IT 2022

03

Relazione speciale

L'introduzione del 5G nell'UE:

vi sono ritardi nel dispiegamento delle reti e le questioni di sicurezza rimangono irrisolte

CURIA RATIONUM

CORTE
DEI CONTI
EUROPEA

Indice

Sintesi

I La “quinta generazione” dei sistemi di telecomunicazione, detta “5G”, è un nuovo standard globale per le comunicazioni senza fili (*wireless*) che offre capacità e velocità di trasmissione dei dati molto maggiori. I servizi 5G sono essenziali per un’ampia gamma di applicazioni innovative che hanno il potenziale per trasformare molti settori delle nostre economie e migliorare la vita quotidiana dei cittadini. Il 5G è quindi di importanza strategica per l’intero mercato unico.

II Nel “Piano d’azione per il 5G” del 2016, la Commissione ha enunciato l’obiettivo di assicurare la copertura ininterrotta, con sistemi 5G, delle aree urbane e dei principali assi di trasporto entro il 2025. Nel marzo 2021, ha esteso detto obiettivo: tutte le zone abitate dovrebbero avere una copertura 5G entro il 2030.

III Il 5G può potenzialmente liberare molte opportunità di crescita, ma comporta alcuni rischi. Nella raccomandazione del 2019 sulla cibersicurezza delle reti 5G, la Commissione ha avvertito che “[p]oiché molti servizi essenziali dipendono dalle reti 5G, le conseguenze di malfunzionamenti sistemici e diffusi sarebbero particolarmente gravi”. Inoltre, data la natura transfrontaliera delle minacce implicate, qualsiasi vulnerabilità significativa o incidente di cibersicurezza in uno Stato membro si ripercuoterebbe su tutta l’UE. Uno degli esiti della raccomandazione della Commissione è stato il “pacchetto di strumenti dell’UE sulla cibersicurezza del 5G”, di seguito “pacchetto di strumenti”, adottato nel gennaio 2020.

IV Nell’UE, il costo totale del dispiegamento del 5G potrebbe raggiungere i 400 miliardi di euro. Nel periodo 2014-2020, l’UE ha fornito finanziamenti per oltre 4 miliardi di euro per progetti relativi al 5G.

V La Corte ha verificato se la Commissione abbia sostenuto in modo efficace gli Stati membri nel conseguimento degli obiettivi dell’UE per l’introduzione delle rispettive reti 5G e nella definizione di una risposta concertata alle preoccupazioni circa la sicurezza del 5G. Gli auditor della Corte hanno valutato aspetti relativi sia all’attuazione delle reti 5G, per la quale il 2020 ha rappresentato un anno cruciale, sia alla loro sicurezza. La finalità della presente relazione è fornire contributi e raccomandazioni per il dispiegamento nei tempi previsti di reti 5G sicure in tutti i paesi dell’UE. L’audit della Corte è stato incentrato sulla Commissione, ma sono stati esaminati anche il ruolo delle amministrazioni nazionali e di altri attori.

VI Dall'audit è emerso che vi sono ritardi nel dispiegamento delle reti 5G degli Stati membri. A fine 2020, 23 Stati membri avevano già varato servizi commerciali 5G e raggiunto l'obiettivo intermedio di aver almeno una grande città con accesso al 5G. Tuttavia, non tutti gli Stati membri fanno riferimento agli obiettivi dell'UE per il 2025 e il 2030 nelle rispettive strategie nazionali in materia di 5G o nei rispettivi piani per la banda larga. Per di più, in numerosi paesi il codice europeo per le comunicazioni elettroniche non è ancora stato trasposto nel diritto nazionale e l'assegnazione dello spettro radio per il 5G ha subìto ritardi. Questi ritardi nell'assegnazione dello spettro 5G possono essere ascritti a diverse ragioni: una debole domanda da parte dei gestori delle reti mobili; problematiche di coordinamento transfrontaliero con paesi non-UE lungo i confini orientali dell'UE; l'impatto della COVID-19 sui calendari delle aste e l'incertezza su come affrontare le questioni di sicurezza. Il ritardo degli Stati membri nell'attuazione del 5G è tale da porre a rischio il conseguimento degli obiettivi dell'UE. La Commissione ha aiutato gli Stati membri ad attuare il piano d'azione per il 5G del 2016 tramite strumenti giuridici vincolanti, *soft law* e orientamenti, nonché finanziando la ricerca in materia di 5G. Tuttavia, non ha definito in modo chiaro la qualità attesa dei servizi 5G.

VII Il "pacchetto di strumenti dell'UE sulla cibersicurezza del 5G" specifica una serie di misure strategiche, tecniche e di sostegno volte ad affrontare le minacce alla sicurezza delle reti 5G ed identifica gli attori pertinenti per ciascuna di dette misure. Molte misure affrontano la questione dei fornitori di apparecchiature 5G ad alto rischio. Questo pacchetto di strumenti è stato approvato dalla Commissione e dal Consiglio europeo. I criteri definiti nel pacchetto offrono un quadro operativo utile per valutare il profilo di rischio dei fornitori in modo coordinato in tutti gli Stati membri. Allo stesso tempo, l'effettuazione di detta valutazione rimane una responsabilità nazionale. Il pacchetto è stato adottato in una delle prime fasi del dispiegamento del 5G, ma alcuni gestori di reti mobili avevano già selezionato i propri fornitori. Dall'adozione del pacchetto, sono stati compiuti progressi per rafforzare la sicurezza delle reti 5G: la maggioranza degli Stati membri applica o è sul punto di applicare restrizioni nei confronti dei fornitori ad alto rischio. Nei prossimi anni, la normativa sulla sicurezza del 5G introdotta dagli Stati membri sulla base del pacchetto potrebbe portare ad approcci più convergenti nei confronti dei fornitori ad alto rischio di apparecchiature 5G. Tuttavia, poiché nessuna delle misure proposte è giuridicamente vincolante, la Commissione non ha il potere di farle rispettare. Pertanto, permane il rischio che il pacchetto di strumenti, di per sé, non riesca a garantire che gli Stati membri affrontino gli aspetti di sicurezza delle reti in modo concertato.

VIII La Commissione ha iniziato ad affrontare la questione delle sovvenzioni di paesi stranieri ai fornitori di apparecchiature 5G, con possibili implicazioni per la sicurezza. La Commissione non dispone di sufficienti informazioni circa il trattamento, da parte degli Stati membri, di potenziali costi di sostituzione che potrebbero sorgere se i gestori di reti mobili fossero obbligati a rimuovere le apparecchiature dei fornitori ad alto rischio dalle reti dell'UE senza un periodo di transizione.

IX La Corte raccomanda alla Commissione di:

- promuovere un dispiegamento bilanciato e tempestivo delle reti 5G nell'UE;
- promuovere tra gli Stati membri un approccio concertato alla sicurezza del 5G;
- monitorare gli approcci degli Stati membri in materia di sicurezza del 5G e valutare l'impatto delle divergenze sull'efficace funzionamento del mercato unico.

Introduzione

Natura e importanza del 5G

01 La "quinta generazione" dei sistemi di telecomunicazione, detta "5G", è un nuovo standard globale per le comunicazioni senza fili (*wireless*). Rispetto alle reti 3G e 4G, offre capacità e velocità di trasmissione dei dati molto maggiori. Il 5G include alcune componenti di rete basate su precedenti generazioni di tecnologie di comunicazione mobili e senza fili, ma non costituisce un'evoluzione incrementale di dette reti. Fornisce connettività universale a banda larga superveloce e a bassa latenza per i singoli utenti e per gli oggetti connessi.

02 Il 5G renderà possibile la connessione nell'"Internet delle cose" di un maggior numero di dispositivi, mai raggiunto prima. A fine 2018, si stima vi fossero 22 miliardi di dispositivi connessi in uso nel mondo. Si prevede che tale cifra aumenterà fino a circa 50 miliardi entro il 2030[1], creando un'enorme rete di dispositivi interconnessi includenti tutto, dagli smartphone agli apparecchi da cucina. Si prevede che entro il 2030 il consumo mondiale di dati balzerà dai 12 exabyte al mese di traffico dati su reti mobili del 2017[2] a oltre 5 000 exabyte[3].

03 I servizi 5G sono essenziali per un'ampia gamma di applicazioni innovative che hanno il potenziale per trasformare molti settori dell'economia dell'UE e migliorare la vita quotidiana dei cittadini (cfr. ***figura 1***). Uno studio condotto per conto della Commissione nel 2017 ha indicato che i benefici dell'introduzione del 5G per quattro importanti settori strategici industriali (automobili, sanità, trasporti e energia) potrebbero ammontare a ben 113 miliardi di euro all'anno[4]. In detto studio si è inoltre previsto che l'attuazione del 5G potrebbe creare 2,3 milioni di posti di lavoro negli Stati membri. In uno studio del 2021, si stima che, tra il 2021 e il 2025, il 5G aggiungerà fino a 1 000 miliardi di euro al prodotto interno lordo (PIL) europeo per il periodo, con il

---

[1] Statista, *Number of internet of things (IoT) connected devices worldwide in 2018, 2025 and 2030*.

[2] *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2017-2022*, febbraio 2019.

[3] ITU-R, *IMT traffic estimates for the years 2020 to 2030*.

[4] *Identification and quantification of key socio-economic data to support strategic planning for the introduction of 5G in Europe*, febbraio 2017.

potenziale di creare o trasformare fino a 20 milioni di posti di lavoro in tutti i settori dell'economia[5].

Figura 1 – La tecnologia 5G interesserà tutti gli aspetti della nostra vita

Fonte: Commissione europea.

Preoccupazioni circa la sicurezza

04 Il 5G può potenzialmente liberare molte opportunità di crescita, ma comporta alcuni rischi (cfr. l'***allegato I*** dove si illustrano le principali opportunità e i principali rischi del 5G). Uno di tali rischi è quello delle minacce alla sicurezza. I sistemi di telecomunicazione sono sempre stati a rischio di ciberattacchi (cfr. ***allegato II***)[6]. Le problematiche di sicurezza sono particolarmente preoccupanti per il 5G, perché quest'ultimo, a causa della natura della sua tecnologia ed in particolare a causa della sua dipendenza dal software, offre una superficie di attacco più ampia rispetto ai sistemi di telecomunicazione 3G o 4G[7].

05 Poiché si prevede che le reti 5G diventino la spina dorsale di un'ampia gamma di servizi e applicazioni, la disponibilità di dette reti diverrà una importante sfida di sicurezza nazionale e dell'UE. Se degli hacker penetrassero una rete 5G, potrebbero comprometterne le funzioni fondamentali per interrompere i servizi o assumere il

---

[5] Accenture Strategy, *The Impact of 5G on the European Economy*, febbraio 2021.

[6] Cfr. Corte dei conti europea, Analisi 02/2019,"Le sfide insite in un'efficace politica dell'UE in materia di cibersicurezza (documento di riflessione)"; Comitato di contatto delle istituzioni superiori di controllo dell'UE, compendio di audit, "La cibersicurezza nell'UE e nei suoi Stati membri", 2020; e Servizio Ricerca del Parlamento europeo, *European Science-Media hub*.

[7] Gruppo di cooperazione NIS, *EU coordinated risk assessment of the cybersecurity of 5G networks*, 9.10.2019. punto 3.4.

controllo di infrastrutture cruciali (ad esempio, le reti elettriche), che nell'UE hanno spesso dimensione transfrontaliera. Secondo quanto stimato in alcuni studi, l'impatto economico della cibercriminalità potrebbe ammontare fino a 5 000 miliardi di euro all'anno in tutto il mondo, ossia oltre il 6 % del PIL mondiale nel 2020[8].

06 Un'altra problematica di sicurezza del 5G è il ruolo cruciale svolto da un numero limitato di fornitori nella costruzione e nella gestione delle reti 5G. Ciò accresce l'esposizione a potenziali interruzioni dell'approvvigionamento quando si dipende da un unico fornitore, specie se detto fornitore presenta un alto grado di rischio, come ad esempio essere soggetto alle ingerenze di un paese non-UE. Nel 2019 il gruppo di cooperazione per le reti e i sistemi informativi (*Network and Information System* – NIS), composto da rappresentanti degli Stati membri e di organismi dell'UE, ha evidenziato il rischio che "entità statali ostili" ottengano un facile punto di accesso a una rete 5G attraverso un accesso privilegiato, esercitando pressioni su un fornitore oppure invocando obblighi giuridici nazionali[9] (cfr. ***riquadro 1***). È in questo contesto che l'UE ha iniziato a sviluppare iniziative nel campo della sicurezza del 5G.

Riquadro 1

Preoccupazioni concernenti la sicurezza nel contesto della cooperazione tra UE e Cina in materia di 5G

- Nel 2015, l'UE ha firmato una dichiarazione congiunta con la Cina sulla cooperazione strategica in materia di 5G, impegnandosi a favore della reciprocità e dell'apertura in termini di accesso ai finanziamenti per la ricerca sulle reti 5G e di accesso al mercato delle reti 5G[10].

---

[8] Forum economico mondiale, *Wild Wide Web – Conseguences of Digital Fragmentation*, 2021.

[9] Gruppo di cooperazione NIS, *EU coordinated risk assessment of the cybersecurity of 5G networks*, 9.10.2019.

[10] Cfr. https://ec.europa.eu/commission/presscorner/detail/it/IP_15_5715

- Nel 2017, la Cina ha adottato una legge sull'intelligence nazionale che dispone l'obbligo, per tutte le organizzazioni e i cittadini cinesi, di collaborare ai fini dell'intelligence nazionale, con tutele concernenti la segretezza[11]. In risposta, nel 2018 gli Stati Uniti hanno adottato misure per limitare il ruolo di numerose imprese cinesi, tra cui Huawei, un importantissimo fornitore di apparecchiature 5G.

Nel marzo 2019, anche il Parlamento europeo si è detto preoccupato che i fornitori cinesi di apparecchiature 5G possano rappresentare un rischio per la sicurezza dell'UE a causa delle leggi del loro paese di origine.

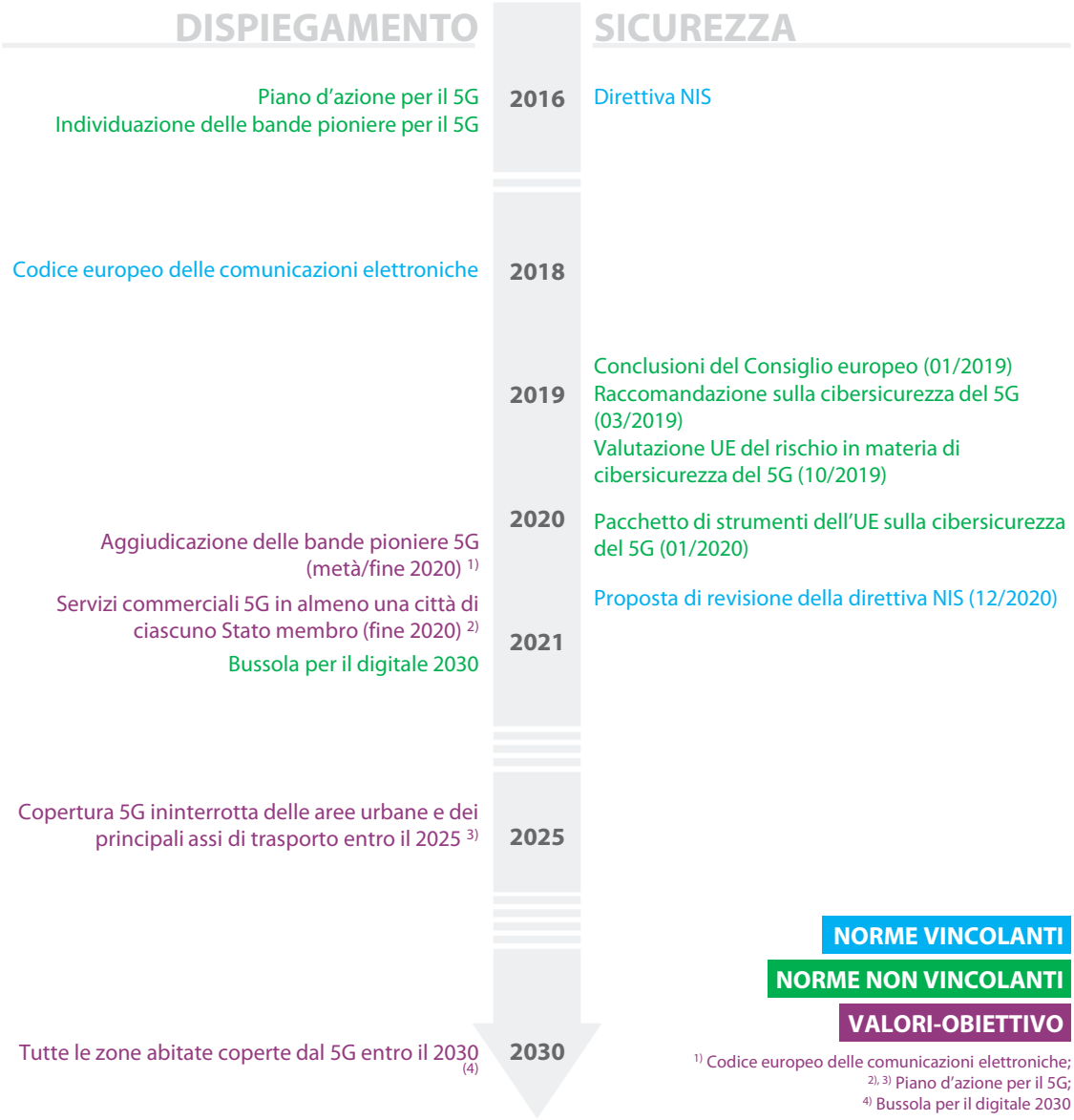
07 Anche la riservatezza e la privacy sono potenzialmente minacciate, in quanto gli operatori delle telecomunicazioni spesso esternalizzano i loro dati a centri dati. Vi è il rischio che tali dati siano conservati in apparecchiature dei fornitori di apparecchiature 5G, situate in paesi non-UE aventi livelli diversi di protezione giuridica e dei dati rispetto a quanto avviene nell'UE.

Iniziative in materia di 5G adottate a livello UE

08 Il quadro d'intervento relativo al 5G e alla sicurezza del 5G è composto sia da *hard law*, ossia atti normativi giuridicamente vincolanti ed aventi forza esecutiva (ad esempio, regolamenti), sia da *soft law*, ossia norme non vincolanti (ad esempio, comunicazioni della Commissione). L'***allegato III*** presenta il quadro giuridico e d'intervento. La ***figura 2*** illustra i principali documenti strategici, insieme ai valori-obiettivo principali.

[11] Cfr. risoluzione del Parlamento europeo del 12 marzo 2019; Legge sull'intelligence nazionale della Repubblica popolare cinese, articolo 14. Cfr. anche una traduzione in inglese di quest'ultima all'indirizzo: https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/

Figura 2 – Principali documenti strategici e valori-obiettivo relativi al dispiegamento e alla sicurezza del 5G



Fonte: Corte dei conti europea.

