punti di contatto unici e CSIRT** (Computer Security Incident Response Team) con compiti connessi alla sicurezza della rete e dei sistemi informativi.
La disciplina dettata dalla direttiva prevede che la strategia nazionale affronti una serie di aspetti ed in particolare, fissi gli obiettivi e le priorità, le opportune misure strategiche e regolamentari al fine di conseguire e mantenere un livello elevato di sicurezza delle reti e dei sistemi informativi, un quadro di governance adeguato, l'individuazione delle misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato, l'indicazione di programmi di formazione, sensibilizzazione ed istruzione, piani di ricerca e sviluppo, un piano di valutazione dei rischi (art. 7). La direttiva NIS richiede altresì agli Stati di designare una o più autorità competenti per il controllo dell'applicazione della direttiva stessa a livello nazionale. Un singolo punto di contatto dovrà essere designato da ognuno degli Stati membri, con il compito di assicurare la cooperazione internazionale e di

collegarsi con gli altri Stati attraverso meccanismi di cooperazione identificati della direttiva stessa. Ogni Stato infine deve designare uno o più CSIRT (Computer Security Incident Response Team) responsabili del monitoraggio degli incidenti a livello nazionale, fornendo allarmi tempestivi, avvisi ed annunci con lo scopo di diffondere informazioni su rischi ed incidenti.
Elemento cardine dell'impianto disegnato dalla direttiva è la **cooperazione** tra i vari enti dei singoli Stati membri. A tal fine è stato individuato un gruppo di cooperazione composto da rappresentati degli Stati membri, dalla Commissione e dall'ENISA con quattro aree di lavoro e, in particolare, pianificazione, guida, segnalazione e condivisione. L'ultimo dei punti principali della direttiva riguarda gli operatori dei servizi essenziali per la Nazione e i fornitori di servizi digitali. Si tratta di aziende pubbliche o private che operano nell'energia, nei trasporti, nel settore bancario e sanitario, nelle infrastrutture dei mercati finanziari, nella fornitura e distribuzione di acqua potabile e nelle infrastrutture digitali sulle quali graverà, ai sensi della direttiva, l'obbligo di dotarsi di misure di sicurezza che comprendono: prevenzione dei rischi; garanzia circa la sicurezza dei sistemi, delle reti e delle informazioni; capacità di gestire gli incidenti. Anche i fornitori di servizi digitali – intendendo per servizi digitali mercato online, motore di ricerca online e servizi nella nuvola (cloud computing) – saranno tenuti, secondo la direttiva NIS, ad attuare misure di sicurezza appropriate e a notificare incidenti rilevanti. Oltre alle misure già previste per gli operatori di servizi essenziali, le misure di sicurezza relative ai fornitori di servizi digitali prevedono alcuni fattori specifici, come ad esempio la sicurezza dei sistemi e degli impianti, la gestione della continuità operativa, il monitoraggio e i test e la conformità a norme internazionali.
Se la direttiva NIS, per la prima volta, è intervenuta a disciplinare in maniera organica il tema della sicurezza delineando la cornice normativa ed organizzativa nell'UE, il **Regolamento n. 881/2019** del 17 aprile 2019 (noto come "Cybersecurity Act"), al fine di garantire il buon funzionamento del mercato interno perseguendo nel contempo un elevato livello di cybersicurezza, cyberresilienza e fiducia all'interno dell'Unione, ha fissato gli obiettivi, i compiti e gli aspetti organizzativi relativi all'**ENISA** ed ha fissato un quadro per l'introduzione di **sistemi europei di certificazione della cybersecurity** al fine di garantire un livello adeguato di cybersecurity dei prodotti TIC, servizi TIC e processi TIC nell'Unione, oltre che al fine di evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione della cybersecurity nell'Unione.
Il Regolamento, in particolare, amplia e specifica i compiti dell'ENISA che, quale centro di competenze nel campo della cybersecurity, assiste le istituzioni, gli organi e gli organismi dell'Unione e gli Stati membri nell'elaborazione e nell'attuazione di politiche dell'Unione relative alla cybersecurity (comprese le politiche settoriali in materia di cybersecurity), nel miglioramento della protezione delle loro reti e dei loro sistemi informativi, nello sviluppo e nel miglioramento delle capacità di ciber-resilienza e di risposta, nonché nello sviluppo di abilità e competenze nel campo della cybersecurity, di promuovere la cooperazione e la condivisione delle informazioni, di contribuire a rafforzare le capacità di cybersecurity a livello di Unione per sostenere le azioni degli Stati membri nella prevenzione delle minacce informatiche e nella reazione alle stesse (in particolare in caso di incidenti transfrontalieri), di promuovere un elevato livello di consapevolezza in materia di cybersecurity e di favorire l'uso della certificazione europea della cybersecurity, con l'obiettivo di evitare la frammentazione del mercato

interno. Lo stesso regolamento, poi, declina le specifiche attività che l'ENISA è abilitata a compiere per contribuire allo sviluppo e all'attuazione delle politiche e della normativa dell'Unione, favorire lo sviluppo delle capacità e la cooperazione operativa a livello di Unione, sostenere e promuovere lo sviluppo e l'attuazione della politica dell'Unione in materia di certificazione della cybersecurity dei prodotti TIC, dei servizi TIC e dei processi TIC, acquisire ed offrire conoscenze ed informazioni, sensibilizzare e promuovere l'istruzione in materia di cybersecurity, individuare e condividere le priorità in materia di ricerca ed innovazione e promuovere la cooperazione internazionale in materia di cybersecurity. Le disposizioni che seguono disciplinano la struttura e l'organizzazione dell'ENISA individuando i poteri e le prerogative di ciascun organo nonché le modalità operative di ciascuno di essi.
A livello generale, il regolamento in esame fissa la cornice di principi entro la quale l'ENISA deve svolgere le proprie attività prescrivendo, in particolare, l'osservanza dei principi di trasparenza e riservatezza.
A partire dell'art. 46, il regolamento fissa il quadro europeo di certificazione della cybersecurity introducendo un approccio armonizzato dei sistemi europei di certificazione della cybersecurity allo scopo di creare un mercato unico digitale per i prodotti, i servizi e i processi TIC.
L'art. 49, in particolare, disciplina la preparazione, adozione e revisione di un sistema europeo di certificazione della cybersecurity (di cui il successivo art. 54 fissa gli elementi), prevedendo che la Commissione possa richiedere all'ENISA di preparare una proposta di sistema rispetto alla quale è prevista la consultazione di tutti i pertinenti portatori di interessi mediante un processo di consultazione formale, aperto, trasparente e inclusivo, l'istituzione di un gruppo di lavoro ad hoc per ciascuna proposta di sistema ed una stretta cooperazione con l'ECCG (che fornisce all'ENISA assistenza e consulenza specialistica in relazione alla preparazione della proposta di sistema e adotta un parere sulla proposta).
La procedura delineata dal Regolamento prevede, inoltre, che la Commissione, sulla base della proposta di sistema preparata dall'ENISA, possa adottare atti di esecuzione, che almeno ogni cinque anni l'ENISA valuti ogni sistema europeo di certificazione della cybersecurity adottato, tenendo conto del riscontro ricevuto dalle parti interessate e che, se necessario, la Commissione o il Gruppo europeo per la certificazione della cybersecurity (ECCG, di cui si dirà *infra*) possa chiedere all'ENISA di avviare il processo di sviluppo di una proposta riveduta di sistema.
Il Regolamento individua, poi, con particolare rigore, un'ampia gamma di obiettivi di sicurezza connessi all'istituzione dei sistemi europei di certificazione e suddivide in tre, sulla base del livello di rischio associato al previsto uso del prodotto, servizio o processo TIC, in termini di probabilità e impatto di un incidente, i livelli di affidabilità dei prodotti, servizi e processi TIC: **di base, sostanziale ed elevato**, declinando, in riferimento a ciascuno dei tre livelli, le specifiche attività di valutazione previste nonchè il ricorso ad attività sostitutive di effetto equivalente qualora le attività di valutazione previste non siano appropriate.
In relazione ai prodotti, servizi e processi TIC che presentano un basso rischio corrispondenti al livello di affidabilità di base è possibile il ricorso ad un'autovalutazione (mediante specifica dichiarazione) della conformità sotto la sola responsabilità del fabbricante o del fornitore.
Il Regolamento prescrive, a livello organizzativo, la designazione, da parte degli Stati membri, di una o più autorità nazionali di certificazione della cybersecurity nel proprio territorio oppure, con l'accordo di

un altro Stato membro, la designazione di una o più autorità nazionali di certificazione della cybersecurity stabilite in tale altro Stato membro affinché siano responsabili dei compiti di vigilanza nello Stato membro designante. Tali autorità sono sottoposte ad una valutazione *inter pares*, effettuata da almeno due autorità nazionali di certificazione della cybersecurity di altri Stati membri e dalla Commissione almeno una volta ogni cinque anni, sulla base di criteri e procedure di valutazione solidi e trasparenti.

Il medesimo regolamento istituisce il **Gruppo europeo per la certificazione della cybersecurity**, composto da rappresentanti delle autorità nazionali di certificazione della cybersecurity o da rappresentanti di altre autorità nazionali competenti, con compiti di assistenza, proposta, collaborazione e consulenza nei rapporti con la Commissione ed ENISA.

Quanto alla valutazione dell'impianto normativo introdotto, il regolamento prevede che entro il 28 giugno 2024, e successivamente ogni cinque anni, la Commissione valuti l'impatto, l'efficacia e l'efficienza dell'ENISA e delle sue prassi di lavoro, l'eventuale necessità di modificarne il mandato e le conseguenti implicazioni finanziarie. La valutazione tiene conto di qualsiasi riscontro fornito all'ENISA in relazione alle sue attività. È prevista, inoltre, la possibilità per la Commissione, qualora ritenga che il mantenimento dell'ENISA non sia più giustificato alla luce degli obiettivi, del mandato e dei compiti che le sono stati assegnati, di proporre di modificare le relative disposizioni.

L'evoluzione tecnologica si muove a ritmi frenetici ponendo questioni nuove e sempre più complesse in termini di sicurezza. Garantire elevati standard di sicurezza rappresenta, in particolare, una questione di vitale importanza nel processo di sviluppo delle reti 5G. Le reti di quinta generazione, infatti, rappresentano il fattore abilitante per un'ampia serie di servizi digitali essenziali per il funzionamento del mercato interno e per il mantenimento e la gestione di funzioni economiche e sociali vitali, quali l'energia, i trasporti, i servizi bancari e sanitari e i sistemi di controllo industriale. Ne discende che essendo il 5G centrale per il funzionamento di servizi essenziali, le conseguenze di malfunzionamenti sistemici e diffusi sarebbero particolarmente gravi. Considerato dunque che garantire la cybersecurity delle reti 5G è una questione di importanza strategica per l'Unione, soprattutto in un momento in cui gli attacchi informatici sono sempre più numerosi e sofisticati, la Commissione europea, il 26 marzo 2019 ha adottato la **Raccomandazione n. 2019/534** sulla cybersecurity delle reti 5G con la quale ha evidenziato i rischi di cybersecurity nelle reti 5G 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 particolare, per affrontare i rischi di cybersecurity nelle reti 5G, il documento pone in evidenza la necessità di considerare, da un lato, i **fattori tecnici**, che possono includere le vulnerabilità di cybersecurity che possono essere sfruttate per l'accesso non autorizzato alle informazioni (ciberspionaggio, per motivi tanto economici quanto politici) o per altri scopi dolosi (attacchi informatici volti a distruggere sistemi e dati o a provocarne il malfunzionamento) e, dall'altro, **fattori ulteriori e diversi** come, ad esempio, requisiti normativi o di altro tipo imposti ai fornitori di apparecchiature per le tecnologie dell'informazione e della comunicazione, il modello di governance esistente nel Paese

analizzato, il rischio generale di influenza da parte di un paese terzo, l'assenza di accordi di cooperazione sulla sicurezza o di disposizioni analoghe, quali le decisioni di adeguatezza, tra l'Unione e il paese terzo interessato per quanto riguarda la protezione dei dati, etc.

