icom
istituto per la competitività

RAPPORTO OSSERVATORIO
RETI & SERVIZI DI NUOVA GENERAZIONE

FARE RETI NELLA RIPRESA

Gli scenari del decennio digitale europeo e italiano

CURATORI

Silvia Compagnucci
Stefano da Empoli

AUTORI

Silvia Compagnucci
Stefano da Empoli
Maria Rosaria Della Porta
Giusy Massaro
Lorenzo Principali
Domenico Salerno

SI RINGRAZIANO

Laura Gagliarducci e Giulia Palocci
per le attente letture e l'impaginazione

I-Com Edizioni

ISBN: 9791280680020
Ottobre 2021


icom
reti & servizi di nuova generazione

INDICE


icom
reti & servizi di nuova generazione

EXECUTIVE SUMMARY

Il **Rapporto I-Com 2021 sulle reti e i servizi di nuova generazione** si colloca in un periodo di profondo cambiamento in cui la pandemia che ancora ci troviamo a fronteggiare ha imposto a cittadini, imprese e pubbliche amministrazioni di ripensare le proprie abitudini, le proprie strutture organizzative e i propri modelli di business, avendo come unica certezza la possibilità di trovare nel digitale un alleato formidabile, certamente l'unico nei periodi di lockdown, in grado di garantire la continuità delle relazioni e delle attività economiche, finanche l'esercizio di diritti di primaria importanza come quello al lavoro e all'istruzione.

In questo momento di ripensamento generale in cui alcune delle decisioni adottate in via emergenziale nelle fasi iniziali della pandemia - come il massiccio ricorso al lavoro da remoto - si stanno ormai affermando come possibile ordinaria modalità organizzativa da affiancare all'attività in presenza in molte organizzazioni, l'osservatorio, come da tradizione ormai consolidata, continua a monitorare il processo di **transizione al digitale** del nostro Paese, verificandone lo stato di avanzamento attraverso un confronto europeo e alla luce di alcune tendenze globali nel tentativo di fotografare lo stato dell'arte e tracciare le prospettive future.

In questa logica, nella prima parte, l'analisi persegue il fine di descrivere, da un lato, il **ruolo del digitale nelle politiche europee** attraverso l'analisi delle principali iniziative messe in campo dalla Commissione per ridisegnare la cornice normativa in materia digitale; dall'altro, verificare lo **stato di sviluppo delle infrastrutture fisse e mobili** e il grado di penetrazione dei servizi digitali nelle abitudini degli individui, nei modelli organizzativi della PA e nel modello di business delle imprese nei vari Paesi europei al fine di individuare, anche attraverso l'elaborazione dell'**I-Com ultraBroadband Index 2021**, i progressi compiuti dall'Italia, le criticità ancora esistenti e le possibili opportunità di miglioramento.

Nella seconda parte, invece, l'attenzione è focalizzata sul contesto nazionale rispetto al quale vengono descritte le iniziative nazionali a sostegno della digitalizzazione sia lato offerta che lato domanda, analizzati i dati di copertura nazionali rispetto alle reti fisse e mobili e verificato lo stato dell'arte e le prospettive future del Fintech e di alcune tecnologie emergenti (intelligenza artificiale, blockchain e cloud).

Nella parte conclusiva, infine, viene offerto qualche sintetico spunto di policy sui temi chiave affrontati nel rapporto.

Parte 1: Il digitale come leva per la ripresa europea

Il digitale nelle politiche dell'UE

Il biennio 2020-2021 rappresenta un momento di straordinaria rilevanza per la definizione del quadro normativo europeo di riferimento per il digitale. È in questo arco temporale, infatti, che la Commissione, con un poker di proposte di regolamento - Data Governance Act, Digital Services Act, Digital Markets Act e Artificial Intelligence Act - che perseguono, evidentemente obiettivi di armonizzazione massima, ha avviato, unitamente alle iniziative in materia di cybersecurity, un'opera di **ripensamento della cornice normativa vigente** che tenga conto della crescente importanza e delle straordinarie opportunità di crescita e miglioramento connesse all'utilizzo dei dati e allo sviluppo dell'intelligenza artificiale nonché del ruolo e della centralità assunta dalle piattaforme e dagli intermediari online.

Dopo la pubblicazione, nel febbraio 2020, della

Strategia europea per i dati, il 25 novembre 2020 la Commissione ha pubblicato la propria proposta di regolamento relativo alla governance europea dei dati (**Data Governance Act**) al fine di disciplinare la messa a disposizione dei dati del settore pubblico per il riutilizzo, qualora tali dati siano oggetto di diritti di terzi, la condivisione dei dati tra le imprese, dietro compenso in qualsiasi forma, il consenso all'utilizzo di dati personali con l'aiuto di un "*intermediario per la condivisione dei dati personali*", il cui compito consiste nell'aiutare i singoli individui a esercitare i propri diritti a norma del regolamento generale sulla protezione dei dati (GDPR) e il consenso all'utilizzo dei dati per scopi altruistici.

Rispetto al **tema piattaforme e intermediari**, nel dicembre 2020 la Commissione ha pubblicato due proposte di regolamento, il **Digital Services Act (DSA)** e il **Digital Market Act (DMA)** attraverso cui disciplinare obblighi, divieti e responsabilità in capo alle piattaforme.