Ruoli e responsabilità

09 Se, da un lato, i gestori di reti mobili sono responsabili dell'introduzione sicura del 5G, utilizzando apparecchiature provenienti dai fornitori di tecnologie, e gli Stati membri sono responsabili della sicurezza nazionale, dall'altro la sicurezza delle reti 5G è una questione di importanza strategica per l'intero mercato unico e la sovranità tecnologica dell'UE[12]. Di conseguenza, per quanto riguarda gli aspetti tecnici e di

[12] Cfr. https://ec.europa.eu/commission/presscorner/detail/it/IP_20_12

sicurezza delle reti 5G, la Commissione e le agenzie dell'UE sostengono e coordinano le azioni degli Stati membri.

10 Nella ***tabella 1*** vengono illustrati con maggiori dettagli i principali ruoli e le principali responsabilità in materia di reti 5G.

Tabella 1 –Ruoli e responsabilità

	Commissione europea e Agenzie dell'UE	Autorità degli Stati membri	Gestori di reti mobili e fornitori di sistemi 5G
Allocazione e assegnazione di bande pioniere per il 5G		✓	
Definizione della politica dell'UE in materia di 5G	✓	✓	
Dispiegamento di reti 5G			✓
Investimenti e finanziamenti	✓	✓	✓
Sicurezza nazionale		✓	
Sicurezza delle reti 5G		✓	✓
Sostegno e coordinamento delle azioni degli Stati membri	✓		

Fonte: Corte dei conti europea.

Costi del dispiegamento del 5G e relativo sostegno finanziario dell'UE

Il costo totale del dispiegamento del 5G in tutti gli Stati membri potrebbe raggiungere i 400 miliardi di euro

11 Nel 2021, il costo totale del dispiegamento del 5G in tutti gli Stati membri dell'UE fino al 2025 è stato stimato pari ad una cifra compresa tra i 281 e i 391 miliardi di euro, equamente suddivisi tra costruzione di nuove infrastrutture 5G e potenziamento delle infrastrutture fisse fino a velocità dell'ordine di gigabit[13]. Il grosso di questi investimenti deve essere finanziato dai gestori di reti mobili.

[13] Stime della Commissione basate su dati della BEI, Analysys, GSMA e annunci societari, nonché su ETNO – European Telecommunications, *Connectivity & Beyond: How Telcos Can Accelerate a Digital Future for All*, marzo 2021.

Nel periodo 2014-2020, l'UE ha sostenuto lo sviluppo del 5G con oltre 4 miliardi di euro

12 Nel periodo 2014-2020, l'UE ha sostenuto lo sviluppo del 5G con oltre 4 miliardi di euro, sia direttamente tramite il bilancio dell'UE che tramite il finanziamento della Banca europea per gli investimenti (BEI). Il bilancio dell'UE ha finanziato progetti relativi esclusivamente alla ricerca, mentre la BEI ha sostenuto sia la ricerca che il dispiegamento.

13 La BEI è stata il principale fornitore di finanziamenti dell'UE per progetti relativi al 5G. Ad agosto 2021, la BEI aveva concesso prestiti per un totale di 2,5 miliardi di euro per nove progetti relativi al 5G in cinque Stati membri[14]. Inoltre, erano stati messi a disposizione circa 1,9 miliardi di euro dal bilancio dell'UE per il periodo 2014-2020. La ***tabella 2*** riassume le principali fonti di sostegno finanziario dell'UE per il 5G.

Tabella 2 – Finanziamenti dell'UE per il 5G (2014-2020)

Finanziamento dell'UE	Importo
BEI	2 485 miliardi di euro[1]
Fondo europeo per gli investimenti strategici (FEIS)	1 miliardo di euro[2]
Orizzonte 2020	755 milioni di euro[3]
FESR	Almeno 147 milioni di euro[4]

1) Elenco dei progetti finanziati dalla BEI.
2) Elenco dei progetti finanziati dal FEIS.
3) Portale di Orizzonte 2020.
4) *Dataset of projects co-funded by the ERDF during the multi-annual financial framework 2014-2020* (Banca dati dei progetti cofinanziati dal FESR durante il quadro finanziario pluriennale 2014-2020).

Fonte: Corte dei conti europea.

14 Il FEIS (gestito dalla BEI) ha sostenuto due progetti volti a conseguire un'installazione di celle più densa e a sostenere la standardizzazione. Il costo totale di investimento per questi progetti è stato di 3,9 miliardi di euro, comprendente 1 miliardi di euro di finanziamenti del FEIS (cfr. ***allegato IV***).

15 Dal 2014, la Commissione ha anche cofinanziato direttamente più di 100 progetti 5G mediante i fondi di Orizzonte 2020 e, in misura minore, del FESR. L'***allegato V*** illustra esempi di progetti di questo tipo.

---

[14] Elenco dei progetti finanziati dalla BEI.

Il dispositivo per la ripresa e la resilienza fornirà finanziamenti dell'UE aggiuntivi per il dispiegamento del 5G nei prossimi anni

16 Il dispositivo per la ripresa e la resilienza fornirà una fonte supplementare di finanziamento per il dispiegamento del 5G nei prossimi anni. Al settembre 2021, 16 Stati membri prevedevano di finanziare il dispiegamento del 5G attraverso tale dispositivo e 10 avevano deciso di non farlo. Per il rimanente Stato membro non erano ancora disponibili informazioni.

Estensione e approccio dell'audit

17 Tramite il presente audit, la Corte ha verificato se la Commissione stia aiutando in modo efficace gli Stati membri a:

- raggiungere gli obiettivi dell'UE per il 2025 e il 2030 relativi al dispiegamento e all'introduzione delle rispettive reti 5G;
- affrontare in modo concertato le preoccupazioni circa la sicurezza del 5G.

Per entrambi gli ambiti, la Corte ha preso in considerazione anche le misure e le attività degli Stati membri.

18 Per "sicurezza del 5G" si intende qui la cibersicurezza e la sicurezza dell'hardware/software. Gli auditor della Corte hanno esaminato sia la sicurezza che l'attuazione delle reti 5G, per le quali il 2020 ha rappresentato un anno cruciale (cfr. ***figura 2***). Tramite la presente relazione, la Corte mira a fornire contributi e raccomandazioni per il dispiegamento nei tempi previsti di reti 5G sicure nell'UE.

19 L'audit ha riguardato il periodo compreso tra il 2016 e il maggio 2021. Per quanto possibile, sono state incluse ulteriori informazioni aggiornate. Come parte delle attività di audit, gli auditor della Corte hanno:

- esaminato la normativa UE, le iniziative della Commissione e altra documentazione pertinente;
- tenuto colloqui con rappresentanti della Commissione, della BEI, dell'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC), dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA), delle associazioni di telecomunicazione, dei gestori di reti mobili, dei fornitori di apparecchiature 5G, di organizzazioni internazionali e con esperti sul campo per raccogliere informazioni, nonché con le autorità di Finlandia, Germania, Polonia e Spagna. Detti Stati membri sono stati scelti sulla base di criteri quali l'importo dei fondi UE destinati ai progetti 5G, lo stato del dispiegamento e l'equilibrio geografico;
- effettuato un'indagine presso tutte le 27 autorità nazionali di regolamentazione delle telecomunicazioni dell'UE, per ottenere una prospettiva più generale delle sfide relative al 5G negli Stati membri;
- analizzato 10 progetti cofinanziati dall'UE (FEIS, FESR e Orizzonte 2020) relativi al 5G, scelti a fini illustrativi.

20 Gli auditor della Corte si sono inoltre basati sulla recente analisi della Corte sulla risposta dell'UE alla strategia cinese di investimenti guidati dallo Stato[15], nonché su altre relazioni, ad esempio quella sulla banda larga[16], sull'iniziativa di digitalizzazione dell'industria europea[17] e sull'analisi della politica dell'UE in materia di cibersicurezza[18].

---

[15] Corte dei conti europea, Analisi n. 03/2020, "La risposta dell'UE alla strategia cinese di investimenti guidati dallo Stato".

[16] Relazione speciale n. 12/2018, "La banda larga negli Stati membri dell'UE: nonostante i progressi, non tutti i target di Europa 2020 saranno raggiunti".

[17] Relazione speciale 19/2020, "Digitalizzazione dell'industria europea: iniziativa ambiziosa il cui successo dipende dal costante impegno dell'UE, delle amministrazioni e delle imprese".

[18] Analisi n. 02/2019, "Le sfide insite in un'efficace politica dell'UE in materia di cibersicurezza (Documento di riflessione)".

Osservazioni

I ritardi nel dispiegamento delle reti 5G stanno mettendo a rischio il raggiungimento degli obiettivi dell'UE per il 2025 e per il 2030

21 Per quanto riguarda il tempestivo dispiegamento delle reti 5G, la Corte ha verificato se:

- gli Stati membri siano sulla buona strada per quanto riguarda il dispiegamento del 5G;
- la Commissione abbia fornito adeguato sostegno agli Stati membri;
- gli Stati membri abbiano rimosso i principali ostacoli alla rapida introduzione delle reti 5G.

Gli Stati membri sono in ritardo nell'attuazione del 5G

Nel piano d'azione per il 5G del 2016, la Commissione ha fissato termini ultimi per il dispiegamento delle reti 5G

22 Nel piano d'azione per il 5G del 2016, la Commissione ha proposto termini ultimi per il dispiegamento di reti 5G nell'UE: gli Stati membri dovevano varare le prime reti 5G entro la fine del 2018, servizi 5G pienamente commerciali in almeno una grande città entro la fine del 2020 e garantire una copertura 5G ininterrotta delle aree urbane e dei principali assi di trasporto entro il 2025.

23 Nel marzo 2021 la Commissione ha aggiunto un ulteriore termine ultimo: la copertura 5G di tutte le zone abitate entro il 2030[19].

Prima della fine del 2020, 23 Stati membri avevano varato servizi commerciali 5G

24 A fine 2020, 23 Stati membri avevano raggiunto l'obiettivo di almeno una grande città dotata di accesso a servizi 5G. Solo Cipro, la Lituania, Malta e il Portogallo non

[19] Commissione europea, Bussola per il digitale 2030: il modello europeo per il decennio digitale, COM(2021) 118 final.

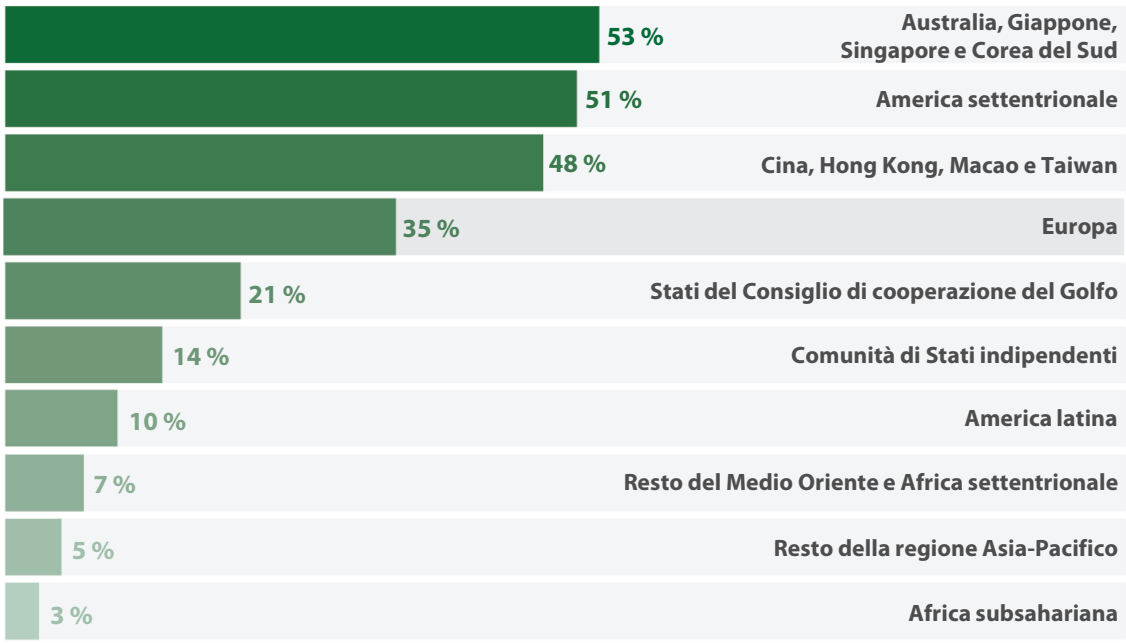
erano riusciti a raggiungere questo obiettivo. A fine ottobre 2021, solo la Lituania e il Portogallo non disponevano ancora di servizi 5G in nessuna delle loro città.

Vi è il rischio che la maggior parte degli Stati membri non rispetti il termine ultimo del 2025 e quello del 2030

25 Secondo un recente studio della Commissione, è probabile che solo 11 Stati membri conseguano una copertura 5G ininterrotta di tutte le loro aree urbane e dei loro principali assi di trasporto terrestre entro il 2025[20]. Per i restanti 16 Stati membri, la Commissione ritiene che la probabilità di conseguire tale obiettivo sia media (Austria, Cechia, Estonia, Germania, Irlanda, Polonia, Lituania e Slovenia) o bassa (Belgio, Bulgaria, Croazia, Cipro e Grecia).

26 Nel 2021, l'organizzazione di settore *Global System for Mobile Communications Association* (GSMA) ha osservato che nell'UE il dispiegamento del 5G sta procedendo a un ritmo diverso rispetto ad altre parti del mondo. Ad esempio, secondo le stime, il 51 % di tutte le connessioni mobili in Nord America sarà basato sul 5G entro il 2025, mentre in Europa (che comprende anche paesi non-UE) tale percentuale sarà verosimilmente solo del 35 % (cfr. ***figura 3***).

Figura 3 – Connessioni 5G come quota del totale delle connessioni mobili entro il 2025



Fonte: GSMA, *The Mobile Economy 2021*.

[20] Cfr. *Study on National Broadband Plans in the EU-27*.

27 Al ritmo attuale di dispiegamento vi è il rischio elevato che il termine ultimo del 2025 – e quindi anche quello del 2030 per la copertura di tutte le zone abitate – non venga rispettato dalla maggioranza degli Stati membri. In tale contesto, la Corte ha verificato se la Commissione abbia efficacemente sostenuto gli Stati membri nel conseguire gli obiettivi dell'UE per il 2025 e il 2030 relativi al dispiegamento e alla diffusione delle reti 5G nazionali.

Alcune carenze nel sostegno della Commissione agli Stati membri

La Commissione non ha definito la qualità di servizio attesa delle reti 5G

28 Finora, la Commissione non ha definito la qualità di servizio attesa delle reti 5G, ad esempio in termini di velocità minima e latenza massima. Inoltre, nel piano d'azione del 2016 veniva chiesto agli Stati membri di varare servizi 5G "pienamente commerciali" in Europa entro la fine del 2020, senza tuttavia definire questi concetti relativi alla qualità.

29 La mancanza di chiarezza sulla qualità del servizio attesa genera il rischio che questi termini siano interpretati in modo diverso dagli Stati membri. Gli auditor della Corte hanno rilevato esempi di approcci divergenti al dispiegamento del 5G tra gli Stati membri (cfr. ***riquadro 2***).

Riquadro 2

Esempi di approcci divergenti al dispiegamento del 5G

La velocità e la latenza sono due aspetti essenziali delle prestazioni dei servizi che utilizzano il 5G. Ad esempio, gli interventi chirurgici a distanza o l'automazione industriale tramite 5G necessitano di velocità elevatissima e di bassa latenza. Ciononostante, finora solo due Stati membri (Germania e Grecia) hanno definito requisiti in materia di velocità minima e di latenza massima[21].

Il requisito che vi fosse "almeno una grande città avente accesso ai servizi 5G entro il 2020" è stato interpretato in modo differente dagli Stati membri. Ciò porta ad una situazione per cui una città classificata come "avente accesso ai servizi 5G" conta una copertura che va da poche strade soltanto (come in Lussemburgo) a quasi tutto il territorio cittadino (come ad Helsinki). L'***allegato VI*** fornisce, per alcune città, esempi di copertura.

[21] Cfr. *5G Observatory Quarterly Report 12, Up to June 2021*.

30 Se persiste, questa situazione potrebbe condurre a disuguaglianze per l'accesso e la qualità dei servizi 5G nell'UE (*digital divide*): in una parte dell'UE le persone godrebbero di un migliore accesso e di una migliore qualità del servizio 5G rispetto ad altre parti dell'UE. Questo divario digitale potrebbe anche incidere negativamente sul potenziale di sviluppo economico, in quanto il 5G può rivoluzionare settori quali l'assistenza sanitaria, l'istruzione e la forza lavoro solo se accompagnato da prestazioni sufficienti per il 5G.

31 È inoltre necessario fare chiarezza sulle prestazioni attese delle reti 5G, alla luce dell'iniziativa della Commissione di imporre una maggiore trasparenza circa la qualità del servizio fornito dai gestori di reti mobili per il *roaming*, per la quale la Commissione ha recentemente presentato una proposta legislativa[22].

Le relazioni trimestrali della Commissione sull'introduzione del 5G non sono sempre affidabili

32 La Commissione monitora il livello di dispiegamento del 5G negli Stati membri attraverso l'Osservatorio 5G. Quest'ultimo fornisce trimestralmente informazioni sul dispiegamento del 5G e sulle strategie degli Stati membri in materia di 5G. La Corte ha tuttavia riscontrato che, per due dei quattro paesi esaminati, le informazioni contenute in tali relazioni non erano sempre attendibili. Ad esempio, la relazione trimestrale n. 10, che presenta le informazioni fino alla fine di dicembre 2020, presentava un numero molto inferiore di comuni con 5G in Finlandia rispetto al dato effettivo (40 anziché 70) e non forniva alcuna informazione sul fatto che le aste dello spettro 5G erano state rinviate in Polonia (cfr. paragrafo ***42***).