Al fine di sostenere lo sviluppo di un approccio dell'Unione volto a garantire la cybersecurity delle reti 5G, la raccomandazione in esame individua un set di azioni da mettere in campo al fine di consentire: a) agli Stati membri di valutare i rischi di cybersecurity che interessano le reti 5G a livello nazionale e adottare le necessarie misure di sicurezza; b) agli Stati membri e alle istituzioni, alle agenzie e ad altri organismi pertinenti dell'Unione di elaborare congiuntamente una valutazione dei rischi coordinata a livello di Unione basata sulla valutazione nazionale dei rischi; c) al gruppo di cooperazione istituito dalla direttiva (UE) 2016/1148 (gruppo di cooperazione) di individuare un'eventuale serie comune di misure da adottare per attenuare i rischi di cybersecurity relativi alle infrastrutture alla base dell'ecosistema digitale, in particolare le reti 5G.

La medesima raccomandazione delinea una **roadmap** chiara e stringente che incoraggia gli Stati membri ad effettuare, entro il 30 giugno 2019, una valutazione dei rischi dell'infrastruttura 5G, anche identificando gli elementi più sensibili in relazione ai quali le violazioni della sicurezza avrebbero un impatto negativo significativo nonché a rivedere i requisiti di sicurezza e i metodi di gestione dei rischi applicabili a livello nazionale, al fine di tenere conto delle minacce di cybersecurity. Sulla base di tale valutazione e revisione nazionale dei rischi e tenendo conto delle azioni coordinate in corso a livello di Unione, gli Stati membri dovrebbero: a) aggiornare i requisiti di sicurezza e i metodi di gestione dei rischi applicati alle reti 5G; b) aggiornare i pertinenti obblighi imposti alle imprese che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico; c) vincolare a condizioni l'autorizzazione generale riguardante la sicurezza delle reti pubbliche contro l'accesso non autorizzato e chiedere alle imprese che parteciperanno alle prossime procedure per la concessione di diritti d'uso delle frequenze radio nelle bande 5G di assumersi impegni per quanto riguarda la conformità ai requisiti di sicurezza per le reti; d) applicare altre misure preventive volte ad attenuare i potenziali rischi di cybersecurity. Per un'efficace azione di prevenzione e contrasto delle minacce, il documento sottolinea l'importanza di porre in essere una valutazione dei rischi coordinata a livello europeo mediante lo scambio di informazioni tra gli Stati e con gli organismi pertinenti dell'Unione al fine di sviluppare una consapevolezza comune dei rischi di cybersecurity esistenti e potenziali associati alle reti 5G. Gli Stati membri dovrebbero, inoltre, trasmettere le valutazioni nazionali dei rischi alla Commissione e all'Agenzia dell'Unione europea per la cybersecurity (ENISA) entro il 15 luglio 2019 così da consentire a quest'ultima di completare una mappatura specifica del panorama delle minacce per le reti 5G.

Tutto ciò considerato, la raccomandazione individua una serie di step temporalmente scanditi ed in particolare: 1) completamento, entro il 10 ottobre 2019, da parte degli Stati membri, con il sostegno della Commissione e dell'ENISA, di una revisione congiunta dell'esposizione a livello di Unione ai rischi relativi alle infrastrutture alla base dell'ecosistema digitale, in particolare delle reti 5G; 2) sulla base di tali migliori pratiche nazionali, condivisione, entro il 31 dicembre 2019, di un insieme di possibili misure di gestione dei rischi adeguate, efficaci e proporzionate al fine di attenuare i rischi di cybersecurity individuati a livello nazionale e di Unione, che orienterà la Commissione nello sviluppo di requisiti minimi

comuni a ulteriore garanzia di un elevato livello di cybersecurity delle reti 5G in tutta l'Unione. Tale insieme di strumenti dovrebbe comprendere: a) un inventario dei tipi di rischi di sicurezza che possono incidere sulla cybersecurity delle reti 5G (ad esempio rischio relativo alla catena di approvvigionamento, rischio di vulnerabilità del software, rischio relativo al controllo degli accessi, rischi derivanti dal quadro giuridico e politico cui possono essere soggetti i fornitori di apparecchiature per le tecnologie dell'informazione e della comunicazione in paesi terzi); e b) una serie di possibili misure di attenuazione. Infine, la raccomandazione invita gli Stati membri a cooperare con la Commissione per valutare gli effetti di quanto previsto dalla stessa, entro il 10 ottobre 2020, al fine di determinare le modalità di azione.

3. La situazione in Italia: il recepimento della direttiva NIS

Nella sfida della sicurezza anche l'Italia è chiamata a giocare la propria partita. Se nel 2017 sono stati adottati alcuni provvedimenti propedeutici o preparatori all'adozione delle misure prescritte dalla direttiva NIS quali il Decreto del Presidente del Consiglio dei Ministri 17 febbraio 2017, "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali" (il cosiddetto "DPCM Gentiloni"), che ha tra l'altro riorganizzato l'architettura per la protezione dello spazio cibernetico nazionale, ed il nuovo "Piano nazionale per la protezione cibernetica e la sicurezza informatica" (marzo 2017), che ha aggiornato gli indirizzi e le direttive stabilite col precedente Piano del 2013 proprio in vista delle indicazioni presenti nella direttiva NIS, con il **D.Lgs. n. 65 del 18 maggio 2018** l'Italia ha recepito la direttiva NIS.

Quanto ai criteri per l'identificazione degli operatori di servizi essenziali (per i quali il decreto istituisce un elenco nazionale presso il MISE), precisando come nell'individuazione degli operatori di servizi essenziali si debba tenere conto anche dei documenti prodotti al riguardo dal Gruppo di cooperazione, l'art. 4 ripropone gli stessi fissati dalla direttiva ed in particolare: a) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali; b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi; c) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

Il successivo art. 5 precisa come ai fini della determinazione della rilevanza degli effetti negativi, si debba considerare il numero di utenti che dipendono dal servizio fornito dal soggetto interessato, la dipendenza di altri settori (di cui all'allegato II) dal servizio fornito da tale soggetto, l'impatto che gli incidenti potrebbero avere, in termini di entità e di durata, sulle attività economiche e sociali o sulla pubblica sicurezza, la quota di mercato di detto soggetto, la diffusione geografica relativamente all'area che potrebbe essere interessata da un incidente e l'importanza del soggetto per il mantenimento di un livello sufficiente del servizio, tenendo conto della disponibilità di strumenti alternativi per la fornitura di tale servizio.

Anche in relazione agli elementi che la strategia nazionale deve contenere, il decreto ripropone pedissequamente quanto previsto dalla direttiva NIS richiedendo, dunque, che essa indichi: a) gli obiettivi e le priorità in materia di sicurezza delle reti e dei sistemi informativi; b) il quadro di governance

per conseguire gli obiettivi e le priorità, inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti; c) le misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato; d) i programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi; e) i piani di ricerca e sviluppo; f) un piano di valutazione dei rischi; g) l'elenco dei vari attori coinvolti nell'attuazione.

Per quanto attiene, invece, alla **designazione delle autorità nazionali competenti e** del **punto di contatto unico**, il modello prescelto è di tipo moderatamente decentrato. Ed infatti, discostandosi dal modello centralizzato francese che ha individuato una sola autorità e da quello decentrato dei paesi nordici come la Svezia dove i poteri e le funzioni in materia di cybersecurity sono affidati a una serie di agenzie pubbliche competenti per settori specifici, il Governo italiano ha individuato, quali "autorità nazionali competenti", ben **5 Ministeri** (Sviluppo economico, Infrastrutture e trasporti, Economia, Salute e Ambiente) (art. 7). Il Dipartimento delle informazioni per la sicurezza (DIS), invece, è incaricato di svolgere le funzioni di punto di contatto unico. Ad esso spetta l'esercizio di una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità competenti NIS con le autorità competenti degli altri Stati membri, nonché con il gruppo di cooperazione e la rete di CSIRT. Il decreto dispone, inoltre, la creazione, presso la Presidenza del Consiglio dei Ministri, di un unico ***Computer Security Incident Response Team*****,** detto **CSIRT** italiano, che è andato a sostituire, andandoli ad inglobare, il CERT Nazionale (operante presso il Ministero dello Sviluppo Economico) e CERT-PA (operante presso l'Agenzia per l'Italia Digitale) – la cui organizzazione e funzionamento saranno disciplinati mediante decreto del Presidente del Consiglio dei Ministri – col compito di definire le procedure per la prevenzione e la gestione degli incidenti informatici e ricevere da parte degli operatori di servizi essenziali e dei fornitori di servizi digitali le notifiche relative ad incidenti.

Anche con riguardo all'**individuazione degli obblighi in materia di sicurezza** gravanti sugli operatori di servizi essenziali, il decreto legislativo ripropone gli obblighi generali di sicurezza previsti dalla direttiva, prescrivendo agli operatori di servizi essenziali l'adozione di misure tecniche ed organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano nelle loro operazioni. Analoghi obblighi in materia di sicurezza sono previsti a carico dei fornitori di servizi digitali.

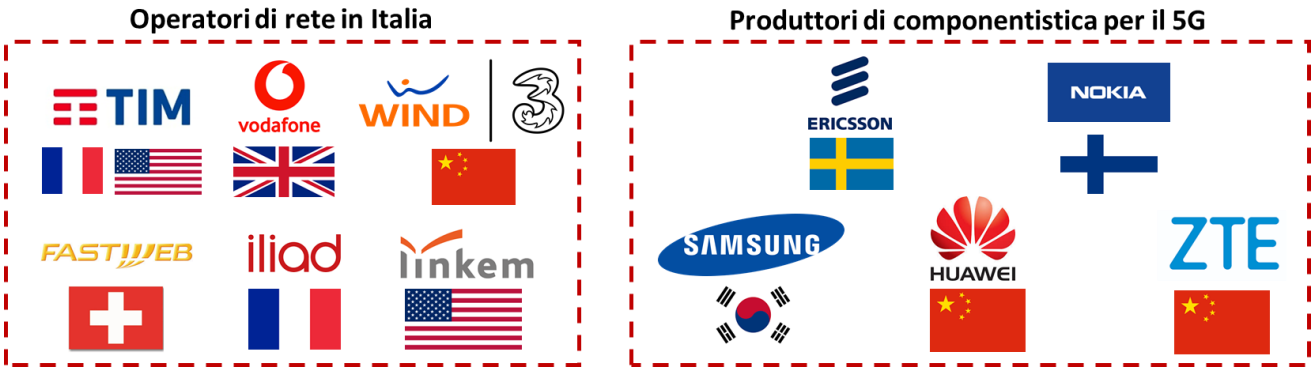
Per quanto concerne gli **obblighi di notifica**, il decreto dispone che gli operatori di servizi essenziali e di fornitori di servizi digitali inoltrino al CSIRT (e per conoscenza all' autorità competente NIS del proprio settore) le notifiche di incidenti informatici con impatto rilevante sui servizi forniti (analogo obbligo è previsto anche a carico dei fornitori di servizi digitali) "senza ingiustificato ritardo", rinunciando dunque alla fissazione di un termine perentorio.

Con riguardo, infine, al **regime sanzionatorio**, premesso che la direttiva NIS garantisce agli Stati ampia discrezionalità riguardo al tipo e alla natura delle sanzioni applicabili, ferma restando la necessità che esse siano effettive, proporzionate e dissuasive, l'art. 21 declina un set di sanzioni in relazione alle diverse possibili infrazioni che possono essere poste in essere dagli operatori di servizi essenziali e dai fornitori di servizi digitali, fino ad un massimo di € 150.000.