In particolare, il **DMA** persegue il fine di disciplinare quelle piattaforme che agiscono sempre più come *gateway* o *gatekeeper* tra utenti commerciali e utenti finali, che godono di una posizione consolidata e duratura e si trovano nella possibilità di fare usi impropri dei dati degli utenti, rafforzare le barriere all'ingresso nel mercato e porre in essere comportamenti scorretti nei confronti degli utenti commerciali e deli utenti finali. In tale logica, la proposta della Commissione fissa i criteri per qualificare un *provider* come *gatekeeper* e individua una serie di obblighi e divieti discendenti dal possesso di tale qualifica. Con il **DSA**, invece, la Commissione intende offrire una risposta normativa agli enormi cambiamenti - cui si accompagnano non solo grandi opportunità ma anche nuovi rischi e criticità - determinati dalla crescente diffusione di servizi digitali a elevata innovatività che hanno rivoluzionato il modo di comunicare, interagire, consumare e fare business, mediante l'introduzione di un quadro orizzontale per tutte le categorie di contenuti, prodotti, servizi e attività sui servizi di intermediazione e la previsione di un regime di responsabilità diversificato in base ai servizi offerti e alla dimensione del fornitore. Per quanto riguarda la *governance*, la proposta di regolamento prevede a carico degli Stati membri specifici obblighi di verifica della *compliance* di fornitori di servizi operanti nei rispettivi territori rispetto alle previsioni contenute nel regolamento proposto, istituisce nuovi soggetti (i Coordinatori per i Servizi Digitali) e delinea meccanismi di *enforcement* e cooperazione tra gli Stati. Centrale, soprattutto nella proposta DMA naturalmente, il ruolo e l'intensità dei poteri attribuiti alla Commissione.

Il 21 aprile 2021, è stata infine pubblicata una proposta di **regolamento AI** intitolato "*Il regolamento del Parlamento europeo e del Consiglio che stabilisce norme armonizzate in materia di intelligenza artificiale e che modifica alcuni atti legislativi dell'Unione*", con il quale si istituisce un quadro di riferimento legale volto a normare il mercato dell'UE dell'intelligenza artificiale. Tale proposta, in particolare, si inquadra nell'ambito di un pacchetto più ampio che comprende anche una comunicazione sulla promozione di un approccio europeo all'intelligenza artificiale e il "*Piano Coordinato con gli Stati Membri: aggiornamento 2021*", con cui si va a istituire la nuova cornice normativa europea in materia e a perseguire gli obiettivi strategici fissati dalla Commissione che consistono nella definizione delle condizioni abilitanti per lo sviluppo e la diffusione dell'IA, nella costruzione di una leadership strategica nei settori d impatto elevato, nella creazione di un ecosistema favorevole al prosperare dell'IA e nella garanzia che le tecnologie di IA siano al servizio delle persone.

Rispetto al tema della **cybersecurity**, il 16 dicembre 2020 la Commissione e l'alto rappresentante dell'Unione per gli Affari esteri e la Politica di sicurezza hanno presentato la

"*Strategia dell'UE in materia di cibersicurezza per il decennio digitale*" al fine di rafforzare la resilienza collettiva dell'Europa contro le minacce informatiche e contribuire a garantire che tutti i cittadini e tutte le imprese possano beneficiare al meglio di servizi e strumenti digitali affidabili. Si tratta di una strategia straordinariamente importante che rientra nel "*Cybersecurity package*", pacchetto che comprende anche una nuova direttiva sulla resilienza delle entità critiche e una proposta di direttiva relativa alle misure necessarie per conseguire un elevato livello comune di cibersicurezza in tutta l'Unione (direttiva NIS rivista) e che rappresenta un nuovo insieme di azioni e iniziative, in parte già effettive e in parte ancora solo proposte, per indirizzare la sicurezza cibernetica dell'Unione nel prossimo decennio.

Con riferimento alla **revisione della direttiva NIS**, una delle innovazioni più rilevanti concerne senza dubbio l'estensione di specifici obblighi in materia di cybersecurity a soggetti ulteriori rispetto a quelli attualmente rientranti nell'ambito applicativo della direttiva, la puntuale identificazione delle tipologie di soggetti operanti nei vari settori e sotto-settori indicati che rientrano nella definizione di "*soggetto essenziale*" e "*soggetto importante*", che confluiscono, secondo quanto previsto dalla proposta di direttiva, in un apposito registro creato e tenuto dall'ENISA e sono sottoposti a regimi di vigilanza parzialmente diversi e la definizione dei contenuti minimi che le misure adottate dai soggetti essenziali e importanti devono contenere. In una logica di modernizzazione, la proposta prevede la divulgazione coordinata delle vulnerabilità e l'istituzione del **registro europeo delle vulnerabilità**, mentre agli Stati membri prescrive un arricchimento dei contenuti della strategia nazionale mediante l'adozione di un piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala (e la designazione delle autorità competenti responsabili). Dal punto di vista della governance, la proposta istituisce la **Rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe)** definendone la composizione e declinandone i compiti e rafforza gli strumenti di cooperazione.

Per quanto concerne la **proposta di direttiva sulla resilienza dei soggetti critici**, essa va a modificare la direttiva sulle infrastrutture critiche europee del 2008 estendendone sia l'ambito di applicazione, sia la profondità. Tale direttiva, in particolare, prescrive agli Stati membri l'adozione di una strategia nazionale, individua 10 settori e sottosettori di base da considerare (energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione e spazio) e prescrive una valutazione di tutti i rischi rilevanti, naturali e di origine umana, compresi i sinistri, le catastrofi naturali, le emergenze di sanità pubblica e le minacce antagoniste, inclusi i reati di terrorismo.

Se queste iniziative sono tese ad accelerare lo sviluppo delle reti, non sono mancati interventi tesi ad accrescere la **sicurezza delle reti 5G**. E infatti, nel febbraio 2020 la Commissione ha pubblicato la Comunicazione "*Dispiegamento del 5G sicuro - Attuazione del pacchetto di strumenti dell'UE*" e del pacchetto di strumenti dell'UE (**Toolbox sul 5G**) che, come noto, affronta tutti i rischi individuati nella relazione coordinata sulla loro valutazione, individuando e descrivendo una serie di misure strategiche e tecniche, nonché di corrispondenti azioni di sostegno volte a rafforzare la loro efficacia e che possono essere attuate per attenuarli. A luglio 2020 è stato pubblicato da parte del gruppo di cooperazione NIS, con il sostegno della Commissione e dell'ENISA, un report sui progressi degli Stati membri nell'attuazione del toolbox sulla sicurezza 5G in cui si fa il punto sul livello di maturità raggiunto dai vari Paesi nell'implementazione delle misure contenute nel Toolbox.