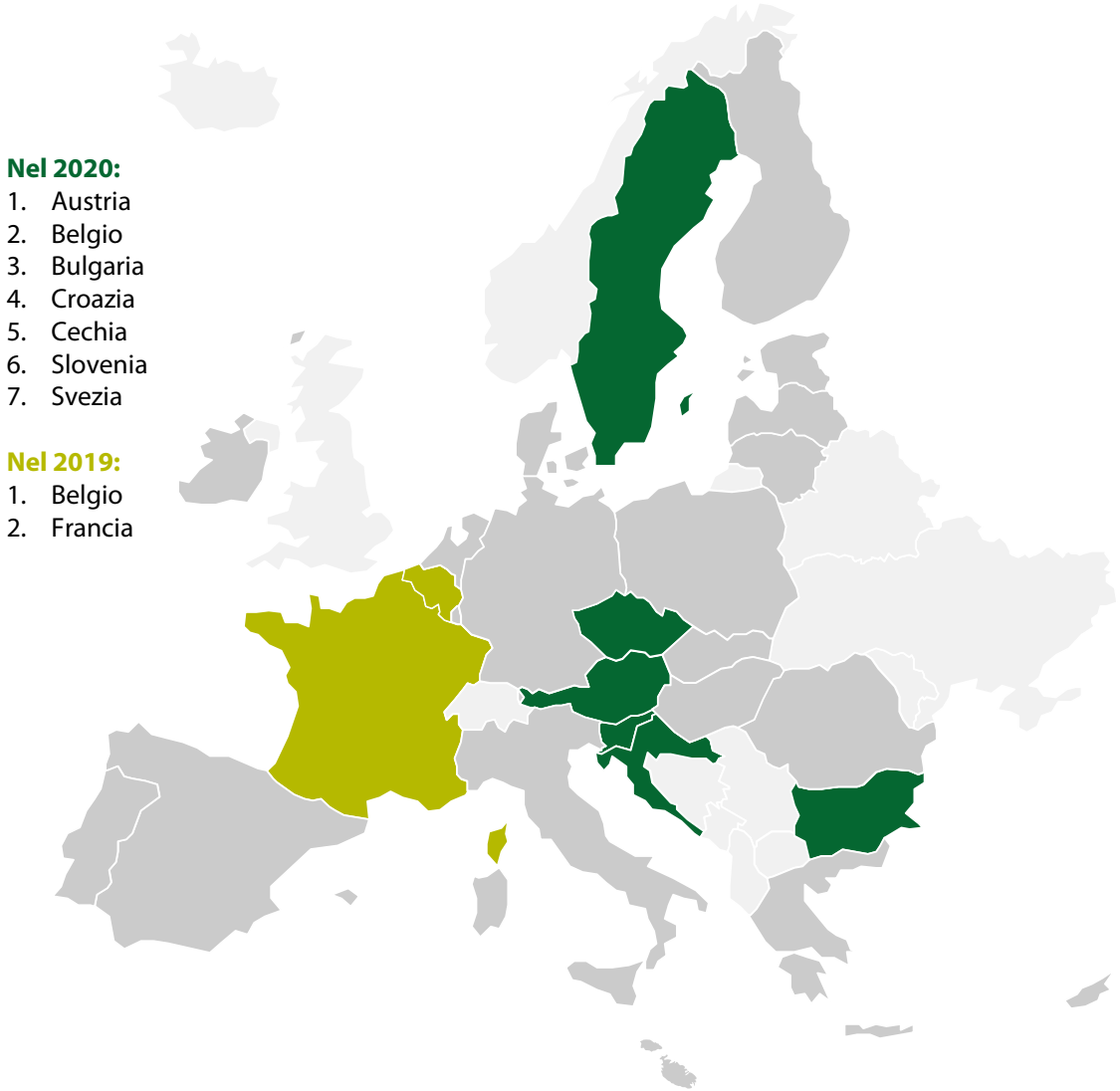
La Commissione si è avvalsa solo di recente del processo del semestre europeo per monitorare i progressi compiuti dagli Stati membri nel dispiegamento delle reti 5G

33 La Corte ha riscontrato che, negli ultimi due anni, la Commissione si è avvalsa maggiormente del processo del semestre europeo per esortare gli Stati membri a compiere progressi nel dispiegamento delle reti 5G. Le raccomandazioni specifiche per paese direttamente pertinenti per il 5G sono aumentate, passando dall'essere indirizzate a due Stati membri nel 2019 a sette nel 2020 (cfr. ***figura 4***).

---

[22] Commissione europea, Proposta di regolamento del Parlamento europeo e del Consiglio relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione (rifusione), COM(2021) 85 final del 24.2.2021.

Figura 4 – Raccomandazioni specifiche per paese in materia di 5G



Fonte: Corte dei conti europea, sulla base delle raccomandazioni specifiche per paese.

Gli Stati membri devono ancora rimuovere i principali ostacoli alla rapida introduzione delle reti 5G

34 Al fine di raggiungere gli obiettivi di dispiegamento del 5G fissati dall'UE per il 2025 e il 2030, gli Stati membri devono realizzare tre importanti elementi fondamentali: uno strategico, ossia garantire che le strategie nazionali per il 5G o i piani nazionali per la banda larga riflettano tali obiettivi[23]; uno legislativo, ossia recepire il codice europeo delle comunicazioni elettroniche del 2018[24]; e uno di carattere commerciale, ossia assegnare lo spettro radio[25]. La ***tabella 3*** fornisce una panoramica dei progressi compiuti dagli Stati membri in relazione a questi tre elementi.

[23] Cfr. Commissione europea, *Study on National Broadband Plans in the EU-27*.

[24] Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio che istituisce il codice europeo delle comunicazioni elettroniche.

[25] Commissione europea, Dispiegamento del 5G sicuro – Attuazione del pacchetto di strumenti dell'UE, COM(2020) 50 final.

Tabella 3 – Situazione relativa agli elementi costitutivi in vista degli obiettivi per il 2025

Stato membro	Piano nazionale per la banda larga in linea con gli obiettivi per il 2025	Recepimento del codice europeo delle comunicazioni elettroniche	Bande pioniere 5G (agosto 2021)			Probabilità di raggiungere l'obiettivo
			700 MHz	3,6 GHz	26 GHz	
Belgio				Uso provvisorio		bassa
Bulgaria		✓		✓		bassa
Cechia	✓	✓	✓	✓		media
Danimarca		✓	✓	✓	✓	alta
Germania	✓	✓	✓	✓	✓	media
Estonia						media
Irlanda				✓		media
Grecia	✓	✓	✓	✓	✓	bassa
Spagna	✓		✓	✓		alta
Francia	✓	✓	✓	✓		alta
Croazia			✓	✓	✓	bassa
Italia			✓	✓	✓	alta
Cipro	✓		✓	✓		bassa
Lituania	✓					media
Lettonia				✓		alta
Lussemburgo			✓	✓		alta
Ungheria	✓	✓	✓	✓		alta
Malta		✓				media
Paesi Bassi	✓		✓			media
Austria	✓	✓	✓	✓		media
Polonia	✓					media
Portogallo				Uso provvisorio		medio-alta
Romania						alta
Slovenia	✓		✓	✓	✓	media
Slovacchia			✓			alta
Finlandia	✓	✓	✓	✓	✓	alta
Svezia	✓		✓	✓		alta

Fonte: Commissione europea, *Study on National Broadband Plans in the EU-27*; Osservatorio 5G e gruppo "Politica dello spettro radio" (RSPG).

Pochi Stati membri hanno incluso nelle loro strategie nazionali per il 5G gli obiettivi di dispiegamento per il 2025 e il 2030

35 Gli Stati membri definiscono la propria politica in materia di 5G attraverso apposite strategie nazionali per il 5G oppure aggiornando gli esistenti piani nazionali per la banda larga. Lo studio della Commissione del 2021 sui piani nazionali per la banda larga[26] ha rilevato che solo 14 Stati membri hanno incluso l'obiettivo dell'UE di "una copertura 5G ininterrotta di tutte le aree urbane e dei principali assi di trasporto terrestre entro il 2025" nelle rispettive strategie nazionali per il 5G o nell'aggiornamento dei piani per la banda larga (cfr. ***tabella 3***). Tale inclusione è fondamentale per sostenere la riuscita attuazione della politica.

La maggior parte degli Stati membri non ha recepito la direttiva che istituisce il codice europeo delle comunicazioni elettroniche entro la fine del 2020

36 Il codice europeo delle comunicazioni elettroniche, che stabilisce i compiti delle autorità nazionali di regolamentazione e fissa i termini ultimi per l'assegnazione delle bande pioniere 5G, avrebbe dovuto essere recepito dagli Stati membri entro il 21 dicembre 2020. A fine febbraio 2021, solo tre Stati membri (Finlandia, Grecia e Ungheria) avevano dichiarato di aver adottato tutte le misure necessarie per il recepimento della direttiva. Di conseguenza, la Commissione ha avviato procedure di infrazione nei confronti dei restanti 24 Stati membri[27].

37 A fine novembre 2021, erano ancora in corso 23 procedure d'infrazione. Per sei Stati membri (Austria, Bulgaria, Cechia, Francia, Germania e Malta) la Commissione si attende di chiudere in tempi rapidi la procedura d'infrazione, mentre per gli altri 17 Stati membri potrebbe dover deferirli alla Corte di Giustizia[28] (cfr. ***tabella 3***).

---

[26] Cfr. *Study on National Broadband Plans in the EU-27*.

[27] Commissione europea, comunicato stampa IP/21/206 del 4.2.2021.

[28] Commissione europea, comunicato stampa IP/21/4612 del 23.9.2021.

Vi sono ritardi nell'assegnazione delle bande pioniere 5G

38 Nel 2016, la Commissione e gli Stati membri hanno individuato tre bande pioniere da utilizzare per i servizi 5G:

- lo spettro di banda a 700 MHz rende più facile per i segnali senza fili penetrare gli edifici e consente ai gestori di fornire una copertura più ampia (centinaia di chilometri quadrati). Tuttavia, la velocità e la latenza della rete 5G sono migliori solo di poco rispetto al 4G (per quanto riguarda la velocità, da 150 a 250 megabit al secondo);
- lo spettro di banda media a 3,6 GHz, che può trasportare quantità significative di dati (fino a 900 megabit al secondo) per distanze significative (in un raggio di diversi km);
- lo spettro di banda alta a 26 GHz, che può fornire velocità elevate, comprese tra 1 e 3 gigabit al secondo su brevi distanze (ossia meno di 2 km), ma che è più sensibile alle interferenze.

39 Gli Stati membri avrebbero dovuto rendere disponibile per l'utilizzo lo spettro radio della banda bassa entro il 30 giugno 2020[29], mentre quelli della banda media ed alta entro il 31 dicembre 2020[30]. Tuttavia, a fine 2020, gli Stati membri avevano assegnato meno del 40 % del totale delle bande pioniere disponibili (cfr. ***tabella 4***):

- la banda dei 700 MHz è stata assegnata in 13 Stati membri;
- la banda dei 3,6 GHz è stata assegnata in 17 Stati membri (due dei quali avevano concesso un uso provvisorio);
- la banda dei 26 GHz è stata assegnata in quattro Stati membri.

A fine ottobre 2021, il tasso di assegnazione era aumentato fino a raggiungere il 53 %[31].

---

[29] Decisione (UE) 2017/899 del Parlamento europeo e del Consiglio relativa all'uso della banda di frequenza 470-790 MHz nell'Unione.

[30] Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio che istituisce il codice europeo delle comunicazioni elettroniche.

[31] Cfr. Osservatorio 5G e gruppo "Politica dello spettro radio".

Tabella 4 – Situazione relativa all'assegnazione delle bande pioniere 5G, dicembre 2020

Stato membro	700 MHZ	3,6 GHZ	26 GHZ
Belgio		Uso provvisorio	
Bulgaria			
Cechia	✓	✓	
Danimarca	✓	✓	✓
Germania	✓	✓	✓
Estonia		-	
Irlanda		✓	
Grecia	✓	✓	✓
Spagna		✓	
Francia	✓	✓	
Croazia			
Italia		✓	✓
Cipro	✓	✓	
Lettonia		✓	
Lituania			
Lussemburgo	✓	✓	
Ungheria	✓	✓	
Malta			
Paesi Bassi	✓		
Austria	✓	✓	
Polonia			
Portogallo		Uso provvisorio	
Romania			
Slovenia			
Slovacchia	✓	✓	
Finlandia	✓	✓	✓
Svezia	✓	✓	

Fonte: Osservatorio 5G e gruppo "Politica dello spettro radio".

40 La Corte ha riscontrato che i ritardi nell'assegnazione della banda dei 26 GHz sono dovuti principalmente a una domanda debole da parte dei gestori di reti mobili. In Spagna, ad esempio, dalla banda dei 26 GHz sono disponibili in totale 1,5 GHz per l'uso ai fini del 5G. Tuttavia, secondo una consultazione pubblica conclusasi nel luglio 2019, le frequenze disponibili non sono ancora state assegnate agli operatori perché non ve ne è domanda. Una nuova consultazione pubblica è prevista entro la fine del 2021, al

fine di mettere all'asta la banda nel secondo trimestre del 2022. Anche in Finlandia i gestori di reti mobili hanno osservato che non vi è ancora molto interesse né convenienza commerciale per la banda dei 26 GHz.

41 Ai ritardi nell'assegnazione dello spettro 5G hanno contribuito anche questioni di coordinamento transfrontaliero con i paesi non-UE (Bielorussia, Russia e Ucraina) lungo i confini orientali dell'UE. Nell'ambito degli accordi internazionali in vigore, questi paesi non-UE utilizzano la banda dei 700 MHz per la radiodiffusione televisiva e la banda dei 3,6 GHz per i servizi satellitari militari. Questa problematica riguarda principalmente i paesi baltici (Estonia, Lettonia e Lituania) e la Polonia. Secondo la Commissione, sono stati compiuti alcuni progressi con l'Ucraina e la Bielorussia, che dovrebbero liberare la banda dei 700 MHz entro la fine del 2022. I colloqui bilaterali con la Russia non hanno ancora fatto registrare progressi. In considerazione di tale situazione, l'Estonia e la Polonia hanno chiesto una deroga ai termini ultimi per l'assegnazione della banda dei 700 MHz, fino alla metà del 2022.

42 Inoltre, in Polonia e Spagna, le aste per lo spettro 5G sono state rinviate durante la pandemia di COVID-19 (cfr. ***riquadro 3***).

Riquadro 3

Esempi di ritardi nell'assegnazione dello spettro 5G causati dalla COVID-19

- Nel marzo 2020, la Polonia ha annunciato un'asta per la banda dei 3,6 GHz, che doveva essere aggiudicata entro il 30 giugno 2020. A seguito dell'insorgere della pandemia, le autorità polacche hanno deciso di sospendere ogni procedimento amministrativo per tutta la durata della pandemia. A settembre 2021, il processo per la messa all'asta di detta banda non era ancora completato.

- In Spagna, l'asta per la banda dei 700 MHz era inizialmente prevista per marzo 2020. Tuttavia, secondo le autorità spagnole, la pandemia di COVID-19 ha ritardato la liberazione di questa banda, utilizzata per la televisione digitale. Successivamente, l'asta è stata rinviata fino al maggio 2020 e poi al primo trimestre del 2021. A seguito di una modifica della legislazione spagnola nell'aprile 2021 per allineare la durata delle licenze con quanto disposto dal codice europeo delle comunicazioni elettroniche, l'asta è stata riprogrammata per l'estate 2021 e la banda a 700 MHz è stata infine aggiudicata nel luglio 2021.

43 Un ulteriore motivo che ritarda l'assegnazione delle bande pioniere 5G è costituito dai diversi approcci adottati dagli Stati membri per la sicurezza del 5G e dai ritardi nell'adozione delle rispettive leggi in materia, il che genera incertezza per le imprese (cfr. paragrafi ***74*** e ***75***).

- In Spagna, l'asta per le bande pioniere conteneva una clausola generale secondo cui i titolari di concessioni pubbliche devono rispettare tutti gli obblighi in materia di sicurezza delle reti 5G stabiliti in qualunque momento futuro dalla normativa europea o spagnola. Il gestore di reti mobili spagnolo intervistato dagli auditor della Corte ha affermato che questa clausola lo ha obbligato a prendere decisioni in merito alle strategie e agli acquisti in condizioni di incertezza. Ha inoltre sottolineato che le autorità nazionali non erano disposte a chiarire alcune condizioni fondamentali, come la possibilità di una compensazione se la futura normativa, la cui adozione è prevista entro la fine del 2022, gli imponesse la sostituzione delle apparecchiature.

- In Polonia, una delle ragioni del rinvio dell'assegnazione dello spettro 5G è stata la necessità di attendere che una legge chiarisse i requisiti di sicurezza per le reti 5G.

Sono necessari ulteriori sforzi per affrontare le questioni di sicurezza nel dispiegamento del 5G

44 Per quanto riguarda gli aspetti di sicurezza del 5G, la Corte ha verificato se:

- la Commissione abbia adottato le misure necessarie per promuovere una corretta progettazione del quadro di sicurezza e abbia fornito un sostegno adeguato agli Stati membri;

- gli Stati membri stiano attuando reti 5G sicure in modo concertato, adottando le misure di attenuazione incluse nel pacchetto di strumenti dell'UE sulla cibersicurezza del 5G e aggiornando la rispettiva normativa.

Quando la sicurezza del 5G è divenuta una delle principali preoccupazioni a livello dell'UE, la Commissione ha reagito rapidamente

45 Il piano d'azione per il 5G del 2016 non include alcuna considerazione in materia di sicurezza. La sicurezza delle reti 5G e la dipendenza eccessiva da fornitori di paesi non-UE, in particolare cinesi, sono state individuate come una problematica cruciale nel marzo 2019. Nella risoluzione del 12 marzo 2019[32], il Parlamento europeo ha espresso preoccupazione in merito ai fornitori non-UE di apparecchiature 5G che potrebbero rappresentare un rischio per l'UE a causa della legislazione dei loro paesi di origine. Lo stesso giorno, nelle sua prospettiva strategica sulle relazioni UE-Cina, la Commissione ha sottolineato la necessità di un approccio comune dell'UE alla sicurezza delle reti 5G per tutelarsi da potenziali gravi implicazioni per la sicurezza di cruciali infrastrutture digitali[33]. Nelle conclusioni del 21 e 22 marzo 2019, il Consiglio europeo ha chiesto alla Commissione di formulare una raccomandazione su un approccio concertato in materia di sicurezza delle reti 5G[34].

46 Pochi giorni dopo, la Commissione ha pubblicato una raccomandazione contenente una serie di misure sia a livello nazionale (ad esempio, valutazione dei rischi per il 5G) che a livello dell'UE (ad esempio, valutazione coordinata dei rischi), al fine di garantire un elevato livello di cibersicurezza delle reti 5G nell'UE[35].

---

[32] Risoluzione del Parlamento europeo del 12 marzo 2019 (2019/2575(RSP)).

[33] JOIN(2019) 5 final del 12.3.2019.Commissione europea, Comunicazione congiunta al Parlamento europeo, al Consiglio europeo e al Consiglio, UE-Cina – Una prospettiva strategica.

[34] Riunione del Consiglio europeo (21 e 22 marzo 2019) – Conclusioni.

[35] Raccomandazione (UE) 2019/534 della Commissione del 26 marzo 2019, "Cibersicurezza delle reti 5G".