4. Profili tecnici relativi alla sicurezza

L'importanza e la strategicità del 5G si riverberano con forza sugli aspetti relativi alla sicurezza delle sue infrastrutture. Infatti, il potenziale spostamento da parte di molteplici settori industriali di una quota crescente delle proprie attività su reti 5G potrebbe determinare situazioni in cui gruppi di malintenzionati che prendessero possesso delle reti 5G di un Paese potrebbe, in un futuro non così remoto, paralizzarne parte dell'economia. Parallelamente, il Rapporto Enisa indica che appena 2,5% dei problemi riscontrati sulle reti di telecomunicazioni europee nel 2017 sono riconducibili a incidenti di sicurezza causati da attacchi di hacker. Dei 169 incidenti di sicurezza analizzati nel corso del 2017 emerge come gli errori di sistema (hardware failure, software bugs ed errati aggiornamenti software) e gli errori umani siano la causa dominante degli incidenti riportati con impatto sul maggior numero di connessioni[2].
A tal proposito, il dibattito recente è stato catalizzato dalle questioni relative alla sicurezza nazionale, in particolare per quanto concerne l'utilizzo, nella realizzazione delle reti 5G, di componentistica proveniente dagli operatori extra europei. Attualmente il **perimetro relativo alle imprese che producono componentistica per il 5G** è piuttosto ristretto, e comprende Ericsson (Svezia), Huawei (Cina), Nokia (Finlandia), Samsung (Corea del Sud) e ZTE (Cina). Allo stesso tempo sono molteplici gli operatori di tlc che si occupano delle reti, in gran parte a capitale estero (Fig. 2).

Fig. 2: Nazionalità degli operatori di rete in Italia e dei vendor 5G nel mondo



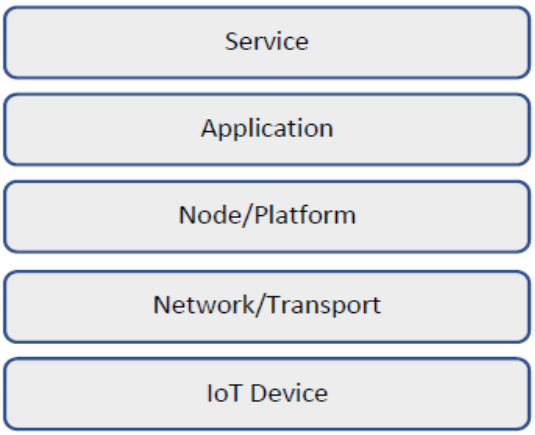
Fonte: elaborazioni I-Com

In Italia si rileva un altissimo grado di internazionalizzazione nel settore tlc, con americani e francesi tra i principali azionisti dell'ex incumbent Tim, britannici alla guida di Vodafone, cinesi prima con e poi senza russi in Wind Tre, svizzeri in Fastweb ed ancora i nuovi entranti francesi in Iliad e americani in Linkem. La

[2] Questa percentuale si è ridotta inoltre della metà se comparata al 5,1% riscontrato nel 2016. Anche il numero di connessioni utente coinvolte risulta in media proporzionalmente il più basso. Fonte: Enisa, *Annual Report Telecom security incidents* 2017, pubblicato il 30 Agosto 2018.

nazionalità degli operatori sembrerebbe quindi essere un problema di secondo livello rispetto alle tematiche tecniche relative alla sicurezza ed alle misure che possono essere assunte per mitigare i rischi. Appare inoltre importante chiarire cosa si intende per "***backdoor***" e perché sia così complicato garantire l'assenza di codici malevoli. Una backdoor (lett. "porta sul retro") consiste in una porta nascosta tramite la quale è possibile accedere da remoto, originariamente usata per attività di assistenza, manutenzione e aggiornamento software. Le backdoor possono essere create in origine dai produttori di hardware e software o generate ex post da malintenzionati ad esempio tramite virus chiamati Trojan o *malware* (codici malevoli). Il termine è diventato noto al grande pubblico in seguito al caso Snowden, un ex agente della Cia che documentò le attività di pressione da parte delle agenzie di intelligence americane affinché i produttori di hardware e software installassero delle porte di accesso che consentivano alle stesse agenzie di bypassare i normali controlli di sicurezza dei sistemi ed accedere direttamente ai dati protetti.

Fig. 3: IoT security levels

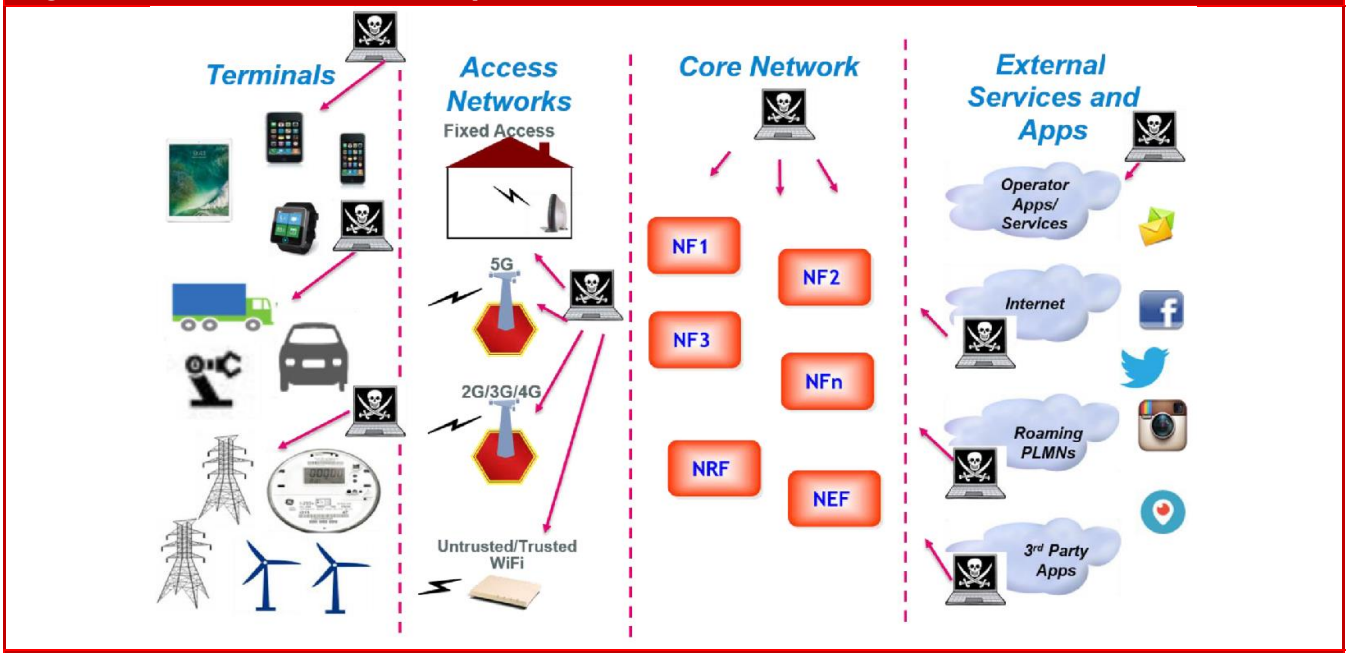


Fonte: 5G Americas, "The Evolution of Security in 5G", ottobre 2018

La natura composita delle reti 5G determina l'**impossibilità di realizzare reti ICT che siano al 100% sicure**. L'utilizzo dei sistemi di sicurezza IT tradizionali, come ad esempio i "*Common Standard Criteria*", appare inefficace, poiché le future reti 5G saranno costituite da sistemi interconnessi e dotati di software aggiornati di frequente. Altre operazioni quali il security assessment, le revisioni del codice e i *penetration test* possono migliorare la qualità del software ma non possono garantire l'assenza di codici malevoli o *backdoor*. Ciò è dovuto al fatto che tali sistemi sono composti da miliardi di transistor e milioni di righe di codice, peraltro realizzati in forma modulare. Inoltre, in molti casi i produttori acquistano in outsourcing il 99% di componenti e software, specializzandosi e innovando solo in una piccola parte di essi. Tale interdipendenza determina una condizione in cui la sicurezza dipende da tutti gli attori della catena e non da uno soltanto. A tal proposito, il Nist parla di *Cyber Supply Chain Risk Management* (C-SCRM), intendendo il processo di identificazione e mitigazione dei rischi associati alla natura distribuita e interconnessa delle supply chain di prodotti e servizi IT (e OT).

Secondo il Nist, il C-SCRM include l'intero ciclo di un sistema, ovvero design, sviluppo, distribuzione implementazione, acquisizione, manutenzione e distruzione, poiché le minacce e le vulnerabilità della supply chain potrebbero compromettere prodotti e servizi in ogni fase del ciclo sia intenzionalmente sia involontariamente. I rischi sono associati alla mancanza di visibility, di understanding e/o di controllo di molti dei processi e delle decisioni coinvolte tanto nello sviluppo quanto nell'acquisizione e nella fornitura di prodotti e servizi IT. In particolare, il Nist distingue le minacce e le vulnerabilità tra conflittuali (cioè derivanti da attacchi), e non conflittuali (dovute a scarsa qualità o disastri naturali), sia interne (relative alle procedure organizzative) che esterni (collegate alla supply chain in cui opera l'azienda o l'organizzazione). Per i sistemi critici, una mitigazione dei rischi efficace richiede agenzie deputate all'identificazione di sistemi e componenti che sono più vulnerabili e che possano avere il maggiore impatto se compromesse.

Fig. 4: The 5G Threat Landscape



Fonte: 5G Americas, "The Evolution of Security in 5G", ottobre 2018

Per le reti 5G, in particolare, la vulnerabilità dipende dal fatto che i sistemi Ict sono complessi e interconnessi, e queste caratteristiche allargano la superficie su cui possibili malintenzionati possono sferrare i propri attacchi. Tale allargamento dipende in buona sostanza da quello che viene definito il Massive IOT, ovvero la diffusione di sensori, device e apparecchiature capaci di comunicare tramite protocollo e talvolta di agire nel mondo fisico.

La **sicurezza dell'IoT comprende 5 livelli, ovvero il device, la rete di trasporto, il nodo/la piattaforma, l'applicazione ed il servizio**. Una simile distinzione può essere effettuata per analizzare le vulnerabilità

della rete 5G, la quale è composta da 4 diversi domini su cui possibili malintenzionati potrebbero attaccare:

1) i terminali;
2) la rete di accesso;
3) la rete core;
4) i servizi e le applicazioni esterne.

1) I **terminali** costituiscono il primo target per via della immensa di diffusione di smartphone, per le molteplici modalità di connessione disponibili e per altri fattori di vulnerabilità. Gli attacchi ai terminali possono essere classificati in 4 categorie: Mobile to Infrastructure (schema in cui molti device infetti attaccano l'infrastruttura per metterla fuori gioco); Mobile to Internet (molti device infetti attaccano siti pubblici per renderli indisponibili); Mobile to Mobile (molti device infettano altri device e/o causano disservizi); Internet to Mobile (codici malevoli diffusi sul web tramite app, giochi o video per infettare i terminali).

2) Per quanto concerne il secondo ambito, si osserva come lo standard 5G supporterà molte **reti di accesso**, tra cui quella 2G, 3G, 4G e Wi-Fi, pertanto ereditando tutte le sfide relative alla sicurezza delle reti precedenti. Gli attacchi che vengono condotti su questa parte di accesso della rete (Fig. 3) mettono a rischio prevalentemente la privacy dell'utente, mentre i rischi per le funzionalità strutturali sono più limitati. Infatti, uno degli attacchi più comuni al network access è costituito dalla *rogue base station* (RBS) *threat*: una stazione "pirata" si camuffa da stazione autorizzata per creare un attacco "*Man in the Middle*", in cui i malintenzionati si pongono a mezza via tra le rete e i terminale dell'utente, intercettandone quindi le comunicazioni, tracciandone gli spostamenti e avendo la possibilità di manomettere le informazioni trasmesse e causare potenziali attacchi DoS ai servizi (che comportano la richiesta dello stesso servizio da parte di molteplici terminali allo stesso tempo per farne venire meno le funzionalità o i servizi interi). Questo tipo di minaccia esiste dalla nascita delle reti GSM e probabilmente continuerà ad esistere ed evolversi con l'evoluzione delle reti mobili. A tal proposito, si osserva come le reti 5G abbiano dei dispositivi di sicurezza più avanzati rispetto a quelli del 4G (es. 5G-GUTI), ma anche con lo standard 5G sono possibili una serie di attacchi tramite RBS, ad esempio sfruttando la fase di transizione dalla rete LTE alla rete 5G per attaccarne i punti più deboli e causare malfunzionamenti e disservizi.