La tutela della sicurezza delle reti nei maggiori Paesi europei

Quello della **sicurezza** è un tema particolarmente sensibile poiché, nella definizione dei requisiti richiesti per poter operare nei vari Paesi si mescolano istanze di natura geopolitica a interventi che influiscono direttamente sulle dinamiche del mercato.

Tra i principali Paesi europei, la **Francia** si è dotata di una strategia nazionale di sicurezza cibernetica già dal 2015, poi aggiornata nel 2017. In seno all'SGDSN (*intelligence*) si trova l'ANSSI, ovvero l'Agenzia Nazionale della Sicurezza delle reti e dell'informazione, responsabile della prevenzione e della reazione a incidenti informatici ai danni delle istituzioni sensibili. Per quanto riguarda le infrastrutture di rete, la legge n.2019-810 modifica il modo in cui gli operatori mobili possono gestire le reti 5G e interviene sulla regolamentazione delle autorizzazioni intorno ad esse, in particolare imponendo che, per poter usare apparecchiature hardware e software per la connessione alla rete radiomobile francese, gli operatori coinvolti nei settori critici debbano ottenere un'autorizzazione preventiva da parte del Presidente del Consiglio. Nonostante la norma sia da applicare solo alle reti 5G, i vincoli tecnici che derivano dalla compatibilità di queste ultime con le infrastrutture *legacy* costituiscono un fattore determinante che rischia di rallentare il *deployment* delle nuove reti.

In **Germania** l'architettura istituzionale di sicurezza cibernetica approvata nel 2016 assegna ampie responsabilità all'Ufficio Federale per la Sicurezza Informatica (BSI) e al Ministero dell'Interno. Per quanto riguarda l'impianto legislativo, centrale importanza ha la legge IT SiG 2.0 (*IT Sicherheitsgesetz*), approvata dal Parlamento nell'aprile del 2021. La nuova norma identifica e amplia il perimetro delle cosiddette infrastrutture critiche, prendendo in considerazione anche i *cyber-critical operators*, ovvero tutti quegli istituti il cui malfunzionamento causerebbe, seppur in maniera indiretta, problemi alle infrastrutture critiche. Un'ulteriore novità è rappresentata dall'introduzione di un meccanismo di *assesment* sulla sicurezza dei componenti delle infrastrutture critiche. La Germania non prevede l'esclusione *ex-ante* di alcun *vendor*, ma lascia in capo al BMI, presso il Ministero dell'Interno, il potere di richiedere un periodo di valutazione delle apparecchiature di 2 mesi, consentendo anche la rimozione delle apparecchiature *ex-post* qualora queste rappresentino un pericolo per l'ordine pubblico o per la sicurezza della Repubblica Federale.

In **Spagna** il sistema istituzionale di sicurezza cibernetica si regge da una parte sulla figura del Primo Ministro, il quale detiene la presidenza del Consiglio di Sicurezza Nazionale (CSN), e dall'altra delega i compiti operativi ai Ministeri, differenziando le responsabilità in base agli ambiti di competenza. Attualmente vige il Regio Decreto Legislativo 14/2019, che conferisce al Governo speciali poteri di intervento sulle infrastrutture, le risorse e ogni elemento associato alle reti e ai servizi di comunicazione elettronica in caso di minaccia all'ordine pubblico o alla sicurezza nazionale. Inoltre, in Spagna è attualmente in discussione il disegno di legge sulla Cybersecurity 5G, che sembra voler subordinare l'utilizzo di un'apparecchiatura, programma o servizio 5G esterno al previo conseguimento di una certificazione prevista dal regolamento europeo sulla sicurezza informatica, mantenendo un approccio neutrale nei confronti dei fornitori.

Il **Regno Unito**, fuoriuscito dall'Unione europea, sembra spingersi sempre di più verso la sfera d'influenza statunitense, anche (e forse soprattutto) sul versante della difesa, sia fisica (si veda la recente vicenda Aukus), sia cibernetica. Per quanto concerne il secondo ambito, attualmente è in discussione in Parlamento un rafforzamento delle misure in materia di *cybersecurity*, in particolare attraverso il

Telecommunication (Security) Bill, una legge che ha l'obiettivo di riformare l'impianto di sicurezza delle reti di telecomunicazione sul territorio nazionale nell'ottica di imporre requisiti all'entrata e rigidi controlli di sicurezza. Tale proposta legislativa punta a rafforzare i poteri degli enti già esistenti, tra cui il National Cyber Security Centre (NCSC) e l'Ofcom, che otterrebbe la possibilità di richiedere ai fornitori di apparecchiature di rete di eseguire specifici test, emettere notifiche di violazione, indicare misure provvisorie per colmare lacune di sicurezza e, in caso di inadempienza, imporre sanzioni pecuniarie, mentre verrebbero spostati dal Parlamento all'Esecutivo alcuni nuovi poteri che consentono di stabilire specifici requisiti di sicurezza e codici di condotta.