47 Quasi tutti gli Stati membri avevano completato la propria valutazione nazionale dei rischi entro il termine ultimo del luglio 2019[36]. Nell'ottobre 2019, il gruppo di cooperazione NIS ha pubblicato la relazione sulla valutazione dei rischi coordinata a livello dell'UE in materia di cibersicurezza delle reti 5G e nel gennaio 2020 il "pacchetto di strumenti dell'UE sulla cibersicurezza del 5G"[37] (cfr. ***allegato VII***). Quest'ultimo è stato approvato dalla Commissione e dal Consiglio europeo[38].

Il pacchetto di strumenti dell'UE del 2020 per la cibersicurezza del 5G ha stabilito per la prima volta misure per far fronte alle minacce alla sicurezza a livello dell'UE, senza avere carattere prescrittivo

Considerare la sicurezza delle reti 5G come una competenza di sicurezza nazionale limita il campo d'azione della Commissione

48 I trattati dell'UE[39] definiscono la portata delle azioni per affrontare sfide quali quelle relative al dispiegamento di reti 5G sicure a livello dell'UE. Tale portata è ampia e lascia un margine di interpretazione alla Commissione e agli Stati membri (cfr. ***riquadro 4***).

---

[36] Comunicato stampa del 19 luglio 2019.

[37] Gruppo di cooperazione NIS, *Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures*, 01/2020.

[38] Commissione europea, Dispiegamento del 5G sicuro – Attuazione del pacchetto di strumenti dell'UE, COM(2020) 50 final; Conclusioni della riunione del Consiglio europeo (1 e 2 ottobre 2020), EUCO 13/20.

[39] Trattato sul funzionamento dell'Unione europea.

Riquadro 4

Competenze dell'UE relative alle reti 5G: una competenza concorrente o una questione di sicurezza nazionale?

In linea di principio, le reti 5G rientrano nell'ambito della competenza dell'UE per il mercato unico (competenza concorrente), sia come servizio (fornitura di un servizio da parte di gestori di reti mobili) sia come bene (le apparecchiature 5G, acquistate da detti gestori per costruire le rispettive reti 5G). Trattandosi di competenza concorrente, l'UE (la Commissione e le altre istituzioni dell'UE) può adottare misure giuridicamente vincolanti (legislazione) per assicurare l'istituzione del mercato unico e promuoverne il corretto funzionamento. La sicurezza delle reti 5G potrebbe essere considerata, in senso più ampio, come relativa allo spazio di libertà, sicurezza e giustizia dell'UE. In tal senso, la sicurezza può essere intesa come un termine generale relativo alla prevenzione e alla lotta contro la criminalità: quindi un'altra materia soggetta a competenza concorrente, per la quale l'UE può adottare misure giuridicamente vincolanti.

Per contro, un'interpretazione più restrittiva della sicurezza consisterebbe nel limitarla alle minacce per la sicurezza nazionale degli Stati membri. Poiché quest'ultima è di esclusiva competenza nazionale, l'UE può intraprendere solo azioni di sostegno per sostenere gli sforzi nazionali degli Stati membri volti a garantire la sicurezza delle rispettive reti 5G.

49 La sicurezza delle reti 5G ricade allo stesso tempo nelle competenze UE e nazionali e riguarda anche la sicurezza nazionale. La Commissione ha affrontato la sicurezza delle reti 5G nel senso di minacce alla sicurezza nazionale ed ha dunque optato per misure di *soft law*. Ciò implica che l'UE non può adottare misure giuridicamente vincolanti che obblighino gli Stati membri ad applicare misure uniformi di mitigazione dei rischi o che impongano obblighi aventi forza esecutiva. La Commissione può invece emettere raccomandazioni e comunicazioni non vincolanti, contribuire a diffondere le migliori pratiche e coordinare le azioni nazionali degli Stati membri. Tuttavia, è possibile adottare un approccio diverso. Ne è un esempio la "direttiva NIS"[40], atto normativo dell'UE che tratta la sicurezza delle reti e dei sistemi informativi nell'UE. Tale atto normativo è stato proposto dalla Commissione e adottato

[40] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

nell'ambito della base giuridica del "mercato unico", sebbene la cibersicurezza sia in larga misura una prerogativa nazionale[41].

Il pacchetto di strumenti dell'UE sulla cibersicurezza del 5G è stato adottato in una delle prime fasi del dispiegamento, ma alcuni gestori di reti mobili avevano già scelto i propri fornitori

50 Nel gennaio 2020, il gruppo di cooperazione NIS ha adottato il "pacchetto di strumenti dell'UE sulla cibersicurezza del 5G", che specifica una serie di misure strategiche, tecniche e di sostegno volte ad affrontare le minacce alla sicurezza delle reti 5G ed identifica gli attori pertinenti per ciascuna di dette misure. Questo pacchetto di strumenti, approvato dalla Commissione e dal Consiglio europeo, è stato adottato solo nove mesi dopo che il Parlamento europeo e il Consiglio avevano sollevato per la prima volta preoccupazioni in merito alla sicurezza del 5G. Più di recente, il pacchetto di strumenti dell'UE sulla cibersicurezza del 5G è stato menzionato, nella nuova strategia europea per il potenziamento di connessioni intelligenti, pulite e sicure nei sistemi digitali mondiali, come uno strumento per guidare gli investimenti in infrastrutture digitali[42]. L'approccio di *soft law* adottato dalla Commissione ha contribuito a mettere in atto rapidamente misure per affrontare le minacce alla sicurezza anche a livello dell'UE e ad agevolare la cooperazione degli Stati membri su questa tematica transfrontaliera. A titolo di confronto, per la direttiva NIS sono stati necessari più di tre anni dalla proposta della Commissione[43] all'adozione[44] e per la direttiva sul codice europeo per le comunicazioni elettroniche ci sono voluti più di due anni[45]. Ancora più tempo è stato necessario per recepire le direttive negli ordinamenti giuridici nazionali degli Stati membri (cfr. anche paragrafi ***36*** e ***37***).

51 Il pacchetto di strumenti dell'UE sulla cibersicurezza del 5G è stato adottato quattro anni dopo che la politica in materia di 5G era stata definita nel piano d'azione per il 5G, ossia nello stesso anno in cui le tappe intermedie di dispiegamento stabilite nell'ambito di detto piano avrebbero dovuto essere raggiunte. In tale contesto, i

---

[41] Analisi n. 02/2019, "Le sfide insite in un'efficace politica dell'UE in materia di cibersicurezza (Documento di riflessione)", paragrafo 36.

[42] Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo, al Comitato delle regioni e alla Banca europea per gli investimenti, "Il Global Gateway", JOIN(2021) 30 final dell'1.12.2021.

[43] COM(2013) 48 final del 7.2.2013.

[44] Direttiva (UE) 2016/1148.

[45] Cfr. COM(2016) 590 final del 12.10.2016 e direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio che istituisce il codice europeo delle comunicazioni elettroniche.

rappresentanti dei ministeri degli Stati membri, delle autorità nazionali di regolamentazione e dei gestori di reti mobili intervistati ai fini del presente audit ritenevano che le misure relative agli aspetti di sicurezza del 5G fossero state avviate troppo tardi.

52 Allo stesso tempo, il pacchetto di strumenti è stato pubblicato quando il dispiegamento ed i piani per il 5G erano nelle primissime fasi nella maggior parte degli Stati membri. La maggior parte dei contratti per apparecchiature 5G tra fornitori ed operatori è stata conclusa nel 2020 e nel 2021. Tuttavia, secondo l'Associazione degli operatori di reti di telecomunicazioni europei (ETNO), alcuni gestori di reti mobili avevano già scelto i propri fornitori quando il pacchetto di strumenti dell'UE sulla cibersicurezza del 5G è stato reso disponibile.

Il pacchetto di strumenti dell'UE sulla cibersicurezza del 5G ha fornito un quadro per valutare il profilo di rischio dei fornitori, ma sono rimaste carenze

Alcuni Stati membri ed alcune autorità nazionali ritengono che una parte dei criteri utilizzati per classificare i fornitori ad alto rischio non sia sufficientemente chiara

53 Una caratteristica fondamentale del pacchetto di strumenti dell'UE sulla cibersicurezza del 5G è la necessità per gli Stati membri di valutare i fornitori e di applicare, per "gli asset chiave definiti critici", restrizioni ai fornitori considerati ad alto rischio. Gli Stati membri dovrebbero effettuare tale valutazione sulla base di un elenco non esaustivo di criteri estratti dalla valutazione dei rischi coordinata a livello dell'UE. Tali criteri sono, ad esempio:

- la probabilità che un fornitore sia soggetto a ingerenze del governo di un paese non-UE: ad esempio, in ragione dell'esistenza di un forte legame tra il fornitore e il governo di un paese non-UE; oppure a causa della legislazione del paese non-UE, specialmente dove non sono operanti controlli ed equilibri legislativi e/o democratici, oppure in assenza di accordi sulla sicurezza o sulla protezione dei dati conclusi tra l'UE e il paese non-UE;
- la capacità del fornitore di assicurare l'approvvigionamento;
- la qualità complessiva dei prodotti e delle pratiche di cibersicurezza dei fornitori.

54 Il pacchetto di strumenti è stato concepito per evitare la frammentazione e promuovere la coerenza nel mercato interno. I criteri definiti nel pacchetto offrono un quadro operativo utile per valutare il profilo di rischio dei fornitori in modo coordinato in tutti gli Stati membri. Il pacchetto ha anche permesso alla Commissione di reagire in modo celere alle emergenti preoccupazioni in materia di sicurezza del 5G, insieme agli Stati membri. Al tempo stesso, resta responsabilità delle autorità nazionali applicare detti criteri nel valutare i rischi associati a specifici fornitori. A ottobre 2021, tenendo conto di questo quadro, 13 Stati membri hanno introdotto o modificato disposizioni normative sulla sicurezza del 5G (cfr. paragrafo ***75*** e ***figura 6***).

55 Tuttavia, i rappresentanti di due dei quattro ministeri degli Stati membri interpellati ai fini del presente audit ritenevano che alcuni di questi criteri di classificazione dei fornitori di apparecchiature 5G sono soggetti a interpretazione e necessiterebbero di essere ulteriormente chiariti. Hanno anche invitato la Commissione a fornire sostegno ed orientamenti aggiuntivi circa la classificazione dei venditori ad alto rischio. I rappresentanti degli Stati membri interpellati hanno anche indicato che questo stato di cose ha creato il rischio che gli Stati membri applichino approcci divergenti in materia di fornitori ad alto rischio (cfr. anche paragrafi ***74***-***75*** e ***riquadro 5***). Undici delle autorità nazionali di regolamentazione interpellate tramite questionario, che hanno diversi gradi di coinvolgimento nella sicurezza del 5G, hanno espresso preoccupazioni analoghe.

Il paese di origine dei fornitori di tecnologie 5G incide sulla valutazione dei rischi per la sicurezza

56 I fornitori di tecnologie 5G variano in termini di caratteristiche societarie e provengono da paesi aventi legami diversi con l'UE. La ***figura 5*** presenta alcune caratteristiche comuni e differenze tra i principali fornitori di apparecchiature 5G e i loro paesi di origine, in particolare per aspetti che – stando a quanto indicato nel pacchetto di strumenti dell'UE – sarebbero in grado di influenzare la valutazione del profilo di rischio (cfr. paragrafo ***53***).

Figura 5 – Caratteristiche comuni e differenze tra i fornitori di apparecchiature 5G e i loro paesi di origine

Fonte: Corte dei conti europea, sulla base dei seguenti criteri e delle seguenti fonti: appartenenza all'OMC; appartenenza all'OCSE; OCSE, *FDI Restrictiveness Index*; Banca mondiale, *Worldwide Governance Indicators Dataset*, 2019; Forum economico mondiale, *Global Competitiveness Dataset*, 2018; Commissione europea, decisioni di adeguatezza; Statista, *Who is leading the 5G patent race?*; dati societari di Ericsson; dati societari di Nokia; dati societari di Qualcomm; dati societari di Sharp; dati societari di LG; dati societari di Samsung; dati societari di Huawei; e dati societari di ZTE. Tassi di cambio al 31.12.2020.

57 Uno dei fattori di rischio è la misura in cui il paese d'origine del fornitore rispetta i valori politici ed economici fondamentali dell'UE. Fattori legati allo specifico paese, quali lo Stato di diritto, l'indipendenza del potere giudiziario, l'apertura agli investimenti esteri e l'esistenza di accordi in materia di protezione dei dati, possono essere considerati come una misura della protezione giuridica di un'impresa dall'ingerenza del governo, nonché della protezione che l'impresa può estendere ai propri clienti.

58 Mentre i fornitori aventi sede negli Stati membri dell'UE sono tenuti a rispettare le norme e gli obblighi giuridici dell'UE, ciò non vale per sei dei principali fornitori, situati in paesi non-UE, che operano nel quadro della legislazione di paesi non-UE (cfr. ***figura 5***). Tali legislazioni possono differire notevolmente dalle norme dell'UE, ad esempio per quanto riguarda la protezione dei dati concessa ai cittadini, l'efficacia di tale protezione o, più in generale, il modo in cui l'indipendenza del potere giudiziario è garantita da controlli ed equilibri legislativi e/o democratici. Per quanto riguarda l'indipendenza del potere giudiziario, gli Stati Uniti e il Giappone mostrano punteggi più elevati di altri paesi di origine non-UE dei fornitori di apparecchiature 5G, mentre per il *rating* dello Stato di diritto è la Corea del Sud a registrare i migliori risultati tra i paesi non-UE.

59 Le reti 5G sono gestite in prevalenza da software. Il fatto che alcuni fornitori operino nel quadro di ordinamenti non-UE potrebbe essere particolarmente preoccupante se anche i centri di controllo del software sono ubicati al di fuori dell'UE: gli utenti dell'UE potrebbero potenzialmente essere soggetti a normativa non-UE.

60 La Commissione ha iniziato ad affrontare tali preoccupazioni, ritenendo che tutte le imprese che forniscono servizi ai cittadini dell'UE debbano rispettare le norme e i valori dell'UE[46]. Ha avviato dialoghi con diversi paesi per garantire una forte protezione della privacy dei dati personali[47]. Come illustrato nella ***figura 5***, la Commissione ha già riconosciuto l'adeguatezza dei regimi di protezione dei dati del Giappone (e, nel passato, degli Stati Uniti). Va osservato, però, che le decisioni di adeguatezza possono essere contestate e sono soggette al rigoroso controllo degli organi giurisdizionali. A titolo di esempio, nel 2015 la Corte di giustizia dell'Unione europea ha annullato lo strumento giuridico allora applicabile per lo scambio di dati con gli Stati Uniti, ossia il

---

[46] Comunicazione della Commissione europea, Plasmare il futuro digitale dell'Europa, COM(2020) 67 final.

[47] Cfr. "UE-Cina – Una prospettiva strategica".

regime “Approdo sicuro”[48], e successivamente, nel 2020, ha stabilito che il regime “Scudo UE-USA per la privacy” (che aveva sostituito “Approdo sicuro”) non offriva adeguate tutele ai cittadini dell’UE[49]. Non vi è dunque al momento alcuna decisione di adeguatezza per gli Stati Uniti. Più in generale, e al di là dell’esistenza di un regime di protezione dei dati, è importante tener conto del più ampio quadro giuridico ed istituzionale, compreso ad esempio il rispetto dello Stato di diritto e il modo in cui è assicurata l’indipendenza del potere giudiziario.

61 Dalla ***figura 5*** emerge inoltre una notevole variabilità tra i fornitori di apparecchiature 5G in termini di quota di brevetti 5G, ricavi e numero di effettivi. Ciò si ripercuote sulle risorse a loro disposizione e, a sua volta, potrebbe incidere sulla loro resilienza e capacità di garantire la continuità dell’approvvigionamento. Ad esempio, Samsung e Huawei sono i fornitori che detengono la quota più elevata di brevetti 5G, generano i ricavi più alti come società e hanno il maggior numero di dipendenti nel complesso.

62 La probabilità che un fornitore subisca interferenze da parte del governo di un paese non-UE è un altro fattore importante, definito nel pacchetto di strumenti come determinante per il profilo di rischio del fornitore. In tale contesto, la proprietà svolge un ruolo importante, in quanto i proprietari con un gran numero di azioni potrebbero esercitare pressioni o influenzare le decisioni di gestione. Inoltre, le società di proprietà privata o statale sono considerate meno aperte al controllo pubblico, in termini di audit e obbligo di rendiconto, rispetto alle società quotate in borsa soggette a rigorosi obblighi di informativa nel corso dell’anno a beneficio degli investitori generali e delle autorità di regolamentazione. La maggior parte dei fornitori di apparecchiature 5G è quotata in borsa, nel proprio paese di origine o all’estero, mentre i fornitori cinesi sono più difficili da classificare e sono generalmente percepiti come strettamente collegati al governo cinese[50].

---

[48] Sentenza nella causa C-362/14 e relativo comunicato stampa.

[49] Sentenza nella causa C-311/18 e relativo comunicato stampa.

[50] Cfr. https://www.europarl.europa.eu/doceo/document/E-9-2020-004305_EN.html e https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637912/EPRS_ATA(2019)637912_EN.pdf

Gli Stati membri ritengono che il sostegno della Commissione e dell'ENISA sia stato utile nell'attuare il pacchetto di strumenti dell'UE sulla cibersicurezza del 5G

63 La Commissione ha fornito sostegno agli Stati membri scambiando le migliori pratiche relativamente ad alcune misure chiave del pacchetto di strumenti dell'UE sulla cibersicurezza del 5G, anche in materia di fornitori ad alto rischio. Tale sostegno, spesso fornito nell'ambito del gruppo di cooperazione NIS, è stato integrato da specifiche attività dell'ENISA, quali l'organizzazione di *webinar* o la messa a disposizione di orientamenti su:

- l'attuazione del pacchetto, con particolare attenzione alle misure tecniche;
- le migliori pratiche in materia di sicurezza delle reti, in particolare per quanto riguarda:
  - gli scenari di minaccia per il 5G[51];
  - la preparazione delle valutazioni nazionali dei rischi relativi al 5G;
  - le misure di sicurezza disposte dal codice europeo delle comunicazioni elettroniche[52], comprese apposite linee-guida sulla sicurezza del 5G[53].

64 La Commissione ha inoltre incaricato l'ENISA di preparare il sistema UE di certificazione della cibersicurezza per le reti 5G, che dovrebbe contribuire ad affrontare i rischi connessi alle vulnerabilità tecniche delle reti e a rafforzare ulteriormente la cibersicurezza[54]. Sebbene tale certificazione possa contribuire a migliorare la sicurezza, non può impedire che le minacce siano integrate nei sistemi mediante aggiornamenti del software.

65 Tutti i rappresentanti delle autorità degli Stati membri intervistati dagli auditor della Corte ai fini del presente audit hanno sottolineato l'utilità del sostegno della Commissione e dell'ENISA ai fini dell'attuazione del pacchetto di strumenti dell'UE sulla sicurezza del 5G. Inoltre, la maggior parte delle autorità nazionali di regolamentazione delle telecomunicazioni (15 su 21) ha dichiarato che la Commissione e/o l'ENISA hanno

---

[51] ENISA, *Threat Landscape for 5G Networks*, 14.12.2020.