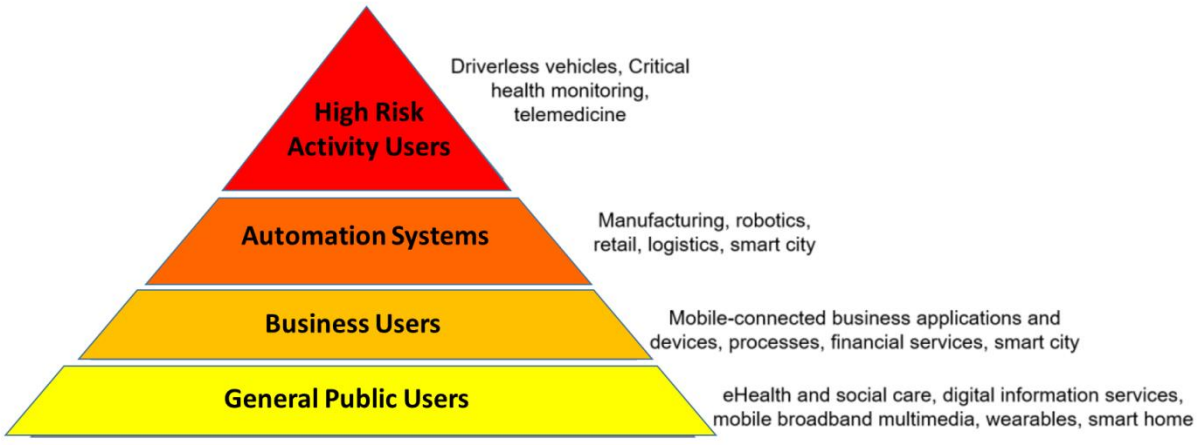
3) Relativamente alla **rete core**, le funzioni di rete più importanti delle reti 5G sono *l'Access and Mobility Management Function* (AMF), *l'Authentication Server Function* (AUSF) e lo *Unified Data Management* (UDM). Il primo consente l'autenticazione, l'autorizzazione e la gestione di servizi in mobilità. L'AUSF conserva i dati per l'autenticazione degli apparecchi utente (UE), mentre l'UDM immagazzina i dati di registrazione. Poiché queste sono funzioni critiche nelle reti 5G, un attacco DDoS contro di loro, sia che avvenga da internet o da una botnet mobile, potrebbe potenzialmente ridurre significativamente la disponibilità di servizi 5G o persino causarne l'interruzione. Di conseguenza, la parte core della rete si configura come la sezione più importante da proteggere, in particolare se si vuole garantire la continuità di funzionamento della maggior parte dei servizi e delle applicazioni che transitano su di essa, soprattutto di quelli critici.

4) Il quarto dominio è costituito dalle **applicazioni e servizi** di terze parti (generalmente OTT) ospitati dagli operatori di telecomunicazioni. A questo livello la sicurezza dipende quindi dalla qualità delle applicazioni esterne, dall'expertise dei loro sviluppatori e dalle operazioni di aggiornamento e manutenzione. In questo caso, infatti, uno dei rischi potrebbe essere costituito dalla minore esperienza in cybersecurity da parte degli sviluppatori di tali servizi terzi[3].

Tra i fattori che determinano l'allargamento del perimetro di attacco si evidenzia anche il c.d. *edge computing*, ovvero la distribuzione di piccoli data center dotati di capacità di elaborazioni che siano il più possibile vicini all'"edge" (cioè al "limite" o al "margine" della rete) che devono servire al fine di garantire la latenza *ultra low* necessaria per i servizi avanzati di IoT.

La Fig. 5 riporta il diverso grado di sicurezza e di rischio, andando dal verde (applicazioni sicure) fino al rosso (applicazioni ad alto rischio). L'assenza del verde sembrerebbe ribadire l'attuale impossibilità di garantire applicazioni completamente sicure, mentre a livello di rischio più basso si trovano i servizi di assistenza medica di base, i servizi digitali e multimediali, quelli connessi ai dispositivi wearable e alle case intelligenti. Risultano più delicate le applicazioni business mobili, i servizi finanziari e le reti intelligenti (relative prevalentemente ad utilities e trasporti). Sono considerati a rischio ancor più elevato le applicazioni legate all'automazione dei sistemi relativi a produzione manifatturiera, robotica e logistica, mentre sono ad alto rischio quelle che coinvolgono potenzialmente l'incolumità delle persone quali auto a guida autonoma e applicazioni critiche relative alla sanità digitale (ad esempio monitoraggio di alto livello e operazioni chirurgiche a distanza).

Fig. 5: Gradi di rischio nelle applicazioni di rete 5G



Fonte: DCMS 5G Testbeds & Trials, UK, dicembre 2018

Le linee guida per determinare il maggiore livello di sicurezza in ambito 5G consistono nello sviluppo una sorta di *trusted execution environment* per ogni sensore e quindi di un sistema di blockchain finalizzato

[3] Questo dominio esclude invece le applicazioni "interne" fornite dai *network operator*, che ricadono nella c.d. parte "core" della rete, così come le loro piattaforme di gestione.

al controllo del work flow degli stessi sensori. Ciò consentirebbe di bloccare loro l'accesso alla rete in tempo reale usando sistemi di access control implementati all'interno della rete internet. In termini più generali, lo sviluppo di sistemi di sicurezza in ambito 5G dovrà includere principi quali **flessibilità**, dovuta al diverso tipo di sensori che verranno collegati (dalla sanità all'agricoltura fino al controllo della tenuta di ponti e altre infrastrutture viarie), ***supreme built-in security*** (implementazione integrata nei sistemi 5G in particolare relativa a smartphones e sensori), e **automatizzata**, ovvero centralizzata e gestita da un orchestratore dotato di intelligenza artificiale in grado di riconoscere in tempo reale anomalie del sistema e di attivare i dispositivi di sicurezza preventivamente implementati nella rete, in un'ottica di Security as a service[4].

Alla luce della vastità e della complessità delle reti 5G e della superficie di attacco da parte di malintenzionati, si osserva come sembri riduttivo limitare l'analisi dei rischi per la sicurezza nazionale alla provenienza dei fornitori delle apparecchiature della rete di accesso, come avvenuto nel dibattito recente. In particolare, un aspetto importante da considerare nel valutare se e come concedere l'autorizzazione a soggetti extra europei ad operare in Italia è relativa proprio alla collocazione di tale componentistica all'interno della rete. Allo stato attuale, e verosimilmente per i prossimi 18-24 mesi, la rete 5G consisterà di fatto in una rete 4G su cui verranno montate delle BTS 5G (ovvero "stazioni radio base" di quinta generazione). Ciò significa che, per questo lasso di tempo, la parte core della rete rimarrà sostanzialmente quella attuale, operante in 4G. La parte core della rete 5G, ovvero quella che comporta la trasformazione radicale dell'architettura e che consentirà il funzionamento strutturale del sistema, dei servizi e delle applicazioni, non verrà toccata fino ad allora e dunque non sarà implementata con componenti provenienti da Paesi extra europei (a meno che non lo sia già, qualora gli operatori di rete siano di origine extra europea).

5. I casi di Germania (BNetzA) e UK (NCSC e HC-SEC) e le possibili misure per minimizzare rischi

Esistono già diversi esempi di come si possano minimizzare i rischi senza minare la concorrenza, bloccando l'accesso alla fornitura di hardware e software per le reti 5G prodotti da aziende extra europee.

In **Germania**, a marzo 2019, la *BNetzA* (il regolatore tedesco dei servizi a rete, tra i quali le tlc) ha pubblicato una serie di requisiti di sicurezza che gli operatori di telecomunicazioni devono rispettare nel Paese. Tra questi, si prevede l'impossibilità per gli operatori di utilizzare componentistica di un singolo vendor e la necessità di utilizzare per le operazioni di infrastrutturazione e manutenzione solo personale qualificato. Peraltro, nei casi in cui gli operatori subappaltino a terze parti tali attività, questi devono essere "professionalmente competenti, affidabili e di fiducia". In generale i sistemi possono essere forniti soltanto da operatori di fiducia che rispondano alla regolamentazione relativa alla sicurezza nazionale e garantiscano la segretezza delle comunicazioni e la *data protection*. Il traffico di rete deve essere

[4] M. Dècina, "5G Security (& Privacy)", giugno 2019.

costantemente monitorato rispetto a possibili anomalie e devono essere previste appropriate misure di protezione per far fronte a possibili criticità. Le misure sono valide per tutte le reti, tutti gli operatori e tutti i service providers, indipendentemente dalla tecnologia che impiegano (quindi non solo per le reti 5G). I componenti possono essere usati solo se certificati dal Federal Office for Information Security e testati regolarmente. Inoltre deve essere dimostrato che l'hardware testato per i componenti di sicurezza ed il codice sorgente siano realmente impiegati nei prodotti utilizzati. I requisiti verranno aggiornati regolarmente alla luce dell'evoluzione del contesto tecnologico e relativi alla sicurezza.

In **Gran Bretagna** esistono lo *UK National Cybersecurity Center* (NCSC) e lo *Huawei Cybersecurity Evaluation Center* (HC-SEC), i quali cooperano con gli operatori di rete e con il vendor Huawei per ridurre i rischi e valutare la sicurezza sia degli apparati che delle configurazioni di rete. L'HC-SEC ha un board indipendente ed ha pubblicato delle specifiche su come gli apparati di Huawei debbano essere sviluppati, ad esempio il divieto di sviluppare capacità di intercettazione legali con Huawei e ZTE e di creare connessioni *Vpn*, insieme all'obbligo di effettuare le attività di manutenzione attraverso gli operatori di rete. Inoltre il governo britannico prevede di utilizzare la tecnologia di diversi vendor e di limitare l'approvvigionamento dei componenti provenienti da operatori extra europei alle parti non-core della rete. Anche in questo caso l'attenzione è posta sulla procedura relative allo sviluppo e alla sicurezza e al modo in cui i componenti vengono implementati nelle parti critiche delle reti.

Fig. 6: Cybersecurity in Germania e Regno Unito: misure a confronto (giugno 2019)

GERMANIA

Requisiti BNetzA (marzo 2019)

- Impossibilità per gli operatori di utilizzare componentistica di un singolo vendor
- Necessità di utilizzare per le operazioni di infrastrutturazione e manutenzione so**lo personale qualificato.**
- Rapporto fiduciario in caso di **subappalto**
- Fornitori di sistemi devono conformarsi alla **regolamentazione** su **sicurezza nazionale**, **segretezza** delle comunicazioni e **data protection**.
- **Monitoraggio** costante del traffico di rete rispetto ad anomalie
- Componenti **certificati** dal **Federal Office for Information Security** e testati regolarmente.
- Dimostrazione che hardware testato e codice sorgente siano realmente impiegati nei prodotti utilizzati.
- I requisiti verranno regolarmente **aggiornati**
- Misure sono valide per tutte le reti, tutti gli operatori e tutti i service providers.

REGNO UNITO

Governo prevede di:

- utilizzare la tecnologia di **diversi vendor**

- limitare l'approvvigionamento dei componenti provenienti da operatori **extra europei** alle parti **non-core** della rete.