Il grado di sviluppo della connettività in Europa

L'evoluzione tecnologica che ha caratterizzato gli ultimi anni e la straordinaria diffusione dei servizi digitali che è conseguita alla pandemia hanno mostrato con una forza senza precedenti quanto sia indispensabile garantire l'ampia disponibilità per cittadini, imprese e PA di reti performanti, in grado di supportare servizi digitali sempre più sofisticati e di sostenere anche repentini incrementi di traffico quali quelli registrati ovunque durante il lockdown. Nonostante il generale avanzamento del processo di digitalizzazione anche in quei Paesi, come l'Italia, che scontano un tradizionale ritardo nell'utilizzo dei servizi digitali, permangono ancora **importanti differenze** non solo, prevedibilmente, tra le diverse aree del mondo, ma anche all'interno del contesto europeo, che necessitano di essere analizzate soprattutto alla luce degli ambiziosi obiettivi di connettività fissati dall'UE e, a cascata, dai singoli Stati membri.

Rispetto alle reti fisse, posto che ormai praticamente tutti i Paesi UE hanno completato il processo di sviluppo della banda larga con la Lituania che, essendosi concentrata sul *deployment* della banda ultra-larga, si posiziona ultima con l'84,8% delle famiglie coperte, a fronte di una media europea dell'97,4% (99,6% in Italia), la domanda rivela un andamento più lento. Rispetto alla percentuale di famiglie connesse alla broadband nell'Unione, il primato spetta ai **Paesi Bassi con il 97% delle famiglie connesse alla broadband**. All'altro estremo della classifica invece troviamo Bulgaria con il 79%, seguita da Grecia (80%), Lituania e Portogallo (appaiate all'82%). Il dato italiano - **87%** - si rivela sostanzialmente in linea con quello europeo (89%). Il tasso annuo di crescita composto (CAGR, *Compound Annual Growth Rate*) dal 2012 al 2020 dei Paesi dell'Unione europea evidenzia come l'Italia, con il 5,9%, presenti un CAGR più del doppio di quello europeo, pari al 2,7%, che le consente di posizionarsi seconda nel continente. Se il dato nazionale rivela progressi incoraggianti, a livello regionale il primato nel 2020 spetta ancora una volta alla provincia autonoma di **Trento** con il 93%, seguita da Friuli-Venezia Giulia e Lazio con il 91% ed Emilia Romagna con il 90%. A chiudere la classifica regionale, invece, le regioni del Sud e in particolare Puglia e Basilicata (80%), Sicilia e Molise (78%) e Calabria (76%).

Quando alla **copertura NGA** - che comprende le tecnologie FTTH, FTTB, Docsis 3.0 e VDSL - i dati mostrano una grande maturità a livello generale, con una percentuale di copertura UE che si attesta all'87,2% e la metà degli Stati membri che registrano coperture superiori al 90%. Le percentuali inferiori riguardano Lituania e Francia dove la copertura si attesta rispettivamente al 70,8% e 69%. L'Italia, con il **92,7%** si posiziona oltre 5 p.p. al di sopra della media europea.

Sebbene il dato complessivo testimoni uno sforzo significativo nello sviluppo infrastrutturale nel nostro Paese, l'analisi della copertura con **tecnologie VHCN** (FTTH, FTTB and Cable Docsis 3.1) e **FTTP** impone maggiori cautele. La copertura con tecnologie VHCN in Italia nel 2020 è ferma al 34%, al di sotto della media europea del 59% e a

distanza siderale dai Paesi *best performer* Malta, Lussemburgo e Danimarca per i quali le percentuali di copertura si attestano rispettivamente al 100%, 95% e 94%.

Anche i dati relativi all'FTTP rilevano un ritardo del nostro Paese con una percentuale, infatti, che si ferma al **33,7%**, quasi 10 p.p. al di sotto della media europea (42,5%) e lontanissima dalle percentuali di Lettonia, Spagna e Portogallo (rispettivamente 88,1%, 84,9% e 82,3%). Si tratta di una situazione che, secondo le stime, è destinata a essere superata nel breve periodo. Infatti, le previsioni dell'FTTH Council Europe pubblicate a maggio 2021 nello studio "*FTTH/B Market Panorama in Europe*" indicano che, entro il 2026, 197 milioni di abitazioni in UE27+Uk saranno raggiunte dal FTTH/FTTB, con un incremento del 67% rispetto a quanto si stima per il 2021 (118 milioni) mentre l'Italia, dal 2020 al 2026, registrerà un **+136%**, pari a 26 milioni di case coperte dalla fibra. Questi tassi di crescita consentiranno all'Italia di posizionarsi al quarto posto nell'Europa dei 39 Paesi considerati, dopo il Regno Unito, che viaggia a ritmi del +488%, la Germania (+385%) e i Paesi Bassi (+144%).

Se nel complesso appaiono positivi i progressi in atto nel nostro Paese lato offerta, le dinamiche della domanda, al contrario, continuano a destare gravi preoccupazioni. Sebbene sia ampia e sempre crescente la disponibilità di reti di ultima generazione, **a giugno 2020 in Italia ben l'83,7% degli abbonamenti fissi concerneva ancora linee DSL**.

In linea con tale dato, la percentuale di abbonamenti in fibra (FTTH, FTTB e FTTP con esclusione di quelli FTTC) sul totale degli abbonamenti in Italia è pari al 10,1%, molto lontana dal valore OECD (30,6%) e distante anni luce da Finlandia, Portogallo e Lussemburgo, dove le percentuali si attestano, rispettivamente, al 57,3, 55,1 e 50,2%.