[52] ENISA, *Guideline on Security Measures under the EECC*, 10.12.2020.

[53] ENISA, *Guideline on Security Measures under the EECC*, 7.7.2021.

[54] Comunicato stampa del 3 febbraio 2021.

sostenuto le autorità nazionali nello scambio delle migliori pratiche di attuazione delle principali misure strategiche.

Il pacchetto di strumenti dell'UE sulla cibersicurezza del 5G è stato adottato troppo tardi per essere preso in considerazione per i progetti cofinanziati dall'UE nel periodo 2014-2020

66 Uno degli obiettivi del pacchetto di strumenti dell'UE sulla cibersicurezza del 5G è far sì che i progetti 5G cofinanziati dall'UE tengano conto dei rischi per la cibersicurezza. Il pacchetto di strumenti però è stato adottato solo nel gennaio 2020. Poiché tutti i progetti esaminati dagli auditor della Corte per il presente audit erano stati selezionati prima dell'adozione del pacchetto di strumenti sulla cibersicurezza del 5G, non ci si poteva aspettare che seguissero l'approccio raccomandato per la cibersicurezza, neanche nei confronti dei fornitori ad alto rischio. Ad esempio, nel campione della Corte sono stati individuati un progetto relativo a Orizzonte 2020 e due progetti FESR in Spagna che utilizzavano apparecchiature 5G cinesi successivamente vietate in Svezia (cfr. paragrafo ***15***).

67 Per il periodo 2021-2027, la Commissione intende promuovere un approccio coerente in materia di sicurezza del 5G per i progetti cofinanziati dall'UE, facendo in modo che il rispetto del pacchetto di strumenti sia una condizione per ottenere i finanziamenti dell'UE. Ciò varierà, tuttavia, in funzione della modalità di attuazione:

- i programmi sottoposti alla gestione diretta della Commissione (ad esempio Orizzonte Europa del periodo 2021-2027) consentirà l'esclusione dei fornitori soggetti a interferenze del governo di un paese non-UE. In questo modo, è probabile che i progetti finanziati dall'UE tengano conto dei rischi per la cibersicurezza e che si evitino situazioni in cui un fornitore che riceve co-finanziamenti dell'UE in uno Stato membro venga considerato ad alto rischio, ed escluso, in un altro Stato membro;

- per i programmi attuati in regime di gestione concorrente, la normativa non contempla requisiti in materia di rischi per la cibersicurezza. La Commissione prevede quindi di promuovere l'introduzione di un riferimento al pacchetto di strumenti negli accordi di partenariato, come modo per permettere che per i finanziamenti FESR a progetti relativi al 5G si tenga conto dei rischi di cibersicurezza;

- per InvestEU (il programma che sostituisce il FEIS)[55] e il dispositivo per la ripresa e la resilienza, la Commissione prevede di incoraggiare gli organismi responsabili a far riferimento al pacchetto di strumenti dell'UE negli accordi di finanziamento.

Quando realizzano le reti 5G, gli Stati membri non affrontano ancora in modo concertato gli aspetti relativi alla sicurezza

Le informazioni sull'approccio agli aspetti della sicurezza adottato dagli Stati membri sono insufficienti

68 La Commissione segue e comunica i progressi compiuti nell'attuazione del pacchetto di strumenti dell'UE sulla cibersicurezza del 5G tramite il gruppo di cooperazione NIS, i colloqui bilaterali con gli Stati membri e, indirettamente, gli organi di informazione. I primi risultati di tale monitoraggio sono stati pubblicati nel luglio 2020[56]. Nel dicembre 2020, la Commissione ha inoltre pubblicato una relazione sull'impatto della propria raccomandazione sulla cibersicurezza delle reti 5G[57]. A settembre 2021, non era pianificata alcuna rendicontazione futura.

69 Le suddette relazioni, tuttavia, sono sprovviste di un insieme comune di indicatori chiave di performance e non presentano una serie comparabile di informazioni dettagliate sul modo in cui gli Stati membri stanno affrontando i timori circa la sicurezza del 5G.

70 Inoltre, vi sono scarse informazioni di dominio pubblico sul modo in cui gli Stati membri entrano in contatto con i fornitori ad alto rischio (cioè come avvenga la loro individuazione) e sull'eventuale esclusione dei fornitori per l'approvvigionamento di apparecchiature 5G; peraltro, le informazioni disponibili sono contraddittorie e incomplete. Ad esempio:

---

[55] Regolamento (UE) 2021/523 che istituisce il programma InvestEU.

[56] *Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity*, luglio 2020.

[57] *Report on the impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks*, SWD(2020) 357 final del 16.12.2020.

- nella relazione di luglio 2020 sui progressi compiuti dagli Stati membri nell'attuazione del pacchetto di strumenti dell'UE (cfr. paragrafo ***68***), la Commissione sosteneva che circa la metà degli Stati membri (14 su 27) aveva valutato il profilo di rischio dei fornitori e applicato restrizioni a quelli considerati ad alto rischio;

- in una relazione del dicembre 2020[58], il BEREC indicava che solo nove Stati membri avevano posto in essere tali restrizioni e che sette degli altri 18 Stati membri non intendevano porle in atto in futuro.

71 Anche quando gli Stati membri hanno adottato norme in materia di sicurezza delle reti 5G (cfr. anche paragrafo ***75***), queste non chiariscono comunque l'approccio degli Stati membri nei confronti dei fornitori ad alto rischio. È probabile che qualsiasi decisione concreta venga presa solo mediante atti di esecuzione o decisioni amministrative o commerciali non pubbliche.

72 Stando ai portatori di interessi e ai responsabili decisionali interpellati (ad esempio, presso il Parlamento europeo), sono scarse anche le informazioni non pubbliche (ad esempio, contenute in relazioni della Commissione o del gruppo NIS) sull'approccio degli Stati membri nei confronti dei fornitori ad alto rischio, per cui si vedono costretti a fare affidamento su mass media e fonti non ufficiali.

73 Nonostante la natura transfrontaliera dei timori circa la sicurezza del 5G, nel complesso sono disponibili al pubblico poche informazioni sul modo in cui gli Stati membri affrontano le questioni di sicurezza, in particolare per quanto concerne i fornitori ad alto rischio. Ciò ostacola la condivisione delle conoscenze tra Stati membri e la possibilità di applicare misure concertate. Questo limita anche le possibilità per la Commissione di proporre miglioramenti alla sicurezza delle reti 5G.

Vi sono indizi secondo i quali alcuni Stati membri seguono approcci divergenti nei confronti dei fornitori di tecnologie 5G

74 Nell'attuare le misure chiave in materia di sicurezza del 5G, le autorità nazionali godono di un ampio margine discrezionale (cfr. paragrafi ***48***-***49***). Il pacchetto di strumenti tiene conto delle competenze nazionali e dei pertinenti fattori specifici di un paese (valutazione delle minacce da parte dei servizi preposti alla sicurezza nazionale, calendario del dispiegamento del 5G, presenza di fornitori, capacità di cibersicurezza).

---

[58] BEREC, *Internal Report concerning the EU 5G Cybersecurity Toolbox Strategic Measures 5 and 6 (Diversification of suppliers and strengthening national resilience)*, BoR 20 (227), 10.12.2020.

Finora, gli Stati membri hanno seguito approcci divergenti riguardo all'utilizzo di apparecchiature di fornitori specifici o alla portata delle restrizioni imposte ai venditori ad alto rischio (cfr. esempi relativi a quattro Stati membri nel ***riquadro 5***).

Riquadro 5

Esempi di approcci divergenti degli Stati membri nei confronti dei fornitori cinesi di tecnologie 5G

Quadro esistente e restrizioni applicate[(1)]

Nell'ottobre 2020 l'autorità nazionale svedese di regolamentazione delle telecomunicazioni (PTS) ha posto le seguenti condizioni per la partecipazione all'asta dello spettro 5G:

— i nuovi impianti e l'attuazione delle funzioni centrali per l'uso radio delle bande di frequenza non devono utilizzare prodotti di fornitori cinesi;

— qualsiasi infrastruttura esistente di tali fornitori deve essere gradualmente dismessa entro e non oltre il 1° gennaio 2025.

Quadro esistente, ma non ancora applicato[(2), (3), (4)]

In Germania, la legge sulla sicurezza informatica 2.0 del maggio 2021 prevede la certificazione obbligatoria delle componenti cruciali prima che ne possa essere autorizzato l'impiego. I gestori tedeschi di reti mobili interpellati dagli auditor della Corte preferirebbero un'unica procedura europea di certificazione sotto l'egida dell'ENISA, che funga da "sportello unico" europeo, piuttosto che dover conseguire un'eventuale pletora di certificazioni nazionali. A norma di detta legge, inoltre, il ministero federale dell'Interno può vietare l'uso di componenti cruciali, qualora possano rappresentare una minaccia per la sicurezza nazionale.

In Austria, la legge sulle telecomunicazioni aggiornata adottata alla fine di ottobre 2021 consente al ministero competente di classificare ad alto rischio i fornitori e di applicare restrizioni o di escluderli dal mercato. Le informazioni di dominio pubblico (ottobre 2021) indicano che il paese sta per estendere la propria rete 5G utilizzando il fornitore cinese Huawei.

Nessun quadro esistente[(5), (6)]

A settembre 2021, l'Ungheria non aveva limitato il ricorso ad alcun fornitore di tecnologie 5G ed è improbabile che lo faccia in un prossimo futuro. Tale paese ha anche ufficialmente rifiutato di aderire al programma internazionale per reti 5G pulite (*Clean Network Program*), promosso dagli Stati Uniti, che mira a limitare la presenza di fornitori cinesi nelle reti centrali 5G.

1) Decisione 18-8496 del 20.10.2020 sui termini dell'asta per le bande di frequenza 3,5 GHz e 2,3 GHz.

2) *Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)*

3) Legge sulle telecomunicazioni austriaca.

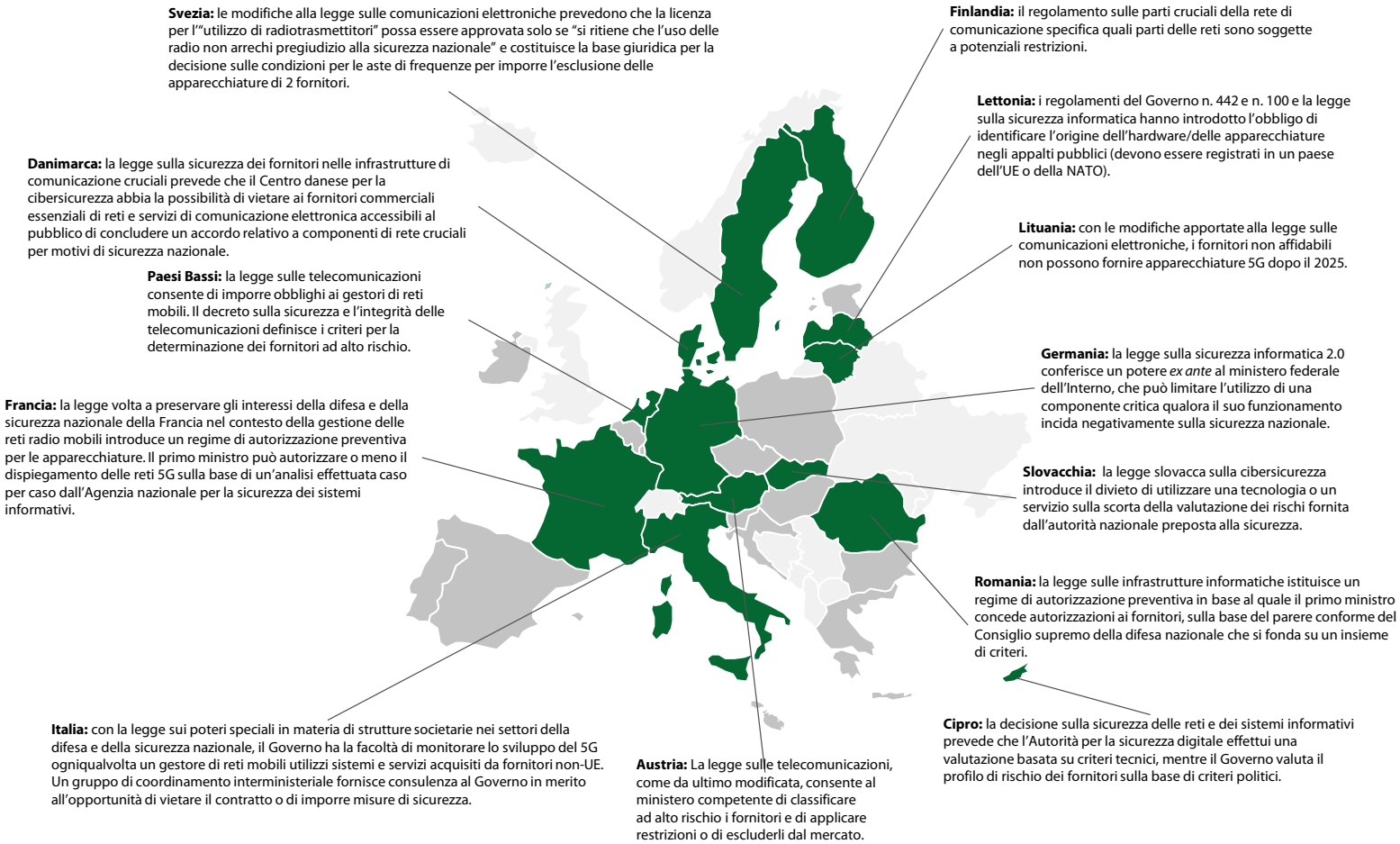
4) https://www.euractiv.com/section/5g/news/austria-to-also-rely-on-huawei-in-5g-rollout/

5) https://chinaobservers.eu/wp-content/uploads/2021/01/briefing-paper_huawei_A4_03_web-1.pdf

6) https://cms.law/en/int/expert-guides/cms-expert-guide-to-5g-regulation-and-law/hungary

75 Dall'adozione del pacchetto di strumenti, sono stati compiuti progressi per rafforzare la sicurezza delle reti 5G: la maggioranza degli Stati membri applica o è sul punto di applicare restrizioni nei confronti dei fornitori ad alto rischio. A fine 2021, 13 Stati membri avevano adottato o modificato leggi nazionali sulla sicurezza del 5G. Queste misure di regolamentazione tengono conto dei criteri fissati nel pacchetto di strumenti dell'UE, ma seguono approcci diversi (cfr. ***figura 6***). Altri Stati membri sono in procinto di introdurre disposizioni normative di questo tipo. Negli anni a venire ciò potrebbe portare ad approcci più convergenti nei confronti dei fornitori ad alto rischio di apparecchiature 5G, almeno tra quelli stati membri che hanno posto in essere detta normativa.

Figura 6 – Stati membri in cui vigono leggi che consentono di escludere dalle rispettive reti apparecchiature di fornitori ad alto rischio, situazione a ottobre 2021



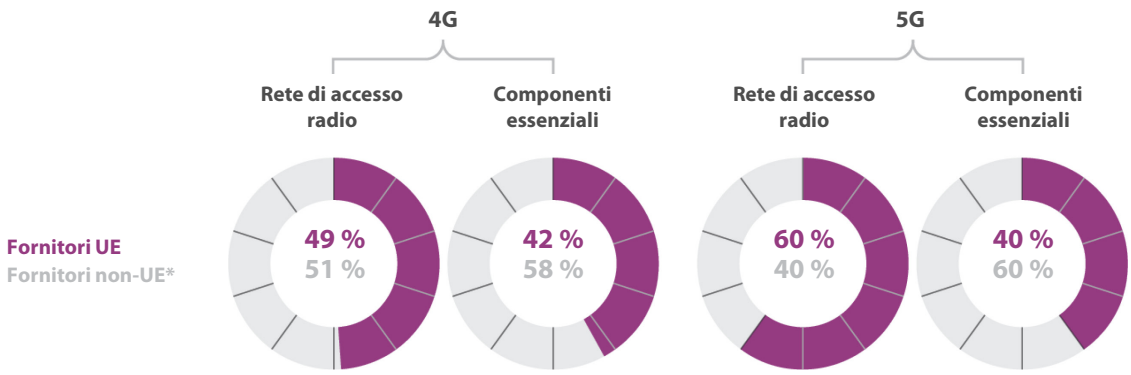
Fonte: Corte dei conti europea, sulla base dei dati della Commissione europea.

76 Finora, la Commissione non ha valutato quale sarà l'impatto di tali approcci divergenti nel caso in cui uno Stato membro costruisca le proprie reti 5G utilizzando apparecchiature di un fornitore considerato ad alto rischio in un altro Stato membro. Tale situazione potrebbe incidere sulla sicurezza transfrontaliera o sulla concorrenza tra gestori di reti mobili operanti nel mercato unico dell'UE.

La Commissione ha iniziato di recente ad affrontare il problema delle sovvenzioni estere distorsive del mercato interno

77 A dicembre 2020, oltre la metà delle apparecchiature 4G e 5G nell'UE proveniva da fornitori non-UE (cfr. ***figura 7***).

Figura 7 – Quota di gestori di reti mobili che utilizzano apparecchiature di fornitori UE/non-UE*



* *Nei fornitori non-UE rientrano i fornitori nordamericani, asiatici e australiani.*

Fonte: Corte dei conti europea sulla base di BEREC, *Internal Report concerning the EU 5G Cybersecurity Toolbox Strategic Measures 5 and 6 (Diversification of suppliers and strengthening national resilience)*, BoR (20) 227.

78 In particolare, alla fine del 2019, 286 milioni di clienti nell'UE-27 (il 64 % della popolazione totale) utilizzavano reti di telecomunicazione basate sulle apparecchiature 4G di fornitori cinesi[59]. Nell'ottobre 2020, un gruppo di deputati del Parlamento europeo si è rivolto con preoccupazione ai ministri delle telecomunicazioni e del commercio degli Stati membri e alla Commissione affermando che uno dei motivi di tale grande quota di mercato dei fornitori cinesi è che questi ultimi hanno goduto di un vantaggio economico sleale, ossia hanno percepito sovvenzioni pubbliche alle quali i fornitori UE non hanno accesso nel quadro della normativa dell'UE sugli aiuti di

[59] StrandConsult, *Understanding the Market for 4G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 102 Mobile Networks*.

Stato[60]. In un'analisi recente, la Corte ha evidenziato rischi analoghi a tale riguardo[61]. Tali sovvenzioni possono falsare il mercato interno, creando così condizioni di disparità tra i fornitori di tecnologie 5G, con eventuali implicazioni per la sicurezza. Nel maggio 2021, per affrontare questo problema, la Commissione ha proposto un nuovo regolamento[62] che stabilisce procedure per indagare su tali sovvenzioni e correggere le relative distorsioni del mercato.