Due entità: UK National Cybersecurity Center (**NCSC**) e lo Huawei Cybersecurity Evaluation Center (**HC-SEC**)

- cooperano con gli operatori di rete e con il vendor Huawei per:
  - → ridurre i rischi
  - → valutare la **sicurezza** sia degli **apparati** che delle **configurazioni** di rete.

L'HC-SEC ha un board **indipendente** ed ha pubblicato delle specifiche su come gli apparati di Huawei debbano essere sviluppati:

- →il divieto di sviluppare capacità di **intercettazione legali** con Huawei e Zte
- →divieto di creare connessioni **Vpn**
- →obbligo di effettuare le attività di **manutenzione** attraverso gli operatori di rete.

Fonte: elaborazione I-Com su varie

In generale, appare utile l'introduzione di una certificazione di sicurezza per gli operatori che fanno parte della filiera del 5G. Un altro strumento che potrebbe rivelarsi utile è costituito dal NESAS (*Network Equipment Security Assurance Scheme*), lo schema di sicurezza definito da GSMA e 3GPP per supportare lo sviluppo di apparecchiature di rete sicure. Laboratori indipendenti effettuano dei test sul processo di sviluppo gestito dal vendor rispetto a requisiti di sicurezza definiti dal 3GPP (non provano assenza di malware ma aiutano ad aumentare la qualità complessiva del software).

Il *Cybersecurity Act* consente di stabilire certificazioni obbligatorie per le apparecchiature di rete mobile, pertanto il NESAS potrebbe essere implementato come schema di certificazione europea. Inoltre, poiché molti paesi non hanno approfonditi requisiti di sicurezza per gli operatori addetti alla sicurezza e alla manutenzione delle apparecchiature di rete, queste dovrebbero essere sviluppate a livello nazionale tra operatori e agenzie per la sicurezza nazionale. Sarebbe importante anche incentivare la collaborazione con ETIS, l'organizzazione no profit che raccoglie i principali provider tlc europei e che è strutturata in diversi gruppi di lavoro, tra i quali uno sulla sicurezza informatica.
Sebbene nessuna di queste azioni sarebbe sufficiente se implementata singolarmente, un pacchetto di misure riguardanti gli standard e la loro implementazione, così come la configurazione delle reti e le procedure di manutenzione, aumenterebbe sensibilmente la resilienza e l'affidabilità delle reti mobili e potrebbe essere implementate indipendentemente dalla discussione sui vendor cinesi.
Di seguito una serie di misure proposte dal think tank tedesco, *Stiftung Neue Verantwortung*, che potrebbero essere adottate in relazione ai diversi domini relativi allo standard ed alla sua implementazione, alla configurazione ed alle procedure di manutenzione:

1. Standard e implementazione
    a. *Security assessment* sui processi di sviluppo dei vendor e certificazione di sicurezza sui prodotti It (NESAS di 3GPP e GSMA).
    b. Sviluppo di schemi di certificazione obbligatori per le apparecchiature di rete mobile nel quadro del Cybersecurity Act europeo (basato su o complementare al NESAS).
2. Configurazione
    a. Sviluppo di requisiti nazionali relativi a configurazione di sicurezza su apparecchiature di rete mobile tra operatori e agenzie nazionali per la sicurezza.
3. Procedure e manutenzione
    a. Sviluppo di requisiti nazionali relativi a configurazione di sicurezza di reti mobili (es. requisiti per i processi di sviluppo software o manutenzione da remoto).
    b. *Risk analysis* continuativa e "*mitigation*" tra operatore, vendor e le agenzie di sicurezza nazionale.

6. Dalla golden share al golden power. L'evoluzione normativa e l'applicazione alle reti 5G

La storia degli ultimi decenni ha visto un mutamento delle modalità di intervento dello Stato nei settori strategici dell'economia. Trainati dall'Unione europea e dall'obiettivo di creare un mercato concorrenziale, infatti, gli stati membri, tra cui l'Italia, sono passati da una gestione pubblicistica ad una privatizzazione delle imprese operanti in tali settori, cui si è accompagnata la previsione della "golden share". Si tratta di uno strumento che affonda le proprie radici nella tradizione britannica e che indica la conservazione, da parte dello Stato, di una partecipazione azionaria con poteri esorbitanti rispetto a quelli attribuiti ad un normale azionista. In Italia tale strumento è stato introdotto con il **decreto legge**

31 maggio 1994, n. 332, convertito con legge 30 luglio 1994, n. 474, che ha disciplinato il potere di introdurre nello statuto delle società oggetto di privatizzazione poteri speciali che il Governo, attraverso il Ministro dell'economia e delle finanze, può esercitare anche dopo aver ceduto il controllo. La Corte di Giustizia ha tuttavia ritenuto che tale meccanismo fosse in conflitto con la libertà di circolazione dei capitali ed il diritto di stabilimento, intervenendo con procedure di infrazione nei confronti di diversi paesi - tra cui l'Italia – ed adottando la **Comunicazione n. C220 del 19/07/1997** nella quale ha affermato che l'esercizio di tali poteri deve comunque essere attuato senza discriminazioni, è ammesso se si fonda su "criteri obiettivi, stabili e resi pubblici" e se è giustificato da "motivi imperiosi di interesse generale". Per quanto riguarda gli specifici settori di intervento, la Commissione ha ammesso un regime particolare per gli investitori di un altro Stato membro qualora esso sia giustificato da motivi di ordine pubblico, di pubblica sicurezza e di sanità pubblica purché, conformemente alla giurisprudenza della Corte di giustizia, sia esclusa qualsiasi interpretazione che si fondi su considerazioni di carattere economico.
Nel tentativo di conformare il proprio ordinamento ai dettami della Corte, il nostro paese, con il **decreto legge 15 marzo 2012 n. 21, convertito con modificazioni con la legge n. 56 del 2012**, ha ridefinito, anche mediante il rinvio ad atti di normazione secondaria (DPCM), l'ambito oggettivo e soggettivo, la tipologia, le condizioni e le procedure di esercizio del c.d. "**golden power**". Con tale locuzione, in particolare, si fa riferimento ad una serie di poteri esercitabili nei settori della difesa e della sicurezza nazionale, nonché in alcuni ambiti di attività definiti di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni.
La principale differenza con la normativa precedente, che segna il passaggio dalla golden share al golden power, risiede nell'ambito operativo della nuova disciplina che, superando il precedente sistema che limitava l'esercizio dei poteri speciali alle società privatizzate o in mano pubblica, abilita l'esercizio di tali poteri speciali rispetto a tutte le società, sia pubbliche che private, che svolgono attività considerate di rilevanza strategica.
Le norme affidano ad uno o più decreti del Presidente del Consiglio l'individuazione di attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale in rapporto alle quali potranno essere attivati i poteri speciali, l'individuazione della tipologia di atti o operazioni infragruppo esclusi dall'ambito operativo della nuova disciplina, la concreta disciplina relativa all'esercizio dei poteri speciali nonché la previsione di ulteriori disposizioni attuative.
Con riferimento all'esercizio dei poteri speciali nei comparti della sicurezza e della difesa la normativa esige la sussistenza di una **minaccia di grave pregiudizio per gli interessi essenziali della difesa e della sicurezza nazionale**. In tali ipotesi, al Governo è consentito: imporre specifiche condizioni all'acquisto di partecipazioni in imprese strategiche nel settore della difesa e della sicurezza; porre il veto all'adozione di delibere relative ad operazioni straordinarie o di particolare rilevanza, ivi incluse le modifiche di clausole statutarie eventualmente adottate in materia di limiti al diritto di voto o al possesso azionario; opporsi all'acquisto di partecipazioni, ove l'acquirente arrivi a detenere un livello della partecipazione al capitale in grado di compromettere gli interessi della difesa e della sicurezza nazionale. Al fine di valutare la minaccia di grave pregiudizio agli interessi essenziali della difesa e della sicurezza nazionale, il Governo considera, tenendo conto dell'oggetto della delibera, la rilevanza strategica dei beni o delle imprese

oggetto di trasferimento, l'idoneità dell'assetto risultante dalla delibera o dall'operazione a garantire l'integrità del sistema di difesa e sicurezza nazionale, la sicurezza delle informazioni relative alla difesa militare, gli interessi internazionali dello Stato, la protezione del territorio nazionale, delle infrastrutture critiche e strategiche e delle frontiere, nonché gli elementi di cui al comma 3 e, nello specifico: a) l'adeguatezza, tenuto conto anche delle modalità di finanziamento dell'acquisizione, della capacità economica, finanziaria, tecnica e organizzativa dell'acquirente nonché del progetto industriale, rispetto alla regolare prosecuzione delle attività, al mantenimento del patrimonio tecnologico, anche con riferimento alle attività strategiche chiave, alla sicurezza e alla continuità degli approvvigionamenti, oltre che alla corretta e puntuale esecuzione degli obblighi contrattuali assunti nei confronti di pubbliche amministrazioni, direttamente o indirettamente, dalla società le cui partecipazioni sono oggetto di acquisizione, con specifico riguardo ai rapporti relativi alla difesa nazionale, all'ordine pubblico e alla sicurezza nazionale; b) l'esistenza, tenuto conto anche delle posizioni ufficiali dell'Unione europea, di motivi oggettivi che facciano ritenere possibile la sussistenza di legami fra l'acquirente e paesi terzi che non riconoscono i principi di democrazia o dello Stato di diritto, che non rispettano le norme del diritto internazionale o che hanno assunto comportamenti a rischio nei confronti della comunità internazionale, desunti dalla natura delle loro alleanze, o hanno rapporti con organizzazioni criminali o terroristiche o con soggetti ad esse comunque collegati.

Dal punto di vista procedurale, il decreto legge ha disciplinato puntualmente **termini e procedure da osservare**; il comma 4, in particolare, prescrive che ai fini dell'esercizio del potere di veto, l'impresa notifichi alla Presidenza del Consiglio dei Ministri una informativa completa sulla delibera o sull'atto da adottare in modo da consentire il tempestivo esercizio del potere di veto. Quest'ultimo, in particolare, deve essere comunicato dal Presidente del Consiglio entro 15 gg dalla notifica con possibilità, qualora si renda necessario richiedere informazioni all'impresa, di sospendere tale termine, per una sola volta, fino al ricevimento delle informazioni richieste, che sono rese entro il termine di dieci giorni. Le richieste di informazioni successive alla prima, invece, non sospendono i termini. Una volta decorsi i predetti termini, l'operazione oggetto di notifica può essere effettuata. Dalla violazione di tale disciplina la normativa fa discendere la nullità delle delibere o degli atti adottati, la facoltà, per il Governo, di ingiungere alla società ed all'eventuale controparte di ripristinare a proprie spese la situazione anteriore, nonché l'imposizione di una sanzione amministrativa pecuniaria fino al doppio del valore dell'operazione e comunque non inferiore all'uno per cento del fatturato cumulato realizzato dalle imprese coinvolte nell'ultimo esercizio per il quale sia stato approvato il bilancio.

L'art. 2 del decreto in esame ha invece affidato a regolamenti (anziché DPCM) da adottare, previo parere delle Commissioni parlamentari competenti, l'individuazione degli asset strategici nel settore dell'energia, dei trasporti e delle comunicazioni, l'esercizio dei poteri speciali e l'individuazione di ulteriori disposizioni attuative della nuova disciplina.