Rispetto al mobile, il *Mobility Report di Ericsson*, pubblicato a giugno 2021, fornisce una panoramica molto interessante dell'andamento delle **connessioni mobili nel mondo** (in particolare 5G) registrando, a livello generale, circa 8 miliardi di abbonamenti mobili di cui ben 6, alla fine del 2020, riguardavano smartphone. Tale numero continuerà a crescere, secondo le stime, per attestarsi a 7,7 miliardi nel 2026, con un peso dell'88% sul totale degli abbonamenti mobili. Lo stesso report quantifica in 160 il numero di fornitori di servizi che hanno lanciato offerte commerciali 5G e segnala una crescita degli abbonamenti con device 5G nel primo quadrimestre dell'anno di ben 70 milioni (quantificando il numero complessivo in 290 milioni) stimando, per il 2026, 580 milioni di abbonamenti 5G. Il Mobility Report calcola, poi, in oltre 60 milioni le connessioni FWA nel mondo nel 2020, stimando una crescita di circa 20 p.p. annui fino al 2026, anno in cui quando tali connessioni giungeranno quota 180 milioni. Le connessioni FWA 5G, invece, sono previste salire a 70 milioni entro il 2026. Del traffico mobile globale, quello su reti FWA si attesta al 15% alla fine del 2020 per superare, secondo le stime, il 20% nel 2026.

Rispetto alle prospettive presenti e future di sviluppo del 5G, i dati mostrano, da un lato, un buon grado di "***5G readiness***", essendo in molti casi giunte a completamento le procedure di assegnazione delle frequenze pioniere destinate al 5G, dall'altro un certo ritardo nella copertura 5G. Le uniche punte di eccellenza sono rappresentate da **Danimarca** e **Paesi Bassi**, dove la copertura è già all'80%, seguite da Austria e Irlanda con un comunque lodevole 50 e 30%, rispettivamente. Per il resto, ben 15 Paesi risultano sprovvisti di copertura 5G nel 2020, mentre l'Italia si ferma all'**8,1%**.

Mentre il processo di sviluppo delle reti 5G in Europa è ancora alle prime battute, il 3G e il 4G rappresentano, ormai, standard consolidati in

tutta l'Ue. La copertura 4G, in particolare, nel 2020 rasenta il 100% in quasi tutti gli Stati membri (99,3% in Italia), attestandosi, a livello UE, al **99,7%**.

Se i dati appena commentati dimostrano una certa omogeneità dell'offerta in tutti i Paesi UE rispetto agli standard più consolidati, lato domanda, al contrario, si registra una maggiore varietà. Guardando alle SIM attive ogni 100 persone, si passa dalle 190,3, 160,5 e 155,5 rispettivamente di Polonia, Estonia e Finlandia, alle 78,1, 76,4 e 75,2 rispettivamente di Malta, Portogallo e Ungheria. L'Italia, con 93,6, si pone al di sotto della media europea di 103,8.

Rispetto al mondo delle imprese, invece, il 62,6% delle imprese italiane rientranti nel campione hanno dotato parte del personale di *device* mobili, a fronte di una media del 69,9%.

Lo stato dell'arte del 5G a livello internazionale

Per quanto concerne il **5G**, il settore delle comunicazioni mobile è in fermento. Secondo le stime del 5G Observatory, a giugno 2021 avevano lanciato servizi 5G oltre 180 operatori a livello globale, ovvero 100 in più rispetto a giugno 2020.

In questo contesto l'Europa purtroppo non spicca, in particolare a livello di istituzioni nazionali. Infatti, lo spettro individuato a livello europeo nelle bande pioniere appare assegnato soltanto per il **45,8%**. Confrontando tale dato con quello delle altre grandi potenze economiche mondiali - mediante la normalizzazione effettuata dal 5G Observatory – rispetto alle bande in bassa frequenza, l'Europa appare seconda dietro agli Usa, che hanno assegnato tutto lo spettro individuato, mentre il Vecchio continente ha assegnato circa la metà dei 6 GHz identificati. Tra le bande medie, l'Europa figura dietro a tutti sia in termini di assegnazione, che in quelli di riserva dello spettro, laddove Cina e Stati Uniti sono i Paesi che intendono dedicare più MHz al 5G.

Nelle frequenze in banda alta, Corea del Sud e Giappone hanno assegnato quasi tutte le porzioni individuate, mentre la Cina non ha ancora assegnato nessuno degli 8.000 Mhz in banda alta e poco meglio ha fatto l'Europa, che pure ha poco più di 3.000 MHz. Infatti, a giugno 2021 la banda a 26 GHz era stata assegnata solo in Italia, in Germania, in Danimarca, in Grecia e in Slovenia.

A livello di policy, alla fine di marzo 2021 la Commissione ha pubblicato un pacchetto di strumenti per la connettività comprendente 39 casi di *best practice* proposte dagli Stati membri. La roadmap prevedeva l'approvazione di una tabella di marcia da parte di ogni Stato entro aprile 2021 e una comunicazione sullo stato di implementazione del toolbox entro aprile 2022. Scopo dell'iniziativa è facilitare la diffusione dell'infrastruttura 5G riducendo i costi e l'onere normativo.

Nel corso del 2019, in Europa il 5G ha effettuato una serie di passi in avanti, tra cui il lancio del servizio da parte di molteplici operatori, l'arrivo sul mercato dei primi smartphone compatibili e la diffusione di numerose *base station* nelle maggiori città europee. Per quanto concerne i **servizi commerciali 5G**, questi risultano attualmente disponibili in 14 Paesi europei (incluso il Regno Unito). Secondo le stime del 5G Observatory, a giugno 2020 avevano lanciato servizi 5G ulteriori 80 operatori situati nei Paesi extra-EU.

È evidente, allo stesso tempo, come il lockdown determinato dal Covid-19 abbia prodotto un rallentamento nei progressi, in particolare in Europa, sia a livello di infrastrutturazione (in particolare relativo al ritardo nella implementazione delle base station) sia a livello amministrativo. Ad esempio, è stato posticipato l'europeo di calcio 2020, che avrebbe dovuto essere il primo grande evento continentale trasmesso in 5G, e le aste per le frequenze in alcuni Paesi sono state rimandate. Tra queste

anche l'asta francese, che si è poi conclusa lo scorso 2 ottobre 2020 raggiungendo un totale complessivo di 2.786 milioni. Tali risultati collocano il Paese transalpino al terzo posto in Europa per proventi complessivi derivanti dalla gara per lo spettro 5G, dietro Italia (che però ha messo all'asta anche la banda 700 MHz) e Germania. La spesa per lo spettro è parte integrante degli investimenti nell'upgrade delle reti al nuovo standard di trasmissione, che secondo GSMA ammonteranno complessivamente a circa 900 miliardi di dollari entro il 2025. In particolare, GSMA stima oltre 250 miliardi di euro di investimenti negli Usa, circa 170 in Asia, oltre 150 in Europa e più di 160 in Cina.