La Commissione non dispone di informazioni sufficienti circa i possibili costi di sostituzione delle apparecchiature dei fornitori cinesi

79 Stando a una relazione del giugno 2020[63], estromettere dall'UE un importante fornitore di infrastrutture 5G comporterebbe un aumento dei costi totali di investimento pari a quasi 2,4 miliardi di euro all'anno nei prossimi dieci anni (ossia 24 miliardi di euro in totale). Secondo un altro studio[64], gli operatori europei stanno già affrontando il potenziamento delle reti 4G costruite tra il 2012 e il 2016, in quanto è prassi commerciale corrente revisionare e ammodernare le apparecchiature di rete che hanno più di tre o quattro anni. Secondo questo studio, il costo totale per "eliminare e sostituire" le apparecchiature aggiornabili acquistate dai fornitori cinesi a partire dal 2016 ammonterà a circa 3 miliardi di euro.

80 La quota elevata di apparecchiature provenienti da fornitori cinesi, insieme alla loro eventuale classificazione nella categoria "ad alto rischio" in taluni Stati membri, potrebbe comportare costi di sostituzione dell'ordine di miliardi di euro se i gestori di reti mobili fossero obbligati a rimuovere e sostituire le apparecchiature dei fornitori cinesi dalle reti europee senza che venga previsto un periodo di transizione (cfr. paragrafi ***77***-***79***). In linea di principio, non possono essere concessi aiuti di Stato per compensare gli operatori per l'adempimento di un obbligo giuridico, a meno che gli Stati membri non riescano a dimostrare alla Commissione che sono soddisfatti i

---

[60] Lettera dei deputati al Parlamento europeo ai ministri delle telecomunicazioni e del commercio degli Stati dell'UE e ai commissari europei Thierry Breton, Margrethe Vestager e Valdis Dombrovskis, 14.10.2020.

[61] Analisi 03/2020 della Corte dei conti europea,"La risposta dell'UE alla strategia cinese di investimenti guidati dallo Stato".

[62] Proposta di regolamento relativo alle sovvenzioni estere distorsive del mercato interno, COM(2021) 223 final del 5.5.2021.

[63] Oxford Economics, *Restricting competition in 5G network equipment throughout Europe*, giugno 2020 (sponsorizzato da Huawei).

[64] StrandConsult, *The real cost to 'rip and replace' Chinese equipment from telecom networks*.

necessari requisiti (come ad esempio un effetto incentivante). Dall'analisi compiuta dagli auditor della Corte è emerso un caso in cui il diritto nazionale potrebbe consentire che i costi di sostituzione siano sostenuti da finanziamenti pubblici nazionali (cfr. legge finlandese sui servizi di comunicazione elettronica[65]). Gli Stati membri sono tenuti a notificare alla Commissione qualunque caso di aiuto di Stato concesso per compensare i gestori di reti mobili per costi di questo tipo. La Commissione sostiene di non essere stata ancora contattata da alcuno Stato membro o portatore d'interesse per discutere di aiuti di Stato per costi di sostituzione di apparecchiature. Secondo i portatori d'interesse del settore interpellati nel corso dell'audit, l'incertezza circa il trattamento di detti costi da parte degli Stati membri, nonché le possibili differenze tra Stati membri, pregiudicano la certezza d'impresa e rischiano di avere ripercussioni sul dispiegamento del 5G nei tempi previsti.

[65] Legge sui servizi di comunicazione elettronica 1207/2020 del 30.12.2020, articolo 301.

Conclusioni e raccomandazioni

81 Nel complesso, dall'audit della Corte è emerso che, nonostante il sostegno della Commissione, vi sono notevoli ritardi nel dispiegamento delle reti 5G degli Stati membri e che sono necessari ulteriori sforzi per risolvere le questioni di sicurezza relative a detto dispiegamento.

82 Nel piano d'azione per il 5G del 2016, la Commissione ha sollecitato la copertura, con sistemi 5G, di tutte le aeree urbane e dei principali assi di trasporto entro il 2025, nonché nel 2021, una copertura totale entro il 2030. A fine 2020, 23 Stati membri avevano già varato servizi commerciali 5G e raggiunto l'obiettivo intermedio di aver almeno una grande città con accesso a detti servizi. Tuttavia, la Corte ha rilevato che non tutti gli Stati membri fanno riferimento agli obiettivi della Commissione nelle rispettive strategie nazionali in materia di 5G o nei rispettivi piani per la banda larga. Per di più, in numerosi paesi il codice europeo per le comunicazioni elettroniche non è ancora stato trasposto nel diritto nazionale e l'assegnazione dello spettro 5G ha subìto ritardi. Questi ritardi nell'assegnazione dello spettro radio possono essere ascritti a diverse ragioni: una debole domanda da parte dei gestori delle reti mobili; problematiche di coordinamento transfrontaliero con paesi non-UE lungo i confini orientali dell'UE; l'impatto della COVID-19 sui calendari delle aste e l'incertezza su come affrontare le questioni di sicurezza. Secondo la Commissione, è probabile che solo 11 Stati membri conseguano l'obiettivo fissato per il 2025 (cfr. paragrafi ***22***-***43***).

83 La Commissione ha aiutato gli Stati membri ad attuare il piano d'azione per il 5G del 2016 tramite iniziative, orientamenti ed il finanziamento della ricerca in materia di 5G. Tuttavia, la Commissione non ha definito la qualità di servizio attesa delle reti 5G, quali ad esempio le prestazioni che dovrebbero offrire in termini di velocità minima e latenza massima. Ne è conseguito che l'espressione "qualità del 5G" è stata interpretata in modi diversi dagli Stati membri. La Corte ha osservato che gli Stati membri hanno adottato approcci diversi nell'erogazione dei servizi 5G, come dimostra il fatto che solo due Stati membri hanno definito la velocità minima e la latenza massima. In ultima analisi, questi approcci divergenti comportano il rischio di disparità nell'accesso e nella qualità dei servizi 5G nell'UE, accrescendo così anziché riducendo il divario digitale tra Stati membri e regioni (cfr. paragrafi ***22***-***31***).

Raccomandazione 1 – Promuovere il dispiegamento bilanciato e tempestivo delle reti 5G nell'UE

La Commissione dovrebbe:

a) elaborare, insieme agli Stati membri, una definizione comune della qualità del servizio attesa per le reti 5G, come i requisiti di prestazione che dovrebbe offrire in termini di velocità minima e latenza massima;

b) incoraggiare gli Stati membri a includere nei prossimi aggiornamenti delle rispettive strategie 5G/digitali o dei rispettivi piani per la banda larga gli obiettivi di dispiegamento del 5G per il 2025 e il 2030, nonché le misure che saranno necessarie per il loro conseguimento;

c) sostenere gli Stati membri nel risolvere i problemi di coordinamento dello spettro 5G con paesi confinanti non facenti parte dell'UE, ad esempio chiedendo che questo tema sia all'ordine del giorno di ciascuna riunione pertinente.

Termine di attuazione: dicembre 2022

84 Gli aspetti della sicurezza delle reti 5G sono divenuti un'importante fonte di preoccupazione a livello dell'UE solo di recente. La necessità associata di un'azione a livello dell'UE è stata sottolineata dal Consiglio europeo nel 2019, quando ha invocato un approccio concertato e la cooperazione tra gli Stati membri su questa tematica a carattere transfrontaliero. La Commissione, insieme agli Stati membri, ha reagito in modo celere alle emergenti preoccupazioni in materia di sicurezza del 5G. Nel 2020, il gruppo di cooperazione NIS ha adottato il pacchetto di strumenti dell'UE sulla cibersicurezza del 5G, che specifica una serie di misure strategiche, tecniche e di sostegno volte ad affrontare le minacce alla sicurezza delle reti 5G ed identifica gli attori responsabili per ciascuna di dette misure. Di tali misure, varie affrontano la questione dei fornitori di apparecchiature 5G ad alto rischio. Questo pacchetto è stato successivamente approvato dalla Commissione e dal Consiglio europeo (cfr. paragrafi ***45***-***47***). Poiché si tratta di uno strumento di *soft law*, dette misure non hanno alcun effetto vincolante per gli Stati membri. Più di recente, il pacchetto di strumenti dell'UE sulla cibersicurezza del 5G è stato menzionato, nella nuova strategia europea per il potenziamento di connessioni intelligenti, pulite e sicure nei sistemi digitali mondiali, come uno strumento per guidare gli investimenti in infrastrutture digitali (cfr. paragrafo ***50***).

85 I criteri definiti nel pacchetto offrono un quadro operativo utile per valutare il profilo di rischio dei fornitori in modo coordinato in tutti gli Stati membri. Allo stesso tempo, l'effettuazione di detta valutazione rimane una responsabilità nazionale (cfr. paragrafo ***54***).

86 Dall'adozione del pacchetto, sono stati compiuti progressi per rafforzare la sicurezza delle reti 5G: la maggioranza degli Stati membri applica o è sul punto di applicare restrizioni nei confronti dei fornitori ad alto rischio. A ottobre 2021, tenendo conto di questo quadro, 13 Stati membri hanno introdotto o modificato disposizioni normative sulla sicurezza del 5G. Altri Stati membri sono in procinto di introdurre disposizioni normative che tengono conto dei criteri definiti nel pacchetto di strumenti dell'UE (cfr. paragrafi ***54*** e ***75***).

87 Il pacchetto è stato adottato in una delle prime fasi del dispiegamento del 5G, ma alcuni gestori di reti mobili avevano già selezionato i propri fornitori (cfr. paragrafo ***52***). Se le preoccupazioni per la sicurezza non vengono affrontate sin dalla concezione di una politica, si rischiano ripercussioni negative nel corso dell'attuazione di quest'ultima: ad esempio, i benefici attesi (quale la crescita del PIL) potrebbero venire erosi dal costo di affrontare le minacce (come i costi della cibercriminalità) (cfr. paragrafi ***02*** e ***04***).

88 Il pacchetto di strumenti tiene conto delle competenze nazionali e dei pertinenti fattori specifici di un paese. Dall'audit della Corte è emerso che, finora, gli Stati membri hanno seguito approcci divergenti per quanto riguarda l'uso di apparecchiature di fornitori ad alto rischio o la portata delle restrizioni (ad esempio, in merito solo alle parti fondamentali o cruciali della rete 5G oppure alla rete di accesso radio o a una sua parte) (cfr. paragrafi ***74***-***75***).

89 Nei prossimi anni, la normativa sulla sicurezza del 5G introdotta dagli Stati membri sulla base del pacchetto potrebbe portare ad approcci più convergenti nei confronti dei fornitori ad alto rischio di apparecchiature 5G. Tuttavia, poiché nessuna delle misure contenute in detto pacchetto è giuridicamente vincolante, la Commissione non ha il potere di farle rispettare. Pertanto, permane il rischio che il pacchetto di strumenti, di per sé, non riesca a garantire che gli Stati membri affrontino gli aspetti di sicurezza in modo concertato (cfr. paragrafi ***49***-***75***).

90 Molti fornitori di tecnologie 5G sono situati al di fuori dell'UE e operano quindi nel quadro della legislazione di paesi terzi, che può differire notevolmente dalle norme dell'UE, ad esempio per quanto riguarda l'efficacia della protezione dei dati concessa ai cittadini e, più in generale, il modo in cui l'indipendenza del potere giudiziario è garantita da controlli ed equilibri legislativi e/o democratici. Anche il fatto che le reti 5G siano gestite in prevalenza da software potrebbe destare particolare preoccupazione, qualora i centri di controllo di tali software siano situati in paesi non-UE, assoggettando potenzialmente i cittadini dell'UE alla legislazione di paesi che non fanno parte dell'Unione. La Commissione ha iniziato ad affrontare tali preoccupazioni, considerando che tutte le imprese che forniscono servizi ai cittadini dell'UE dovrebbero rispettare le norme e i valori dell'UE. Ha inoltre avviato dialoghi con diversi paesi per garantire una forte protezione della privacy dei dati personali (cfr. paragrafi ***56***-***62***).

91 Nonostante la natura transfrontaliera dei timori circa la sicurezza del 5G, sono disponibili al pubblico poche informazioni sul modo in cui gli Stati membri affrontano le questioni di sicurezza e sulla loro dipendenza da fornitori ad alto rischio. La Commissione effettua un monitoraggio dell'attuazione del pacchetto di strumenti dell'UE e riferisce in merito. Queste relazioni, tuttavia, non presentano informazioni dettagliate e comparabili sul modo in cui gli Stati membri affrontano i timori circa la sicurezza del 5G. Inoltre, a settembre 2021 non era pianificata alcuna rendicontazione futura. Questa carenza di informazioni ostacola la condivisione delle conoscenze tra Stati membri e la possibilità di applicare misure concertate. Limita anche le possibilità per la Commissione di proporre miglioramenti alla sicurezza delle reti 5G (cfr. paragrafi ***68***-***73***).

Raccomandazione 2 – Promuovere tra gli Stati membri un approccio concertato alla sicurezza del 5G

La Commissione dovrebbe:

a) fornire ulteriori orientamenti o sostenere azioni in merito agli elementi chiave del pacchetto di strumenti dell'UE sulla cibersicurezza del 5G, quali i criteri per la valutazione dei fornitori di tecnologie 5G e per la classificazione di questi ultimi nella categoria "ad alto rischio" e gli aspetti relativi alla protezione dei dati;

Termine di attuazione: dicembre 2022

b) promuovere la trasparenza in merito agli approcci degli Stati membri alla sicurezza del 5G, monitorando e riferendo in merito all'attuazione delle misure di sicurezza previste dal pacchetto di strumenti dell'UE sulla cibersicurezza del 5G. Ciò dovrebbe esser fatto utilizzando un insieme comune di indicatori chiave di performance;

Termine di attuazione: dicembre 2022

c) insieme agli Stati membri, valutare per quali aspetti della sicurezza delle reti 5G vi sia la necessità di specificare requisiti da far rispettare e, all'occorrenza, proporre atti legislativi.

Termine di attuazione: dicembre 2022

92 La Commissione ha iniziato a fronteggiare i presunti vantaggi economici sleali associati alle sovvenzioni estere. Tali sovvenzioni possono falsare il mercato interno, creando così condizioni di disparità tra i fornitori di tecnologie 5G, con eventuali implicazioni per la sicurezza (cfr. paragrafo ***78***).

93 La Commissione non dispone di sufficienti informazioni circa il trattamento, da parte degli Stati membri, di potenziali costi di sostituzione che potrebbero sorgere se i gestori di reti mobili fossero obbligati a rimuovere le apparecchiature dei fornitori ad alto rischio dalle reti dell'UE senza un periodo di transizione. Le differenze di trattamento potrebbero pregiudicare la certezza d'impresa e rischiare di avere ripercussioni sul dispiegamento nei tempi previsti del 5G (cfr. paragrafi ***79***-***80***). Allo stesso tempo, gli approcci degli Stati membri in materia di sicurezza del 5G e, in particolare, l'assenza di un approccio concertato in tutta l'UE possono compromettere l'efficace funzionamento del mercato unico. Finora, la Commissione non ha esaminato tale questione (cfr. paragrafi ***74***-***76***).

Raccomandazione 3 – Monitorare gli approcci degli Stati membri in materia di sicurezza del 5G e valutare l'impatto delle divergenze sull'efficace funzionamento del mercato unico

La Commissione dovrebbe:

a) promuovere un approccio trasparente e coerente al trattamento, da parte degli Stati membri, dei costi sostenuti dai gestori di reti mobili per sostituire le apparecchiature 5G acquistate da fornitori ad alto rischio; a tal fine, dovrebbe monitorare questo aspetto e rendicontare in merito nel quadro dell'attuazione del pacchetto di strumenti dell'UE sulla cibersicurezza del 5G;

b) valutare quale sarebbe l'impatto sul mercato unico qualora uno Stato membro costruisse le proprie reti 5G utilizzando apparecchiature di un fornitore considerato ad alto rischio in un altro Stato membro.

Termine di attuazione: dicembre 2022

La presente relazione è stata adottata dalla Sezione II, presieduta da Iliana Ivanova, Membro della Corte dei conti europea, a Lussemburgo il 15 dicembre 2021.

Per la Corte dei conti europea

Klaus-Heiner Lehne
Presidente

Allegati

Allegato I – Principali opportunità e rischi del 5G

OPPORTUNITÀ	RISCHI
Sviluppo di nuove tecnologie da parte delle imprese	**Rischi per la privacy**
Maggiore mobilità e **modernizzazione** del sistema dei trasporti	**Minacce** alla sicurezza nazionale
Consentire ulteriormente l'interconnettività degli oggetti fisici di uso quotidiano	**Dipendenza** dalla catena di approvvigionamento
Migliorare l'utilizzo dei processi elettronici nell'assistenza sanitaria (sanità digitale)	**Ciberattacchi**
Aumentare la sicurezza dei cittadini	**Effetti negativi** sulla salute
Sostenere i cambiamenti nell'uso dei media da parte della società	**Perdita di posti di lavoro** dovuta a incrementi di efficienza
Stimolare la creazione di posti di lavoro in molti settori e **trasformare** il mercato del lavoro	
Rafforzare la democrazia	
Ridurre il divario digitale	

Fonte: Corte dei conti europea, sulla base del Servizio Ricerca del Parlamento europeo, *European Science-Media hub*.

Allegato II – Impatto del malfunzionamento delle reti di telecomunicazione e degli incidenti di cibersicurezza: alcuni esempi

Francia: guasto ai numeri telefonici di emergenza[66, 67]

01 Il 3 giugno 2021, un'interruzione della rete Orange, la più grande società di telecomunicazioni della Francia, ha impedito per diverse ore di effettuare chiamate di emergenza. Sebbene si ritenga che la causa non sia stata un ciberattacco, l'incidente dimostra il potenziale impatto di un malfunzionamento per una infrastruttura di rete cruciale.

Irlanda: attacchi *ransomware* al sistema sanitario pubblico[68, 69, 70]

02 Nel maggio 2021 il servizio sanitario irlandese (*Health Service Executive*) ha chiuso tutti i propri sistemi informatici a causa di un attacco *ransomware*. L'attacco ha interessato tutti gli aspetti dell'assistenza ai pazienti, in quanto ha causato difficoltà nell'accesso alle cartelle cliniche, accrescendo il rischio di ritardi ed errori. Sebbene i funzionari irlandesi non siano a conoscenza di dati compromessi dei pazienti, la condivisione delle cartelle cliniche avrebbe potuto dare adito a ogni sorta di reato, tra cui frode e ricatto. Secondo il direttore generale di *Health Service Executive*, i costi stimati per il ripristino del sistema ammonterebbero verosimilmente a 500 milioni di euro (600 milioni di dollari statunitensi).