I poteri speciali esercitabili nel settore dell'energia, dei trasporti e delle comunicazioni si sostanziano nella possibilità di far valere il veto dell'esecutivo alle delibere, agli atti e alle operazioni concernenti asset strategici, in presenza dei requisiti richiesti dalla legge, ovvero imporvi specifiche condizioni; di

porre condizioni all'efficacia dell'acquisto di partecipazioni da parte di soggetti esterni all'UE in società che detengono attivi "strategici" e, in casi eccezionali, opporsi all'acquisto stesso.
Gli obblighi di notifica sono estesi alle delibere, atti o operazioni aventi ad oggetto il mutamento dell'oggetto sociale, lo scioglimento della società, la modifica di clausole statutarie riguardanti l'introduzione di limiti al diritto di voto o al possesso azionario. Il veto alle delibere, atti o operazioni può essere espresso qualora essi diano luogo a una situazione eccezionale, non disciplinata dalla normativa - nazionale ed europea - di settore, di minaccia di grave pregiudizio per gli interessi pubblici relativi alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti, ivi compresi le reti e gli impianti necessari ad assicurare l'approvvigionamento minimo e l'operatività dei servizi pubblici essenziali. Nel computo della partecipazione rilevante ai fini dell'acquisto si tiene conto della partecipazione detenuta da terzi con cui l'acquirente ha stipulato patti parasociali. Anche in tal caso, dalle violazioni delle previsioni appena descritte discende la sanzione della nullità degli atti.
Se questo era la cornice normativa nell'ambito della quale sono stati adottati numerosi DPCM attuativi, il **D.L. 25 marzo 2019, n. 22** (c.d. **Decreto Brexit**), convertito con modificazioni dalla Legge 20 maggio 2019, n. 41, ha aggiunto all'ambito previsto dalla legge n. 56/2012 **l'art. 1 bis**, rubricato "Poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G", con il quale sono stati inclusi, nelle attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale, i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G.
La nuova disposizione, in particolare, introducendo una chiara innovazione rispetto al regime generale precedente, prevede che:

1) il meccanismo di tutela dello Stato scatterà non solo nei casi di acquisizioni di partecipazioni azionarie, ma **anche nel caso di forniture di materiali e servizi**;
2) l'obbligo di notifica ai fini dell'esercizio del **potere di veto** o dell'i**mposizione di specifiche prescrizioni o condizioni** riguarda la stipula di contratti o accordi aventi ad oggetto l'acquisto di beni o servizi relativi alla **progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti 5G, ovvero l'acquisizione di componenti ad alta intensità tecnologica funzionali alla predetta realizzazione o gestione**;
3) le operazioni sopra descritte sono sottoposte a notifica qualora poste in essere con "**soggetti esterni all'Unione europea**" con ciò intendendo: a) qualsiasi persona fisica o persona giuridica, che non abbia la residenza, la dimora abituale, la sede legale o dell'amministrazione ovvero il centro di attività principale in uno Stato membro dell'Unione europea o dello Spazio economico europeo o che non sia comunque ivi stabilito; b) qualsiasi persona giuridica che abbia stabilito la sede legale o dell'amministrazione o il centro di attività principale in uno Stato membro dell'Unione europea o dello Spazio economico europeo o che sia comunque ivi stabilito, e che risulti controllato direttamente o indirettamente da una persona fisica o da una persona giuridica di cui al n. 1); c) qualsiasi persona fisica o persona giuridica che abbia stabilito la residenza, la dimora abituale, la sede legale o dell'amministrazione o il centro di attività principale in uno Stato membro dell'Unione europea o dello Spazio economico europeo o che sia comunque ivi stabilito, al fine di eludere l'applicazione della disciplina in esame;

4) ai fini dell'esercizio dei poteri speciali, è prevista la valutazione anche 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".

Posta l'applicazione, alle ipotesi sub b), dei termini di cui al comma 4 del dl n. 21/2012, sopra descritti, l'art. 1 bis prevede la possibilità di adottare con DPCM misure di semplificazione delle modalità di notifica, dei termini e delle procedure relativi all'istruttoria.

Al fine dell'adozione di tale decreto di semplificazione, il 28 giugno 2019 la Presidenza del Consiglio dei Ministri ha indetto una **consultazione pubblica** tesa a raccogliere dai soggetti interessati - entro il 19 luglio 2019 - contributi circa l'individuazione delle modalità semplificate di notifica, eventualmente differenziate (ad esempio, in base all'attività svolta, ai servizi offerti o alla tipologia di infrastruttura interessata) nonché la definizione di procedure e termini semplificati per l'istruttoria in presenza di specifiche circostanze.

In ossequio al dettato normativo tracciato dal decreto Brexit, il Governo è stato chiamato a pronunciarsi sull'**accordo commerciale tra Fastweb ed il colosso tecnologico sudcoreano Samsung** per la progettazione, fornitura, configurazione e manutenzione di apparati software relativi alle componenti radio e core network per la realizzazione della rete 5G FWA nelle città pilota di Bolzano e Biella. Nel pronunciarsi su tale operazione, il Gruppo di Coordinamento che affianca la Presidenza del Consiglio nell'esercizio del golden power ha adottato un decreto datato 26 giugno 2019, destinato probabilmente a rappresentare un modello per future simili operazioni, con il quale ha deciso di esercitare i poteri speciali nella forma dell'imposizione di specifiche prescrizioni, in relazione all'operazione notificata. Si tratta di misure puntuali che si sostanziano, tra le altre, nell'effettuare test e verifiche ad opera di un soggetto terzo (riconosciuto dai soggetti istituzionali competenti) tesi a confermare l'inesistenza di interazioni funzionali tra le reti core e non virtuali della sperimentazione e l'attuale rete core di Fastweb, l'adozione, da parte di quest'ultima, di misure di protezione e l'invio, alla Presidenza del Consiglio, degli esiti delle verifiche compiute sulla sicurezza al termine della sperimentazione, il coinvolgimento della funzione aziendale Security nei processi di governance relativi ad attività considerate strategiche alla luce del quadro normativo vigente, la trasmissione, entro 60 gg dall'adozione del decreto e successivamente ogni sei mesi, di una relazione descrittiva delle misure adottate per ottemperare a quanto prescritto dal decreto ed infine la tempestiva comunicazione di qualsiasi determinazione societaria o aziendale rilevante rispetto alle condizioni dettate dall'esecutivo nell'esercizio dei poteri speciali di cui lo stesso è titolare.

La disciplina del golden power, così come fissata dal decreto legge 15 marzo 2012 n. 21, convertito con modificazioni con la legge n. 56 del 2012 e successivamente integrata dal decreto Brexit, ha subito un'ulteriore rimodulazione ad opera del **decreto legge n. 64 dell'11 luglio 2019** decaduto, per mancata conversione in legge, il 9 settembre scorso. Nonostante la macchina normativa fosse stata avviata, essendo iniziato l'iter di conversione del decreto presso la Commissione Finanza del Senato e nonostante il Governo abbia già esercitato, nel caso Fastweb-Samsung sopra menzionato, il golden power, il Governo - prima che si aprisse la crisi politica poi culminata nella definitiva rottura dell'alleanza Movimento 5Stelle/Lega e nella creazione del Governo Conte bis sostenuto da Movimento 5 Stelle,

Partito Democratico e LeU - ha deciso di non alimentare tale procedimento di conversione anche in considerazione del fatto che era in agenda la sottomissione all'esame del Consiglio dei ministri di un disegno di legge per disciplinare in modo più organico la materia della sicurezza informatica nazionale.
Sebbene si tratti di una disciplina al momento decaduta è comunque importante svolgere una sintetica analisi dei principali contenuti della stessa in considerazione del fatto che sulla base delle norme introdotte dal decreto non convertito sono stati esercitati i poteri speciali non solo dal Governo che lo aveva adottato (nel caso Fastweb-Samsung citato) ma anche dal Governo Conte *bis*. Quest'ultimo, infatti, considerato che il termine di 45 giorni introdotto dal decreto sarebbe venuto meno il 9 settembre, in conseguenza della mancata conversione in legge del medesimo decreto e, dunque, sarebbe venuta meno la possibilità per il Governo di apporre condizioni a ben 5 operazioni *medio tempore* notificate, si è affrettato, il 5 settembre scorso, ad autorizzare, con condizioni, le operazioni notificate che coinvolgevano, nello specifico, Linkem, Tim, Vodafone, Fastweb e Wind.
In particolare, con il decreto n. 64 del 2019 la nuova disposizione prescriveva l'invio alla Presidenza del Consiglio dei ministri, entro dieci giorni dalla conclusione di un contratto o accordo di cui al comma 2, di un'informativa completa, in modo da consentire l'eventuale esercizio del potere di veto o l'imposizione di specifiche prescrizioni o condizioni e fissava in **45 giorni** dalla notifica il termine entro cui il Presidente del Consiglio dei ministri comunicava l'eventuale veto ovvero l'imposizione di specifiche prescrizioni o condizioni (l'inutile decorso di tale termine assume il significato di un mancato esercizio dei poteri speciali). Queste ultime, nello specifico, venivano formulate ogniqualvolta ciò fosse sufficiente ad assicurare la tutela degli interessi essenziali della difesa e della sicurezza nazionale. Qualora si fosse reso necessario richiedere informazioni all'impresa o formulare richieste istruttorie a soggetti terzi, la norma prevedeva la sospensione, per una sola volta, di tale termine di quarantacinque giorni, fino al ricevimento delle informazioni richieste, da rendere entro il termine di trenta giorni. Le richieste di informazioni successive alla prima, al contrario, non sospendevano i termini. In caso di incompletezza della notifica, il termine di quarantacinque giorni previsto dal presente comma decorreva dal ricevimento delle informazioni o degli elementi che la integrano. Qualora, invece, fosse stato necessario svolgere approfondimenti riguardanti aspetti tecnici relativi alla valutazione di possibili fattori di vulnerabilità in grado di compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano, era ammessa la sospensione del termine di quarantacinque giorni fino a quarantacinque giorni, prorogabili una sola volta in caso di particolare complessità.
Molto rilevante per l'impatto che poteva esercitare sulle imprese, la disposizione che attribuiva al Governo, nell'esercizio dei poteri speciali, di ingiungere all'impresa acquirente e all'eventuale controparte il ripristino, a proprie spese, della situazione anteriore.
Quanto al regime sanzionatorio, all'inosservanza degli obblighi di notifica ovvero delle disposizioni contenute nel provvedimento di esercizio dei poteri speciali, la norma ricollegava una sanzione amministrativa pecuniaria fino al doppio del valore dell'operazione e comunque non inferiore all'uno per cento del medesimo valore.
In relazione all'ambito applicativo, è interessante evidenziare come il decreto prevedeva l'applicazione di tali nuovi disposizioni anche ai procedimenti pendenti alla data di entrata in vigore del presente

decreto per i quali i termini non erano ancora spirati (per cui ferma restando la data di inizio, i termini erano prorogati fino al raggiungimento della nuova durata stabilita, se maggiore di quella anteriormente prevista).

Se questo era il quadro introdotto, si è già evidenziato come tra le ragioni alla base della decisione del Governo Conte di non alimentare il procedimento di conversione vi fosse la sottomissione all'esame del Consiglio dei ministri di un disegno di legge per disciplinare in modo più organico la materia della sicurezza informatica nazionale. Il 19 luglio, infatti, è stato varato uno schema di disegno di legge "in materia di perimetro di sicurezza nazionale cibernetica" recante disposizioni volte ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli 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 o interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. Tale disegno di legge, in particolare: 1) definisce le finalità del perimetro e le modalità di individuazione dei soggetti pubblici e privati che ne fanno parte, nonché delle rispettive reti, dei sistemi informativi e dei servizi informatici rilevanti per le finalità di sicurezza nazionale cibernetica per i quali si applicano le misure di sicurezza e le procedure descritte; 2) introduce un sistema di procurement più sicuro per i soggetti rientranti nel perimetro che intendano procedere all'affidamento di forniture di beni e servizi ICT destinati a essere impiegati sulle reti, sui sistemi e per i servizi rilevanti; 3) attribuisce competenza al Ministero dello sviluppo economico per i soggetti privati inclusi nel perimetro e all'Agenzia per l'Italia Digitale (AgID) per le amministrazioni pubbliche; 4) introduce un sistema di vigilanza e controllo sul rispetto degli obblighi e procedure introdotti fissando altresì le sanzioni connesse ad eventuali violazioni degli stessi; 5) prevede attività di ispezione e verifica da parte delle strutture specializzate in tema di protezione di reti e sistemi nonché, per quanto riguarda la prevenzione e il contrasto del crimine informatico, delle Amministrazioni da cui dipendono le Forze di polizia e le Forze armate, che ne comunicano gli esiti.