La penetrazione di Internet e dei servizi digitali tra tendenze globali ed europee

Il 2020 si è caratterizzato per essere un anno all'insegna dell'accelerazione digitale. Le forti limitazioni che la pandemia ci ha imposto nell'ottica di ridurre i contagi limitando le occasioni di contatto sociale, hanno determinato il graduale trasferimento in rete di moltissime attività e l'esercizio di diritti di primaria importanza come quello al lavoro e all'istruzione, dimostrando come il canale online rappresenti un alleato indispensabile per assicurare la continuità delle relazioni sociali e delle attività economiche. Sebbene si tratti di tendenze che hanno riguardato tutte le aree del mondo, permangono ancora diversi gradi di maturità e sensibilità sia con riguardo allo sviluppo delle infrastrutture e tecnologie abilitanti i servizi digitali sia con riferimento alla fruizione di tali servizi da parte di cittadini/consumatori, imprese e PA.

Secondo il report "*Digital in 2021*", pubblicato da WeAreSocial, a livello globale, su un totale di quasi 8 miliardi di individui (7,83 miliardi per l'esattezza), **gli utenti di Internet a gennaio 2021 ammontavano a 4,66 miliardi**, pari al 59,5% della popolazione mondiale, con un incremento rispetto all'anno precedente del 7,3% (pari a 316 milioni). Dal punto di vista territoriale, se Europa e Nord America primeggiano con percentuali di utenti di Internet sul totale della popolazione che arrivano al 96% nell'Europa del Nord, esistono ancora aree del mondo – l'Africa in particolare – in cui la percentuale di penetrazione di Internet si attesta su valori decisamente molto bassi (addirittura non oltre il 26% nelle nazioni centrali africane).

Nonostante le tendenze globali dimostrino una sempre crescente penetrazione di Internet nelle abitudini degli individui, non mancano le preoccupazioni tra gli utenti circa le possibili criticità connesse all'**utilizzo online dei dati personali** e al fenomeno della **disinformazione** che trova nella rete uno strumento straordinariamente efficace di diffusione.

A tale riguardo, se la percentuale massima di utenti preoccupati per gli utilizzi dei dati personali compiuti online è del 53,9% in Portogallo, ancora più forte risulta il timore legato alla disinformazione e alle fake news, che in Brasile e Portogallo è stato espresso rispettivamente da ben l'84 ed il 75,7% degli utenti di Internet. Per quanto concerne l'Italia, i dati appaiono leggermente al di sotto della media.

Si tratta di dati importanti che vanno letti in combinato con quelli relativi ai motivi che spingono ad utilizzare Internet. Al riguardo, i dati We Are Social collocano in vetta alla classifica dei moventi per l'utilizzo di Internet la **ricerca di informazioni** (per il 63% degli utenti globali di internet), seguita dal **desiderio di stare in contatto con amici e parenti** (56,3%).

Rispetto alla variabile di base, ossia l'utilizzo di Internet, la percentuale di non utilizzo di Internet continua positivamente a ridursi, attestandosi nel 2020 al 21% in Bulgaria e al 20 e 18% in Grecia e Portogallo, a fronte del 24 e 22% del 2019. A primeggiare, come d'altronde ormai rileviamo da anni, il **Nord Europa** dove le percentuali sono

dell'1-2%. Anche rispetto all'utilizzo quotidiano di Internet, il Nord Europa primeggia all'interno dell'Unione con Danimarca, Svezia, Finlandia e Lussemburgo, dove ben il 94 e 92% degli individui ha utilizzato Internet ogni giorno. L'Italia registra un dato leggermente al di sotto della media UE (76 vs 80%).

Andando ad analizzare l'utilizzo quotidiano di Internet per fascia d'età nel 2020, emerge, prevedibilmente, una maggior convergenza verso un suo elevato utilizzo.

Rispetto al **mondo delle imprese**, premesso che l'impatto della pandemia sia sugli aspetti meramente organizzativi, sia sul modello di business è stato enorme, i dati mostrano trend diversificati. In particolare, rispetto alle imprese con elevato livello di intensità digitale, i dati evidenziano una flessione rispetto al 2019 anche nel Nord Europa, secondo una tendenza generalizzata seppur con intensità variabile di Paese in Paese, che probabilmente si spiega con la crisi economica che è conseguita allo scoppio della pandemia e che ha determinato una contrazione anche degli investimenti nella digitalizzazione e il ripiegamento, forse, verso livelli di sofisticazione digitale inferiore. Tale conclusione sembra trovare conferma nelle evidenze relative alla percentuale di imprese con un basso grado di intensità digitale che, al contrario, hanno subito un forte incremento nel 2020. **L'Italia, a tale riguardo, si posizione al secondo posto in Europa**, dopo la Svezia, con una percentuale di imprese a bassa intensità del 51%, con un incremento di ben 13 p.p. rispetto al 2019. Andando ora ad analizzare più nel dettaglio, il 73% delle imprese italiane (con almeno 10 persone impiegate e con esclusione del settore finanziario) possiede un sito web, mentre il 57%, con un mirabile +21 p.p. rispetto al 2019, ne possiede uno con funzionalità avanzate (ad esempio per personalizzare il design di un prodotto). Si tratta di numeri importanti, soprattutto il secondo, che recupera gran parte del gap rispetto alla media europea riducendolo a solo 4 p.p. a fronte dei 21 del 2019.