---

66 https://www.euronews.com/2021/06/03/french-telecom-operator-orange-apologises-after-emergency-numbers-crash-nationwide

67 https://www.reuters.com/business/media-telecom/orange-blames-network-outage-software-failure-audit-2021-06-11/

68 https://www.wsj.com/articles/irish-healthcare-service-shuts-down-it-systems-after-ransomware-attack-11620998875

69 https://www.reuters.com/technology/irish-health-service-hit-by-ransomware-attack-vaccine-rollout-unaffected-2021-05-14/

70 https://www.cert.europa.eu/cert/moreclusteredition/en/blog_DataBreachTodayinRSSSyndication-in-299786a86ffeab5aec16d55392d94819.20210624.en.html

Solarwinds[71], [72], [73]

03 Solarwinds è una società americana che sviluppa software per aiutare le imprese e gli enti statali e federali a gestire le reti, i sistemi e le infrastrutture informatiche. Agli inizi del 2020, Solarwinds è stata oggetto di un attacco software. I pirati informatici sono riusciti a diffondere gli attacchi ai clienti di Solarwinds mediante aggiornamenti del software contenenti codice malevolo che apriva falle nelle piattaforme dei clienti, consentendo un facile accesso agli attacchi e all'installazione di ulteriori *malware* e software spia.

[71] https://www.solarwinds.com/

[72] https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R

[73] https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?international=true&r=US&IR=T

Allegato III – Quadro giuridico e strategico

- **Commissione europea**
- **Consiglio europeo/ Consiglio dell'UE**
- **Normativa**
- **Gruppo di cooperazione NIS**

2016 Direttiva NIS, luglio 2016: introduce provvedimenti giuridici per innalzare il livello di cibersicurezza generale nell'UE.

2016 Piano d'azione per il 5G, settembre 2016: era teso a varare servizi 5G in tutti gli Stati membri al più tardi entro la fine del 2020; sarebbe poi seguito un rapido sviluppo per assicurare una copertura 5G ininterrotta delle aree urbane e dei principali assi di trasporto entro il 2025.

2018 Codice europeo delle comunicazioni elettroniche, dicembre 2018: era mirato a realizzare un mercato interno delle reti e dei servizi di comunicazione elettronica.

2019 Conclusioni del Consiglio europeo, marzo 2019: si attende con interesse la raccomandazione della Commissione su un approccio concertato in materia di sicurezza delle reti 5G.

2019 Raccomandazione sulla cibersicurezza delle reti 5G, marzo 2019: si raccomanda agli Stati membri di valutare i rischi di cibersicurezza che interessano le reti 5G a livello nazionale e adottare le necessarie misure di sicurezza.

2019 Conclusioni del Consiglio sull'importanza del 5G per l'economia europea, dicembre 2019: si evidenzia che una rapida e sicura diffusione delle reti 5G è fondamentale per rafforzare la competitività dell'UE e richiede un approccio coordinato a livello dell'UE.

2020 Pacchetto di strumenti per la cibersicurezza del 5G, gennaio 2020: si individua un possibile insieme comune di misure in grado di mitigare i principali rischi delle reti 5G per la cibersicurezza.

2020 Dispiegamento del 5G sicuro – Attuazione del pacchetto di strumenti dell'UE per la cibersicurezza del 5G, gennaio 2020: la Commissione approva il pacchetto di strumenti e ne definisce le tappe successive (ad esempio, una relazione sull'attuazione entro giugno 2020).

2020 Conclusioni del Consiglio sul tema "Plasmare il futuro digitale dell'Europa", giugno 2020: si sostiene la necessità di assicurare e attuare un approccio coordinato teso a mitigare i rischi principali per una diffusione sicura del 5G nell'UE.

2020 Conclusioni del Consiglio europeo, ottobre 2020: si approva il pacchetto di strumenti per la cibersicurezza del 5G, in particolare la necessità di applicare le pertinenti restrizioni ai fornitori ad alto rischio.

2020 Raccomandazione per […] garantire un accesso allo spettro radio 5G, settembre 2020: vengono definiti orientamenti per lo sviluppo delle migliori pratiche per promuovere la connettività e fornire un accesso allo spettro radio 5G tempestivo e favorevole agli investimenti.

2020 La strategia dell'UE in materia di cibersicurezza per il decennio digitale, dicembre 2020: documento non vincolante giuridicamente che illustra le priorità della Commissione e le azioni da questa previste per la cibersicurezza nel suo complesso, comprese le reti 5G.

2020 Proposta di direttiva NIS 2, dicembre 2020: mira a modernizzare e ampliare il campo di applicazione della direttiva in vigore, anche riguardando in modo più esplicito la cibersicurezza delle reti 5G.

2020 Proposta di direttiva sulla resilienza dei soggetti critici, dicembre 2020: è volta a ridurre le vulnerabilità delle infrastrutture critiche che sono essenziali per il funzionamento della società e dell'economia dell'UE.

2020 Bussola per il digitale 2030: il modello europeo per il decennio digitale, marzo 2021: delinea un percorso verso una visione e azioni comuni che consentano all'Europa di avere successo nel decennio digitale.

2021 Conclusioni del Consiglio sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale, marzo 2021: sono sostenute le prossime misure da adottare in materia di cibersicurezza delle reti 5G, presentate nella strategia della Commissione in materia di cibersicurezza.

Allegato IV – Esempi di progetti cofinanziati dal FEIS

Progetti FEIS relativi al 5G

I due progetti FEIS esaminati dalla Corte riguardavano gli investimenti in ricerca, sviluppo e innovazione per lo sviluppo di portafogli di prodotti per le reti 5G. Prevedevano lo sviluppo di hardware e software per la rete di accesso radio e per la rete centrale. Entrambi i progetti hanno contribuito a un'installazione di celle più intensa, hanno sostenuto la standardizzazione e hanno facilitato importanti esperimenti tecnologici.

I progetti sono stati avviati nel 2018 e si sono conclusi nel dicembre 2020. I relativi costi d'investimento combinati sono ammontati in totale a 3,9 miliardi di euro, di cui 1 miliardo di euro di finanziamenti del FEIS.

Allegato V – Esempi di progetti co-finanziati da Orizzonte 2020 e FESR

Progetto co-finanziato da Orizzonte 2020 relativo alle tecnologie 5G

In questo progetto, vengono utilizzate apparecchiature di tutti e tre i principali fornitori di tecnologie 5G (Ericsson, Huawei e Nokia), per testare queste ultime nel corridoio transfrontaliero che collega le città di Metz (Francia), Merzig (Germania) e Lussemburgo. Avviato nel novembre 2018, il progetto sarebbe dovuto durare 31 mesi. L'UE ha erogato 12,9 milioni di euro a fronte di un totale preventivato di 17,1 milioni di euro.

Progetto FESR relativo alle reti 5G

Questo progetto in Spagna è teso a fornire informazioni sul dispiegamento delle reti 5G. Comprende la sperimentazione di tecniche di gestione delle reti abilitate dalla tecnologia 5G, come la virtualizzazione della rete, l'*edge computing*, l'assegnazione dinamica dei servizi di rete e il *network slicing*, nonché lo sviluppo di casi d'uso per il 5G. Avviato nel 2019, il progetto sarebbe dovuto durare 30 mesi. Il contributo dell'UE è stato pari a 2,2 milioni di euro, a fronte di un costo totale atteso di 7,1 milioni di euro.

Allegato VI – Copertura 5G in città selezionate

Le immagini riportate di seguito sono basate su dati relativi alla connettività mobile a banda larga ricavati da test condotti da utenti della applicazione Nperf. Le aree in cui è stato individuato il 5G non sono necessariamente aperte sul piano commerciale. Poiché la performance delle reti dipende dai singoli gestori di reti mobili, le mappe seguenti, estratte il 4 ottobre 2021, mostrano solo la copertura e non la performance, ad esempio in termini di velocità e latenza.

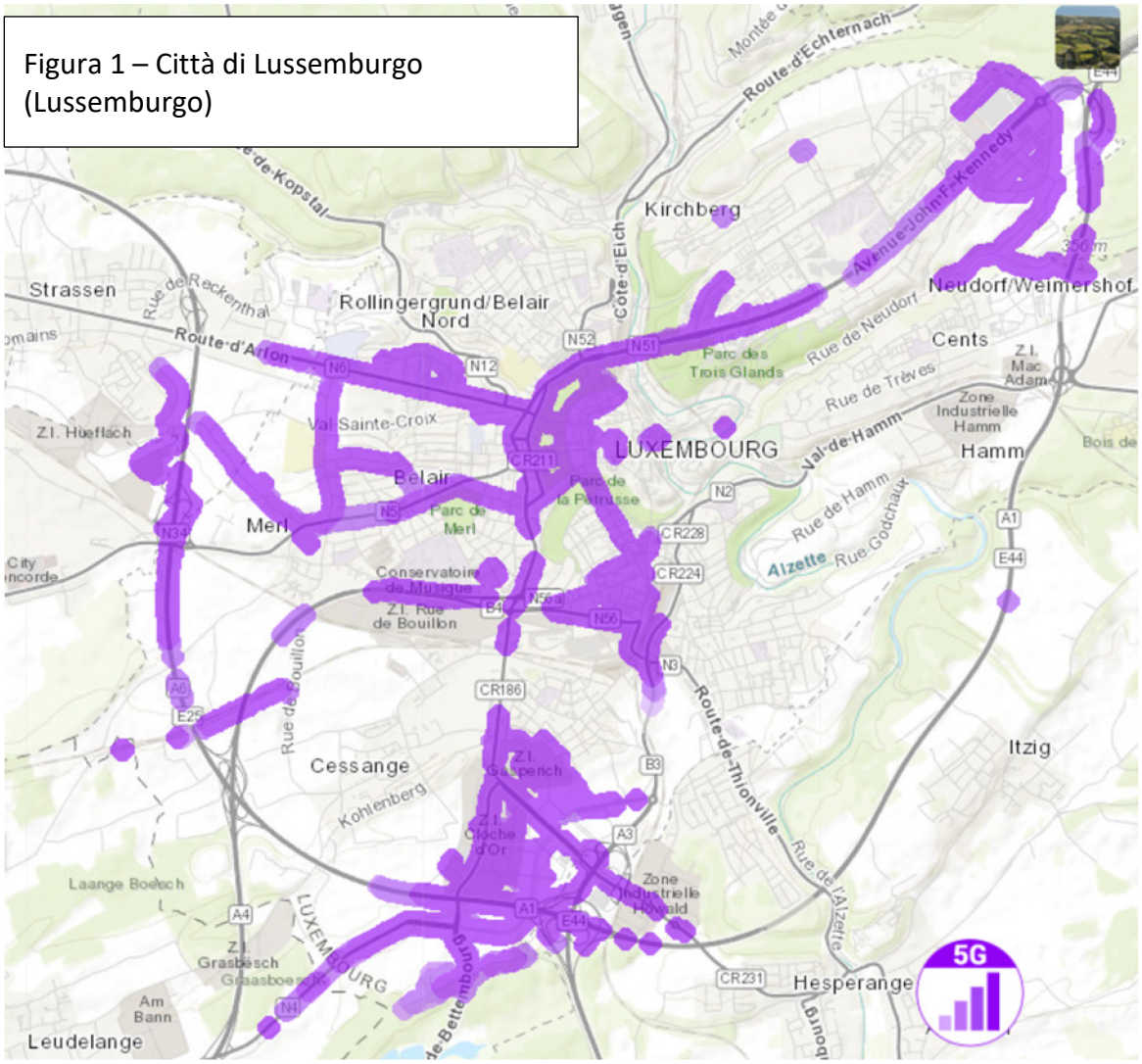


Figura 1 – Città di Lussemburgo (Lussemburgo)

© nPerf.

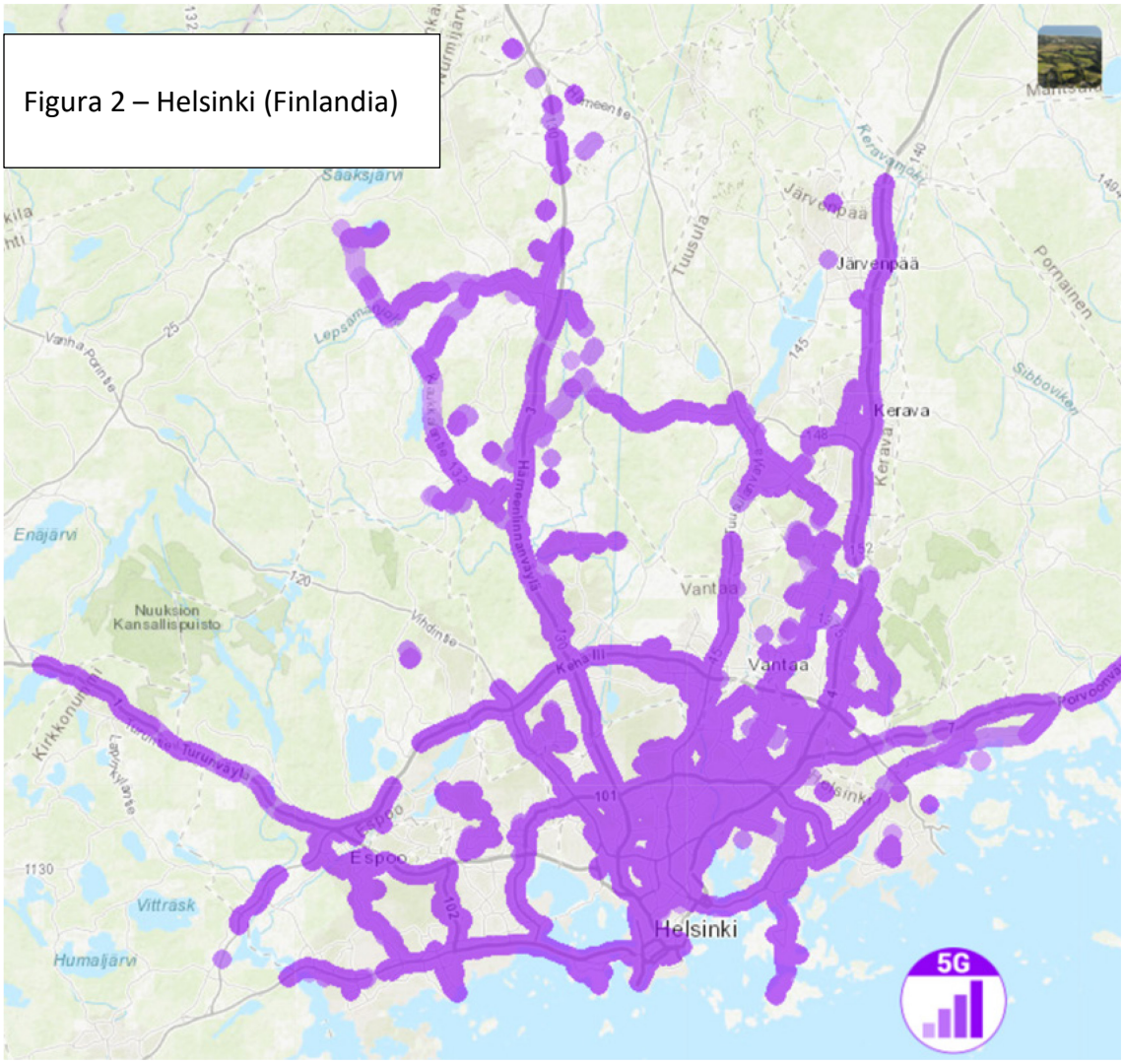


Figura 2 – Helsinki (Finlandia)

© nPerf.

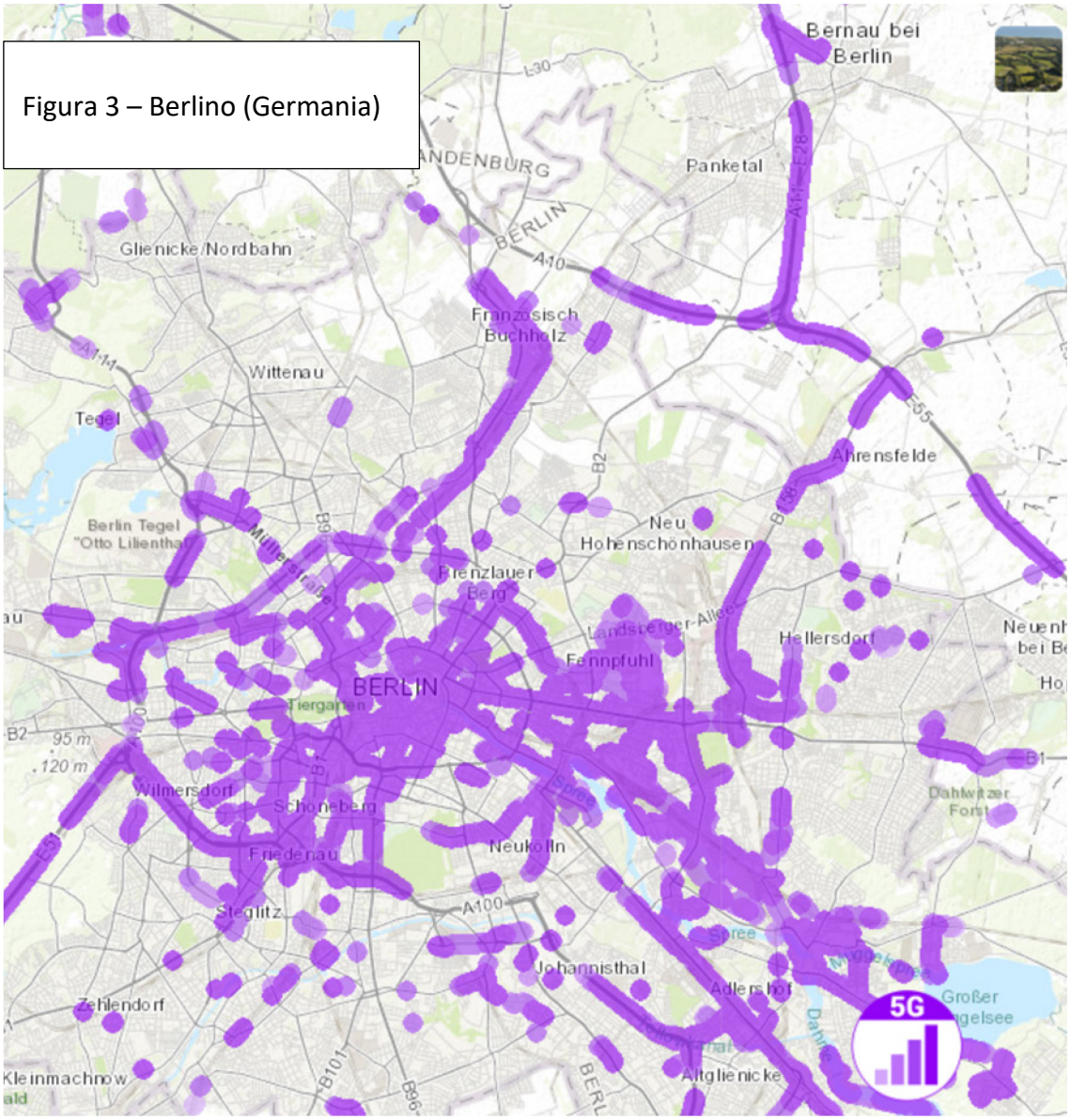


Figura 3 – Berlino (Germania)

© nPerf.