Centrale, nell'impianto delineato dal disegno di legge, il ruolo del Cento di valutazione e certificazione nazionale (CVCN) - istituito a febbraio scorso ma ancora non operativo - al quale è attribuito il potere di imporre condizioni e test di hardware e software sulla base di una valutazione del rischio, anche in relazione all'ambito di impiego e in un'ottica di gradualità nonché il dovere di segnalare la mancata collaborazione per l'effettuazione delle attività di test, dei soggetti individuati quali fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi e ai servizi rilevanti al MISE o all'AGID a seconda della natura privata o pubblica del soggetto destinatario della fornitura. Allo stesso CVCN sono poi affidati compiti specifici nell'ambito dell'approvvigionamento ICT destinato a reti, sistemi e servizi rilevanti ed in particolare: a) contributo all'elaborazione delle misure di sicurezza per ciò che concerne affidamenti di forniture di beni e servizi; b) svolgimento delle attività di verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità note, anche in relazione all'ambito di impiego, dettando, se del caso, anche prescrizioni di utilizzo al committente; c) elaborazione e adozione di schemi di certificazione cibernetica, laddove, per ragioni di sicurezza nazionale e su conforme avviso del CISR-tecnico, gli schemi di

certificazione esistenti non siano ritenuti adeguati alle esigenze di tutela del perimetro di sicurezza nazionale cibernetica.
Lo stesso disegno di legge affidava a tre successivi DPCM e ad un regolamento, da adottarsi rispettivamente entro sei mesi ed un anno dall'entrata in vigore della legge, l'individuazione dei soggetti rientranti nel perimetro e dei criteri per la formazione degli elenchi delle reti, dei sistemi e dei servizi rilevanti, nonché la disciplina dei termini e delle modalità attuative. Rilevante anche la previsione che impone ai soggetti rientranti nel perimetro di sicurezza nazionale cibernetica di predisporre e comunicare (ad AGID o al Ministero), con cadenza almeno annuale, un elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica secondo criteri la cui fissazione è affidata all'organismo tecnico di supporto al CISR.
Per lo svolgimento di tali attività, il medesimo disegno prevedeva assunzioni a tempo indeterminato, mediante concorso pubblico, di un contingente massimo di 57 unità reclutate dal Dipartimento della funzione pubblica per il MiSE, nel limite di spesa annua 1.002.000 per l'anno 2019 ed euro 3.005.000 annui a decorrere dall'anno 2020. Per la realizzazione, l'allestimento e il funzionamento del Centro di valutazione e certificazione nazionale (CVCN) è autorizzata la spesa di euro 3.200.000 per l'anno 2019 e di euro 2.850.000 per ciascuno degli anni dal 2020 al 2023 e di euro 750.000 annui a decorrere dall'anno 2024.
Questo, tuttavia, non ha rappresentato l'ultimo approdo in materia. Il Governo Conte *bis*, infatti, è tornato a riflettere sull'argomento e, ravvisando la straordinaria necessità ed urgenza *"di disporre, per le finalità di sicurezza nazionale, di un sistema di organi, procedure e misure che consenta un'efficace valutazione sotto il profilo tecnico della sicurezza degli apparati e dei prodotti"*, ha predisposto uno **schema di decreto legge,** teso a sostituire il descritto disegno di legge, **che ha ottenuto il via libera del Consiglio dei Ministri il 19 settembre scorso**. Si tratta, invero, non soltanto della scelta di un diverso e ben più potente strumento normativo, ma anche dell'introduzione di importanti novità. Il decreto in esame, infatti, pur conservando l'impianto generale delineato nel disegno di legge, attribuisce le competenze di verifica e controllo alla Presidenza del Consiglio dei ministri, in luogo dell'AGID, nel caso di soggetti pubblici (ferma restando la possibilità per la Presidenza di avvalersi dell'AGID) - prevedendo dunque 10 nuove assunzioni presso la Presidenza e non più presso l'AGID - e riduce, rispettivamente, a quattro e dieci mesi i termini per individuare le amministrazioni pubbliche, gli enti e gli operatori pubblici e privati che devono entrare a far parte del cosiddetto perimetro cibernetico, a garanzia della sicurezza di reti e servizi considerati "strategici" e per la definizione delle procedure secondo cui i soggetti che fanno capo al perimetro notificano gli incidenti che hanno impatto su reti, sistemi e servizi.
Molto rilevante, per l'impatto sulla normativa in materia di golden power, l'art. 3. Tale disposizione, infatti, da un lato, prevede che l'esercizio dei poteri speciali in relazione alle reti, ai sistemi informativi e ai servizi strategici di comunicazione a banda larga basati sulla tecnologia 5G sia effettuato previa valutazione degli elementi indicanti la presenza di fattori di vulnerabilità da parte dei centri di valutazione individuati dalla nuova normativa; dall'altro, con riguardo ai contratti già autorizzati con DPCM - nell'esercizio del golden power di cui al D.L. 21/2012 così come integrato dal decreto Brexit - consente di modificare o integrare le misure prescrivendo la sostituzione di apparati e prodotti *"che*

risultano gravemente inadeguati sul piano della sicurezza". Si tratta di una disposizione molto importante che, fissando un termine di 60 gg. dall'entrata in vigore del regolamento di cui all'art. 1 comma 6, per modificare o integrare le condizioni e prescrizioni relative, appunto, a contratti già autorizzati, non può non sollevare qualche perplessità. Infatti, considerato che il regolamento sopra citato deve essere adottato entro 10 mesi dalla data di entrata in vigore della legge di conversione del decreto e che dall'entrata in vigore dello stesso decorrono ulteriori 60 gg. per valutare se intervenire apponendo nuove prescrizioni o modificando quelle già fissate, si palesa il rischio, neanche troppo astratto, di creare un clima di generale incertezza in grado di impattare negativamente sugli investimenti e lo sviluppo delle reti 5G.
Risulta inoltre confermato quanto previsto dal disegno di legge con riguardo al ruolo, i poteri e le competenze del CVCN così come - al netto della sostituzione dell'AGID con la Presidenza del Consiglio - la disposizione che prescrive ai soggetti rientranti nel perimetro di sicurezza nazionale cibernetica di predisporre e comunicare (alla Presidenza o al Ministero), con cadenza almeno annuale, un elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica secondo criteri la cui fissazione è affidata all'organismo tecnico di supporto al CISR.

Conclusioni e spunti di policy

Il 5G è una tecnologia capace di impattare notevolmente sui sistemi economici e, conseguentemente, di avere degli effetti sensibili anche sugli assetti geopolitici, grazie alle proprie caratteristiche tecniche che lo configurano come il principale abilitatore per l'Internet of Things. Per quanto concerne il primo versante, i dati forniti dalla Commissione Europea hanno mostrato come l'impatto del 5G sull'economia continentale potrebbe arrivare sino a 113 miliardi di euro l'anno già dal 2025. I principali benefici potrebbero derivare dall'automotive (fino a 42 miliardi l'anno), dalla digitalizzazione di fabbriche e uffici (fino a 30 miliardi l'anno), nonché dai trasporti e dalle smart cities (oltre 8 miliardi ciascuno l'anno). Per tali ragioni, eventuali ritardi o extra-costi nell'implementazione delle reti 5G avrebbero un sensibile impatto nella riduzione di tali benefici e quindi sull'economia dell'Europa e dei singoli Stati membri. Lo studio condotto da Assembly, descritto nel par. 1, mostra come eventuali restrizioni del mercato ai soli vendor europei genererebbero ritardi dai 18 ai 24 mesi, con conseguenti costi o mancate entrate che ammonterebbero fino a 6,8 miliardi di sterline nella sola Gran Bretagna, nel triennio 2020-2022.
Le tematiche tecnologiche ed economiche si intrecciano necessariamente a quelle geopolitiche. La guerra commerciale tra Stati Uniti e Cina, il grande livello di avanzamento raggiunto da quest'ultima in ambito 5G e il fatto che, a livello mondiale, i vendor di apparecchiature di rete 5G siano solo 5, di cui due di nazionalità cinese, complicano ulteriormente la situazione, anche perché talvolta i diversi piani (tecnologico, economico e relativo alla sicurezza) vengono sovrapposti, aggiungendo caos a una situazione già complicata e altamente tecnica per sua natura.
Non c'è dubbio che la sicurezza nazionale vada perseguita e garantita e allo stesso tempo coniugata con la prosperità del Paese. Per tali ragioni, occorre ricercare un bilanciamento tra le esigenze di sicurezza e lo sviluppo delle reti e degli operatori, rispondendo sia a una contingenza geopolitica, che in alcune fasi

temporali può presentare momenti di criticità, sia attenuando l'impatto che procedure volte a mantenere la sicurezza possono determinare sul mercato, sugli operatori e sui consumatori. Questa dinamica appare amplificata dalla natura abilitante e cross-sector del 5G e della trasformazione digitale tout court, che determinano un allargamento del perimetro della sicurezza nazionale anche a comparti che fino a qualche anno fa ne sarebbero rimasti ampiamente al di fuori.

A tal fine, è importante distinguere gli aspetti geopolitici da quelli meramente tecnici, relativi alla sicurezza delle reti 5G. Rispetto a quest'ultimo tema, il 5G presenta infatti una duplice veste. Da un lato, considerata la sua conformazione distribuita e interconnessa (il Nist parla di *Supply chain risk management*), non è possibile garantirne al 100% l'imperforabilità. Ciò è dovuto all'allargamento della superficie di attacco (che includerà anche tutta la sensoristica proveniente da diversi ambiti) e al coinvolgimento di molteplici sistemi che ne rendono il funzionamento globale sempre più complesso, interdipendente da molteplici attori e continuamente in fase di sviluppo e aggiornamento. D'altro canto, si osserva come i sistemi di rete mobile siano sempre stati soggetti a possibili attacchi informatici, e come il 5G porti con sé, oltre a tutte le criticità e le vulnerabilità cui sono soggetti i sistemi basati sugli standard precedenti, anche delle possibilità di difesa capaci di innalzare il livello di sicurezza complessivo (si pensi alla creazione di un *trusted execution environment* per ogni sensore e allo sviluppo di sistemi di "Security as a Service") a un livello superiore rispetto a tutti gli standard precedenti.

A livello normativo, infrastrutture e servizi così complessi, con processi interni e architetture altrettanto intrecciate, vengono condivisi dalla sicurezza nazionale e pertanto richiedono una specifica disciplina. A tal proposito, una prospettiva interessante consiste nel suddividere il campo in tre aree: un'area "bianca", dove avviene tutto liberamente secondo le regole già fissate (da normative sugli appalti, codice civile, ecc.); un'area "nera", che riguarda strettamente la sicurezza nazionale e che andrebbe secretata; un'area "grigia" intermedia, nella quale il livello di sicurezza è importante ma non tale da arrivare alla secretazione prevista per la sicurezza nazionale, in cui possono essere dettate regole più stringenti ma a cui si partecipa in maniera aperta e pubblica. Tale area grigia potrebbe essere definita con una norma interpretativa in grado di armonizzare la legislazione e gli strumenti già in vigore (ad es. la legge sulle infrastrutture limite, il regolamento sulla privacy, la direttiva NIS, e lo stesso golden power). In essa sarebbe quindi possibile operare con un sistema di certificazione meno stringente rispetto a quello previsto per la sicurezza nazionale, ma comunque in grado di garantire l'accreditamento degli operatori e la certificazione dei prodotti utilizzati, verosimilmente da parte del nascente centro di valutazione e certificazione nazionale del MiSE. Tale allargamento del perimetro della sicurezza a un'area intermedia potrebbe consentire di risolvere contemporaneamente le questioni aperte relative a sicurezza nazionale e competitività.