Andando a verificare i dati di utilizzo di alcuni servizi digitali, emerge a pieno il ritardo italiano. Ssiamo penultimi nella classifica europea per utilizzo dei social network (48% degli individui contro il 57% a livello UE), ci posizioniamo terzultimi nell'*e-commerce* (44% degli individui che acquistano online a fronte del 65% a livello UE) e quartultimi per ricorso all'*Internet banking* (39% degli individui contro il 58% a livello UE).

Rispetto ai servizi di ***e-government***, emerge rispetto all'offerta una diversa tendenza: da un lato, l'offerta di servizi pubblici digitali per i cittadini risulta al di sotto della media (69% vs 75%); dall'altro, rispetto al mondo delle imprese, l'offerta di servizi digitali, con l'89% si colloca al di sopra del dato UE dell'84%. Lato domanda, invece, sebbene sia ancora grave il ritardo rispetto alla media europea, si registra un fortissimo incremento nell'utilizzo del **Sistema Pubblico di Identità Digitale SPID**: da gennaio a settembre 2021, infatti, sono circa 374 milioni gli accessi con SPID ai servizi online pubblici e privati. I primi nove mesi del 2021 hanno visto un massiccio uso dell'identità digitale tale da superare il totale degli accessi del biennio precedente: 143,9 milioni nel 2020 e oltre 55 milioni nel 2019. L'accelerazione ha riguardato anche il numero di amministrazioni che utilizzano SPID, cresciuto del 70%, superando gli 8.308 enti (dato del 3/10/2021), il doppio rispetto a ottobre 2020. Alle amministrazioni si aggiungono poi 53 fornitori privati che consentono l'uso di SPID per usufruire dei propri servizi.

L'I-Com Broadband Index (IBI): gli effetti della pandemia e degli investimenti nel 5G

L'**IBI** sintetizza i dati relativi allo sviluppo digitale contenuti all'interno dello studio e misura la maturità digitale dei Paesi europei. Dal punto di vista metodologico, oltre alla versione

complessiva, si mantiene la suddivisione nella duplice versione IBI lato offerta e IBI lato domanda.

In testa alla classifica sono sempre i Paesi dell'Europa settentrionale, con un avvicendamento tra Danimarca e Svezia: la prima guadagna il primo posto a spese della seconda, grazie in particolare alla capillarità della copertura della rete 5G, già pari all'80% (solo il 14% per la Svezia).

Una delle novità di questa edizione dell'indice, che hanno parzialmente rimescolato le carte, è proprio la copertura della rete mobile di ultima generazione: sono ancora pochi i Paesi che hanno investito sotto questo profilo e quelli che lo hanno fatto in maniera consistente guadagnano ampio terreno. È il caso della Danimarca, ma anche dei Paesi Bassi (80%) e dell'Austria (50%).

La performance danese è spiegata, comunque, anche da una buona copertura delle reti fisse fiber-to-the-premises (FTTP) e dall'elevato grado di sviluppo della domanda digitale.

L'Italia, sul fronte 5G, pur essendo uno dei 13 Paesi con una copertura positiva della rete 5G, resta **al di sotto della media**, per via della presenza di pochi Paesi con una copertura altissima. Questo dato, unitamente a quello della rete fissa FTTP, anch'esso al di sotto della media europea e, soprattutto, con un ritardo rispetto al resto d'Europa che, anziché ridursi, si amplia (da 3,7 p.p. a 8,8 p.p.), porta a un rallentamento sul fronte dell'offerta digitale.

Ciononostante, l'Italia guadagna due posizioni rispetto alla scorsa edizione, piazzandosi al 20° posto. A dispetto di un rallentamento sul piano dell'offerta, si registra, finalmente, un **segnale positivo sul fronte domanda**. L'Italia è, per la prima volta, al di sopra della media UE nel grado di penetrazione della banda larga ultra veloce, con quasi il 47% degli abbonamenti in banda larga che prevedono una velocità almeno pari a 100 Mbps: un dato cresciuto di oltre 11 p.p. (+7,2 p.p. per l'UE), elemento che le ha consentito di superare la media UE di 2,2 p.p. Si tratta, senza dubbio, dell'effetto Covid-19, che è il secondo dei fattori di novità sopra citati. La pandemia ha portato molte famiglie, prima "*disinteressate*", a equipaggiarsi con un servizio di connettività a elevate prestazioni per poter continuare a svolgere attività prima svolte prevalentemente fuori casa.

A stupire è, invece, il dato relativo all'*e-commerce*, abitudine di solo il **44%** degli italiani e solo +6 p.p. rispetto all'anno precedente, rimanendo ben al di sotto della media UE (65%), nonostante il 2020 sia stato un anno particolare, caratterizzato da frequenti e prolungati lockdown, soprattutto in Italia nella prima metà dell'anno (ricordiamo che i dati sono aggiornati a giugno 2020).

Grazie alle dinamiche descritte, la posizione che l'Italia guadagna sul piano della domanda – piazzandosi 22° e riducendo di 6 punti il divario rispetto all'apice della classifica - viene, invece, persa sul piano dell'offerta, dove il nostro Paese si colloca al 16° posto, presentando un maggior divario rispetto al miglior Paese europeo.

Si registra, in generale, un'inversione di tendenza nel processo di convergenza tra Paesi: migliora per quanto riguarda la domanda di digitale, risultando ridotto il divario tra il primo e l'ultimo Paese nella graduatoria generale, e peggiora quello relativo all'offerta, aumentando la distanza tra migliore e peggior Paese di 10 p.p.