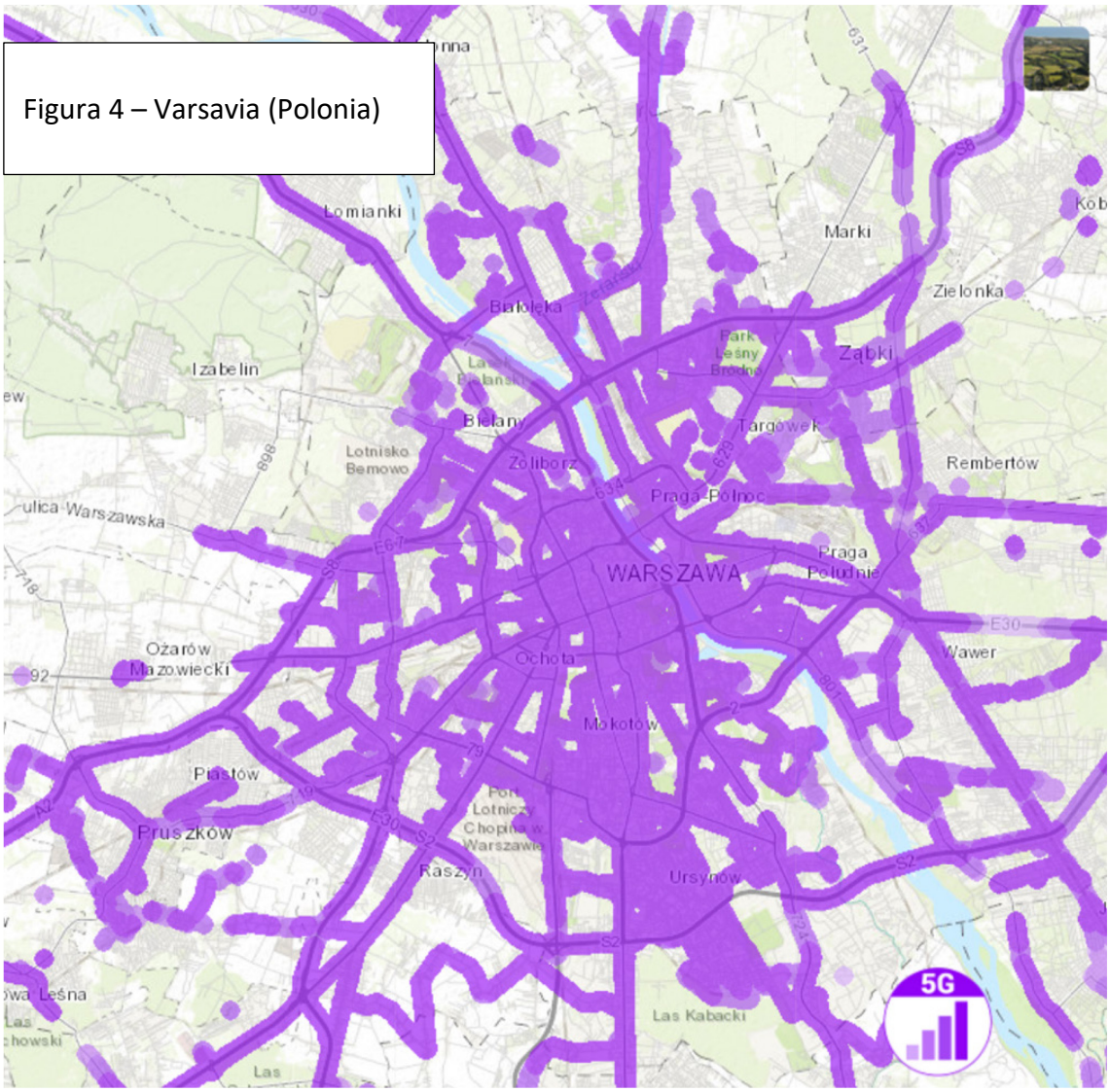


Figura 4 – Varsavia (Polonia)

© nPerf.

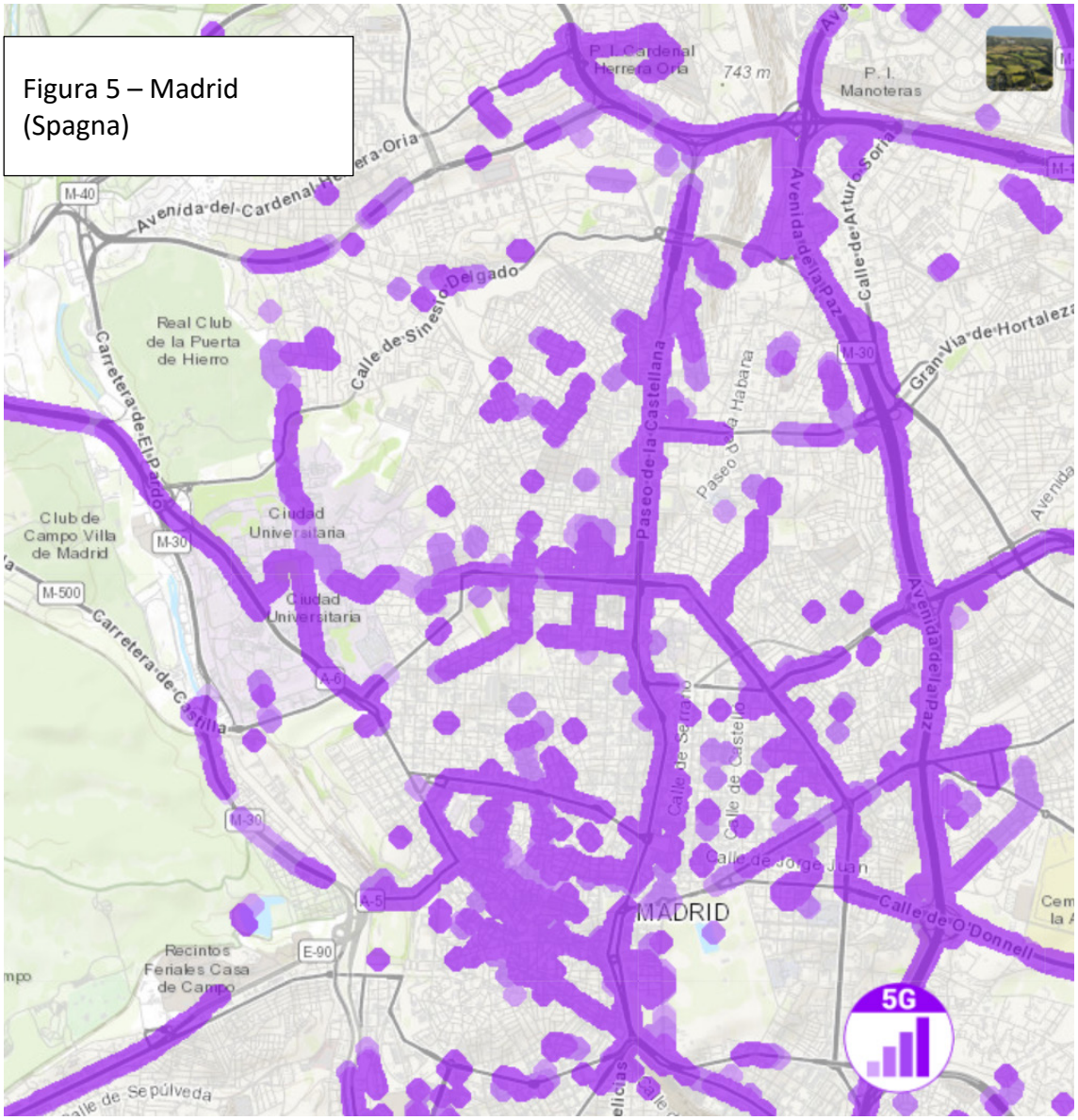


Figura 5 – Madrid (Spagna)

© nPerf.

Allegato VII – Pacchetto di strumenti dell'UE sulla cibersicurezza del 5G

Il pacchetto di strumenti dell'UE sulla cibersicurezza del 5G, adottato dal gruppo di cooperazione NIS e approvato dalla Commissione, contiene tre tipi di misure non vincolanti (strategiche, tecniche e di sostegno) che dovrebbero essere attuate da vari attori, come di seguito illustrato in sintesi.

Misure	Attori coinvolti				
	Autorità degli Stati membri	Gestori di reti mobili	Commissione europea	ENISA	Portatori di interessi (fornitori compresi)
Misure strategiche (SM)					
SM01 – Rafforzare il ruolo delle autorità nazionali	✓	✓			
SM02 – Sottoporre ad audit i gestori ed esigere informazioni	✓	✓			
SM03 – Valutare il profilo di rischio dei fornitori e applicare restrizioni a quelli considerati ad alto rischio (comprese le necessarie esclusioni per mitigare con efficacia i rischi) per gli elementi essenziali	✓	✓			
SM04 – Controllare il ricorso a fornitori di servizi gestiti e la terza linea di supporto dei fornitori di apparecchiature	✓	✓			
SM05 – Assicurare la diversità dei fornitori per i singoli gestori delle reti mobili attraverso adeguate strategie con molteplici fornitori	✓	✓			
SM06 – Rafforzare la resilienza a livello nazionale	✓	✓			
SM07 – Individuare gli elementi essenziali e promuovere un ecosistema diversificato e sostenibile per il 5G nell'UE	✓		✓		
SM08 – Creare e preservare la diversità e le capacità dell'UE nelle tecnologie di rete future	✓		✓		✓
Misure tecniche (TM)					
TM01 – Assicurare l'applicazione di requisiti di sicurezza di base (impostazione e architettura sicure delle reti)	✓	✓			
TM02 – Assicurare e valutare l'attuazione delle misure di sicurezza negli standard 5G esistenti	✓	✓			✓
TM03 – Assicurare rigorosi controlli di accesso	✓	✓			

Misure	Attori coinvolti				
	Autorità degli Stati membri	Gestori di reti mobili	Commissione europea	ENISA	Portatori di interessi (fornitori compresi)
TM04 – Accrescere la sicurezza delle funzioni di rete virtualizzate	✓	✓			
TM05 – Assicurare per le reti 5G una gestione, un funzionamento e un monitoraggio sicuri	✓	✓			
TM06 – Rafforzare la sicurezza fisica	✓	✓			
TM07 – Rafforzare per la gestione dell'integrità, degli aggiornamenti e delle *patch* del software	✓	✓			
TM08 – Innalzare gli standard di sicurezza nei processi dei fornitori attraverso solide condizioni di appalto	✓	✓			✓
TM09 – Utilizzare la certificazione UE per i componenti delle reti 5G, le apparecchiature per clienti e/o i processi dei fornitori	✓	✓	✓	✓	✓
TM10 – Utilizzare la certificazione UE per altri prodotti e servizi informatici non specifici per il 5G (dispositivi connessi, servizi "cloud")	✓		✓	✓	✓
TM11 – Rafforzare la resilienza e i piani di continuità	✓	✓			✓
Azioni di sostegno (SA)					
SA01 – Rivedere o sviluppare orientamenti e migliori pratiche per la sicurezza delle reti	✓	✓		✓	
SA02 – Rafforzare le capacità di collaudo e di audit a livello nazionale e dell'UE	✓		✓	✓	
SA03 – Sostenere e plasmare la normazione per il 5G	✓	✓	✓	✓	✓
SA04 – Sviluppare orientamenti sull'attuazione delle misure di sicurezza negli standard 5G esistenti	✓			✓	
SA05 – Assicurare l'applicazione di misure di sicurezza standard di natura tecnica e organizzativa mediante uno specifico regime di certificazione a livello di UE	✓			✓	✓
SA06 – Scambio delle migliori pratiche sull'attuazione delle misure strategiche, in particolare per quanto concerne i quadri nazionali per valutare il profilo di rischio dei fornitori	✓				
SA07 – Migliorare il coordinamento nella risposta agli incidenti e nella gestione delle crisi	✓			✓	
SA08 – Condurre audit delle interdipendenze tra reti 5G e altri servizi essenziali	✓				
SA09 – Rafforzare i meccanismi di cooperazione, coordinamento e condivisione delle informazioni	✓			✓	
SA10 – Fare in modo che i progetti in materia di 5G destinatari di finanziamenti pubblici tengano conto dei rischi per la cibersicurezza	✓		✓		

Fonte: Pacchetto di strumenti dell'UE sulla cibersicurezza del 5G.

Acronimi e abbreviazioni

BEI: Banca europea per gli investimenti

BEREC: Organismo dei regolatori europei delle comunicazioni elettroniche

ENISA: Agenzia dell'Unione europea per la cibersicurezza

FEIS: Fondo europeo per gli investimenti strategici

FESR: Fondo europeo di sviluppo regionale

NIS: rete e sistema informativo

PIL: prodotto interno lordo

Glossario

Agenzia dell'Unione europea per la cibersicurezza: agenzia dell'UE istituita per sviluppare e mantenere un elevato livello di sicurezza delle reti e dell'informazione in tutti i settori della vita pubblica e privata.

Banda larga: trasmissione simultanea ad alta velocità di più formati informativi (quali dati, voce e video).

Exabyte: misura della capacità di archiviazione delle informazioni digitali, equivalente a 1 miliardo di gigabyte.

Fondo europeo per gli investimenti strategici: meccanismo di sostegno agli investimenti istituito dalla Banca europea per gli investimenti (BEI) e dalla Commissione, nell'ambito del piano di investimenti per l'Europa, per mobilitare investimenti privati in progetti di importanza strategica per l'UE.

Gestore di rete mobile: società di telecomunicazioni che offre servizi di comunicazione vocale e di dati agli utenti di telefonia mobile abbonati.

***Global System for Mobile Communications Association* (GSMA):** organizzazione di settore che rappresenta gli interessi dei gestori di reti mobili di tutto il mondo, nonché le imprese e le organizzazioni manifatturiere e di servizi che nutrono un interesse nell'infrastruttura mobile.

Gruppo "Politica dello spettro radio": gruppo consultivo ad alto livello, costituito dai rappresentanti degli Stati membri, che assiste e fornisce consulenza alle istituzioni dell'UE sullo sviluppo del mercato unico dei prodotti e dei servizi senza fili.

Gruppo di cooperazione per le reti e i sistemi informativi: organismo istituito dalla direttiva NIS per garantire la cooperazione e lo scambio di informazioni tra Stati membri; è composto di rappresentanti degli Stati membri dell'UE, della Commissione europea e dell'Agenzia dell'UE per la cibersicurezza.

Internet degli oggetti: oggetti fisici in cui sono integrati sensori, software e altre tecnologie che consentono loro di collegarsi senza fili e scambiare dati con altri dispositivi e sistemi.

Latenza: nelle reti informatiche, il tempo necessario al trasferimento di un insieme di dati da un punto a un altro.

Organismo dei regolatori europei delle comunicazioni elettroniche: Organismo composto dai rappresentanti delle autorità nazionali di regolamentazione degli Stati membri che assiste queste ultime e la Commissione nell'attuazione del quadro normativo dell'UE al fine di creare un mercato unico delle comunicazioni elettroniche.

Piano nazionale per la banda larga: documento di uno Stato membro contenente obiettivi strategici per il raggiungimento dei valori-obiettivo fissati dall'UE per la banda larga.

***Ransomware*:** software "maligno" che impedisce alle vittime di accedere a un sistema informatico o di leggere i file, costringendole a pagare un riscatto per ripristinare l'accesso.

Rete di accesso radio: parte importante della tecnologie di telecomunicazione moderna, che collega i singoli dispositivi ad altre parti di una rete mediante connessioni radio.

Spettro radio: porzione dello spettro elettromagnetico corrispondente alle frequenze radio.

Risposte della Commissione

https://www.eca.europa.eu/it/Pages/DocItem.aspx?did=60614

Cronologia

https://www.eca.europa.eu/it/Pages/DocItem.aspx?did=60614

Équipe di audit

Le relazioni speciali della Corte dei conti europea illustrano le risultanze degli audit espletati su politiche e programmi dell'UE o su temi relativi alla gestione concernenti specifici settori di bilancio. La Corte seleziona e pianifica detti compiti di audit in modo da massimizzarne l'impatto, tenendo conto dei rischi per la performance o la conformità, del livello delle entrate o delle spese, dei futuri sviluppi e dell'interesse pubblico e politico.

Il presente controllo di gestione è stato espletato dalla Sezione di audit II – presieduta da Iliana Ivanova, Membro della Corte – specializzata nei settori di spesa riguardanti gli investimenti a favore della coesione, della crescita e dell'inclusione. L'audit è stato diretto da Annemie Turtelboom, Membro della Corte, coadiuvata da:
Florence Fornaroli, capo di Gabinetto, e Celil Ishik, attaché di Gabinetto; Niels-Erik Brokopp, primo manager; Paolo Pesce, capoincarico; Jussi Bright, Rafal Gorajski, Zuzana Gullová, Alexandre Tan, Aleksandar Latinov e Nils Westphal, auditor.

Annemie Turtelboom

Florence Fornaroli

Celil Ishik

Niels-Erik Brokopp

Paolo Pesce

Jussi Bright

Rafal Gorajski

Zuzana Gullová

Aleksandar Latinov

Nils Westphal

PDF	ISBN 978-92-847-7407-4	ISSN 1977-5709	doi:10.2865/242424	QJ-AB-21-029-IT-N
HTML	ISBN 978-92-847-7398-5	ISSN 1977-5709	doi:10.2865/97533	QJ-AB-21-029-IT-Q

Secondo le previsioni, tra il 2021 e il 2025 il 5G farà aumentare il PIL europeo di un importo fino a 1 000 miliardi di euro, con un potenziale di creazione o trasformazione di posti di lavoro, fino a 20 milioni, in tutti i settori dell'economia. La Corte osserva che i ritardi stanno mettendo a rischio il raggiungimento degli obiettivi dell'UE per il dispiegamento del 5G e che sono necessari ulteriori sforzi per risolvere le questioni di sicurezza. Nella presente relazione, la Corte rivolge alla Commissione una serie di raccomandazioni volte ad accelerare l'attuazione tempestiva e concertata di reti 5G sicure nell'UE.

Relazione speciale della Corte dei conti europea presentata in virtù dell'articolo 287, paragrafo 4, secondo comma, del TFUE.

CORTE DEI CONTI EUROPEA

Ufficio delle pubblicazioni dell'Unione europea

CORTE DEI CONTI EUROPEA
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tel. +352 4398-1

Modulo di contatto: eca.europa.eu/it/Pages/ContactForm.aspx
Sito Internet: eca.europa.eu
Twitter: @EUAuditors