Guardando al mondo delle aziende è forte la necessità che, almeno a livello europeo, si arrivi a una normativa unica o a **forme di certificazione unificate**. In particolare, considerando l'esiguo numero di aziende produttrici di apparecchiature 5G, che quindi operano su decine di mercati nazionali, la difficoltà di trovarsi di fronte a 28 diverse normative, che verosimilmente verrebbero riprese come criteri selettivi dai rispettivi bandi pubblici nazionali, rischierebbe di comportare criticità e ritardi sia sul fronte delle tempistiche sia su quello dell'osservanza delle diverse normative nazionali.

Una soluzione importante a tal proposito potrebbe essere costituita dal NESAS (*Network Equipment Security Assurance Scheme*), le cui specifiche sono sviluppate congiuntamente dal 3GPP e dalla GSMA proprio per superare le criticità dovute ad una moltiplicazione e sovrapposizione di requisiti di sicurezza dei singoli Stati. Un punto rilevante in tale direzione consisterebbe nel coinvolgimento di operatori di rete, vendor e istituzioni per la definizione di un protocollo di certificazione.
A livello di configurazione e di procedure, una via interessante è vicina a quanto avviene in UK, e coinvolge la realizzazione del Centro di valutazione italiano per la cybersecurity (CVCN).
In generale, uno dei criteri più importanti appare l'applicazione di una discriminazione non per provenienza geografica ma rispetto al *risk assessment*, che consiste nel segmentare prodotti e operatori non sulla base della nazionalità ma secondo il criterio della rilevanza del rischio.
A tal proposito, la tassonomia dei possibili rimedi realizzata dalla *Stiftung Neue Verantwortung* fornisce un quadro interessante, distinguendo tra tre livelli: **standard e implementazione**, per i quali potrebbero essere applicati il NESAS e sviluppati schemi di certificazione europei; **configurazione**, relativa allo sviluppo di requisiti nazionali di sicurezza per le apparecchiature di rete mobile tra operatori e agenzie nazionali; **procedure e manutenzione**, consistenti sia nello sviluppo di requisiti nazionali di sicurezza delle reti mobili per le attività di manutenzione, sia nelle operazioni di *risk analysis* continuativa e *risk mitigation* che verrebbero effettuate dal Centro di valutazione e certificazione nazionale coinvolgendo anche vendor e operatori tlc.
In questo contesto, grande importanza riveste anche il fattore tempo, considerato fondamentale sia rispetto alle tempistiche relative alle operazioni di notifica e feedback, sia per quanto concerne l'orizzonte entro cui gli operatori di rete otterranno un ritorno sugli ingenti investimenti effettuati per le bande 5G, per le quali il costo è stato il più alto in Europa. Per quanto riguarda il primo aspetto, occorre tenere presente che la programmazione, la progettazione e la realizzazione delle reti 5G richiedono una tempistica che va ben oltre il mese o l'anno, e i tempi relativi alle procedure di sicurezza si sommano e si propagano esponenzialmente sui mesi e gli anni necessari al roll out. Rispetto al rientro dagli investimenti, è importante che il nuovo standard si configuri rapidamente come una tecnologia capace di garantire servizi che producono ricavi aggiuntivi, perché se così non fosse, si determinerebbe inevitabilmente un inaridimento della propensione a investire, con conseguenti ripercussioni economiche sia dirette (mancati introiti) che indirette (crescente interdipendenza dai servizi di operatori esteri).
Nel complesso, alla luce degli importanti investimenti già effettuati dagli operatori tlc e della strategicità della tecnologia 5G nel contesto economico e politico, appare importante e auspicabile che, pur mantenendo delle peculiarità a livello nazionale, si cerchi di armonizzare il più possibile la normativa a livello europeo, introducendo specifiche certificazioni e procedure quanto più standardizzate e snelle, in modo da favorire, da un lato, il rapido roll-out di reti che siano sicure e, dall'altro, di traguardare lo sviluppo dell'economia nazionale e dell'intero sistema-Paese.
Soffermando ora l'attenzione sul contesto nazionale, il decreto Brexit ha esteso l'ambito applicativo dei poteri speciali alle reti di telecomunicazione elettronica a banda larga con tecnologia 5G prevedendo l'applicazione del meccanismo di tutela dello Stato non solo nei casi di acquisizioni di partecipazioni

azionarie, ma anche in quello di forniture di materiali e servizi. In tal senso è stato previsto l'obbligo di notifica ai fini dell'esercizio del potere di veto o dell'imposizione di specifiche prescrizioni o condizioni, in relazione a contratti o accordi aventi ad oggetto l'acquisto di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti 5G, ovvero l'acquisizione di componenti ad alta intensità tecnologica funzionali alla predetta realizzazione o gestione che vedano coinvolti soggetti esterni all'Unione europea. Il **decreto 64 dell'11 luglio 2019** – che tuttavia il precedente Esecutivo, prima di cadere a seguito della crisi intervenuta nel mese di agosto, ha deciso di non convertire in legge – aveva valorizzato fortemente il ruolo del Governo al quale veniva attribuito il potere di influenzare fortemente lo sviluppo delle reti 5G. Si tratta di un potere estremamente forte che il Governo Conte 2 ha deciso di esercitare prima che la disciplina decadesse e le operazioni notificate non potessero più essere vagliate (essendo il termine "lungo" previsto dal decreto venuto meno).

Premesso che la disciplina è decaduta lo scorso 9 settembre, a seguito della mancata conversione del suddetto decreto, non può non segnalarsi, proprio nella logica di avviare una riflessione su eventuali ulteriori interventi normativi in materia, come a livello generale il quadro normativo configurato desti **alcune perplessità** relative, innanzitutto, alla tipologia dello strumento utilizzato: se infatti il golden power risulta particolarmente adatto al trasferimento di pacchetti azionari e, dunque, a questioni su cui il feedback è binario (concedere o meno l'acquisto in un dato momento), di più difficile applicazione risulta il caso di un procedimento di verifica degli apparati che di fatto è dilatato nel tempo. In questo senso, sembrerebbe preferibile un meccanismo come la certificazione, che non si applica a un singolo momento temporale, dietro notifica, ma continuativamente, da parte di un ente certificatore e attraverso procedure che siano pragmatiche e allo stesso tempo neutrali rispetto agli elementi competitivi, in modo da garantire la rapidità di esecuzione così come l'apertura e l'efficienza del mercato.

La disciplina del golden power in relazione alle reti 5G appare particolarmente pervasiva andando a incidere anche su forniture di materiali e servizi ogniqualvolta queste coinvolgano soggetti esterni all'Ue. Premessa la necessità, in termini generali, di approfondire la riflessione circa le conseguenze che inevitabilmente si ricollegano all'introduzione di strumenti di direzione delle dinamiche di mercato, considerati gli enormi investimenti da mettere in campo per lo sviluppo dei servizi e delle reti 5G e l'importanza, anche in un'ottica pro-consumatore, di assicurare adeguati livelli di concorrenza nel mercato, è fondamentale che tale potere sia esercitato in maniera proporzionata e secondo modalità improntate alla massima trasparenza per contemperare l'esigenza di garantire la **sicurezza nazionale**, con la necessità di preservare e, se possibile, rafforzare, la **capacità del sistema Paese di attrarre investimenti stranieri** e conservare – ed eventualmente anche incrementare – il **vantaggio finora accumulato, nel contesto europeo,** nello sviluppo del 5G rispetto agli altri Stati membri.

Quanto all'ambito applicativo, date le considerazioni svolte nei precedenti paragrafi sulle questioni di sicurezza inerenti il 5G, non può non suscitare qualche interrogativo la scelta, evidentemente riconducibile a considerazioni di carattere geo-politico, di circoscrivere l'esercizio di poteri speciali di controllo unicamente alle ipotesi di accordi che coinvolgano soggetti extra-Ue. Tale scelta, invero, rischia di non risultare efficace in termini di sicurezza non essendo a priori escludibile una minaccia ad opera

delle altre imprese (o di loro fornitori/clienti), tenendo anche conto che molti dei principali player operanti a vario titolo nell'ampia filiera, a partire dagli operatori tlc, sono partecipati o addirittura filiali di soggetti basati al di fuori dell'Unione europea.
Anche la scelta di allungare i termini, prevista dal decreto legge non convertito, entro i quali il Governo doveva decidere se esercitare – e in che modo – i poteri speciali, desta qualche perplessità. Infatti, se da una parte la disponibilità di un maggior arco temporale dovrebbe consentire una maggiore ponderazione e valutazione da parte dell'Esecutivo chiamato a pronunciarsi in merito a una determinata operazione, dall'altra rischia di frenare (tenendo conto anche delle possibili proroghe) quella dinamicità imprenditoriale assolutamente imprescindibile nella realizzazione e nel lancio delle reti 5G.
È chiaro che la proliferazione delle procedure e l'allungamento delle tempistiche per le verifiche possano ostacolare l'implementazione delle nuove reti da parte degli operatori che hanno investito somme molto ingenti per aggiudicarsi i diritti d'uso delle frequenze destinate al 5G e disincentivare ancora una volta le imprese straniere a investire in Italia ritardando così il godimento, da parte dell'intero sistema Paese, dei benefici socio-economici connessi all'implementazione del 5G.
Alla luce delle considerazioni svolte, appare dunque opportuna e condivisibile la decisione del Governo di non alimentare il procedimento di conversione del decreto legge sopra descritto e di approfondire la riflessione sui tanti profili di importante rilievo. Infatti, se tutti condividiamo che le reti 5G rappresentano uno dei principali volani dello sviluppo futuro del Paese, ci pare allora indispensabile tenere nella dovuta considerazione gli interessi e le prerogative di tutti gli stakeholder nell'ottica di individuare il **migliore bilanciamento possibile delle due esigenze compresenti ma non necessariamente confliggenti**: tutelare efficacemente la sicurezza nazionale e assicurare il rapido sviluppo delle reti 5G in un ecosistema investment-friendly.
In un contesto a così elevata complessità attenta riflessione merita, infine, lo schema di decreto legge licenziato dal Consiglio dei Ministri che è andato a sostituire il disegno di legge approvato il 19 luglio scorso dal precedente Governo. Premesso che, a livello generale, sarebbe forse utile, prima di procedere all'adozione di ulteriori atti normativi, riflettere sull'opportunità, anche in un'ottica di certezza del diritto e maggior semplificazione del quadro normativo, di far confluire in un unico testo tutte le norme che allo stato disciplinano il tema della sicurezza, non si può non rilevare che se tale decreto, da un lato, ha il merito di delineare un quadro piuttosto snello e di non introdurre alcuna forma di discriminazione o disincentivazione in base alla nazionalità dei vendor, dall'altro, solleva diverse preoccupazioni e perplessità. In particolare, il decreto non procede all'individuazione di standard di sicurezza minimi e, con riguardo alle reti 5G, consente di rimettere mano a contratti già autorizzati con decreti della Presidenza del Consiglio nell'esercizio del golden power entro 60 giorni dall'entrata in vigore di un regolamento di cui si prevede l'adozione entro 10 mesi dall'entrata in vigore della legge di conversione del decreto stesso e, dunque, con tempi piuttosto differiti, rischiando di instaurare un clima di generale incertezza nocivo per l'attrattività del Paese, gli investimenti e lo sviluppo del 5G.
In tale ottica, considerata l'importanza di non perdere il vantaggio finora accumulato dall'Italia nello sviluppo del 5G, non può non condividersi la scelta del Governo di ridurre, come evidenziato nel corso dell'analisi che precede, i termini per l'adozione del DPCM e del regolamento con cui individuare i

soggetti rientranti nel perimetro e disciplinare termini e procedure, con l'auspicio che i diversi iter di adozione degli stessi non subiscano rallentamenti e sia presto garantita la piena operatività del CVCN.