La correlazione positiva (e pari al 60%) tra il grado di interazione online con la PA e l'indice IBI lato domanda lascia immaginare che un sostegno alla domanda digitale, volto a rafforzare e accelerare il processo di convergenza tra Paesi sul piano della domanda, possa venire dal **settore pubblico**. In particolare, a un 10% in più di cittadini che utilizzano i servizi pubblici digitali è associato, in

media, un punteggio IBI lato domanda superiore di circa 3,4 punti. Dall'altro lato, un miglioramento appare necessario, in quanto la domanda digitale rappresenta un importante input dei processi di avanzamento tecnologico che caratterizzeranno il futuro della nostra società, quale l'Intelligenza Artificiale (IA): la relazione positiva tra domanda digitale e investimenti in IA mostra come a un punteggio IBI lato domanda superiore di 10 punti sia associato, in media, un investimento pro-capite di 6,5 euro in più.

Parte 2: La nuova strategia digitale per il rilancio dell'Italia

Le iniziative nazionali a sostegno della digitalizzazione

In attuazione del dispositivo RRF che richiede agli Stati membri di presentare un pacchetto di investimenti e riforme, il 25 aprile scorso il Governo ha presentato il **Piano Nazionale di Ripresa e Resilienza (PNRR)** - definitivamente approvato il 13 luglio scorso con decisione di esecuzione del Consiglio - che si articola in sei Missioni e 16 Componenti. Le sei Missioni del Piano, in particolare, sono: digitalizzazione, innovazione, competitività, cultura e turismo; rivoluzione verde e transizione ecologica; infrastrutture per una mobilità sostenibile; istruzione e ricerca; inclusione e coesione; salute.

Per quanto concerne le risorse assegnate a missioni e componenti del PNRR, alla missione n. 1, digitalizzazione, innovazione, competitività, cultura e turismo, sono state assegnati 40,32 miliardi di euro, di cui 9,75 miliardi per digitalizzazione, innovazione e sicurezza nella PA, 6,68 per turismo e cultura 4.0 e 23,89 per digitalizzazione, innovazione e competitività nel sistema produttivo. In tale segmento, in particolare, si collocano le iniziative relative alle infrastrutture (investimento 3: Reti ultraveloci).

Partendo dagli obiettivi fissati dalla nuova strategia europea **Digital Compass** che si prefigge di garantire entro il 2030 una connettività a 1 Gbps per tutti e la piena copertura 5G delle aree popolate, il Piano fissa obiettivi ancora più ambiziosi in termini di tempistiche, prevedendo connessioni a 1 Gbps su tutto il territorio nazionale entro il 2026. Quanto all'impiego delle risorse, il Piano ha stanziato fondi per portare la connettività a 1 Gbps a circa 8,5 milioni di famiglie, imprese ed enti nelle aree grigie e nere NGA a fallimento di mercato, nel rispetto del principio della neutralità tecnologica, per completare il **Piano "*Scuola connessa*"**, teso a garantire la connessione in fibra a 1 Gbps ai 9.000 edifici scolastici rimanenti (pari a circa il 20 per cento del totale), assicurare connettività da 1 Gbps fino a 10 Gbps simmetrici agli oltre 12.000 punti di erogazione del Servizio sanitario nazionale (**Piano "*Sanità connessa*"**), munire 18 isole minori di un *backhauling* sottomarino in fibra ottica (**Piano "*Collegamento isole minori*"**) ed incentivare lo sviluppo e la diffusione dell'infrastruttura 5G nelle aree mobili a fallimento di mercato (**Piano "*Italia 5G*"**).

Rispetto al **Piano Italia 1 Giga**, la soglia minima di intervento è stata fissata a 300 Mbps (in download) - con un innalzamento rispetto ai 100 Mbps previsti inizialmente dalla Strategia formulata a maggio - ritenuta necessaria e sufficiente per raggiungere, entro il 2026, l'obiettivo di connettività ad almeno 1 Gbps definito nel Digital Compass.

Per la tecnologia **Fixed Wireless Access (FWA)**, il Piano distingue utenti raggiunti, ovvero "*passed*" e utenti effettivamente serviti o "*served*" e ritiene ragionevole, in attesa di compiere comunque ulteriori approfondimenti, applicare il **criterio del 10%**, che consiste nel considerare effettivamente serviti con tutta la banda richiesta circa il 10% degli utenti coperti dalle celle elettromagnetiche (o "*passed*"). Rispetto al modello di intervento, la proposta contenuta nel Piano punta a un modello "*ad incentivo*" (o *gap funding*) in cui le risorse

previste dal PNRR per il medesimo Piano Italia 1 Giga vengono assegnate a seguito di bandi per le aree risultate a fallimento di mercato (ai quali gli operatori possono presentarsi sia in forma individuale che associata), in forma di contributo pubblico determinato come percentuale massima sul costo complessivo delle opere che - in discontinuità rispetto a quanto previsto per le aree bianche – sono e restano di proprietà dell'operatore privato. Tali risorse vengono sbloccate solo a seguito del raggiungimento da parte dell'operatore di una soglia base di copertura.

Per quanto riguarda il **Piano Italia 5G**, le risorse assegnate, 2 miliardi di euro, sono relative a tre voci principali: 1) la copertura di 10 mila chilometri di strade extraurbane per la realizzazione del *backhauling* in fibra (600 milioni di euro); 2) i corridoi di trasporto europei (420 milioni di euro), con l'obiettivo di incentivare lo sviluppo di servizi e applicazioni 5G dedicate a sicurezza stradale, mobilità, logistica e turismo; 3) il potenziamento della rete mobile nelle aree a fallimento di mercato, ovvero quelle zone del Paese in cui gli operatori non hanno interesse a investire (1 miliardo di euro). La realizzazione della mappatura, alla data del 31 maggio 2021, i cui esiti sono in attesa di pubblicazione, è stata affidata ad Infratel, la quale ha indetto una consultazione pubblica a partire dal 10 giugno 2021 (con scadenza 26 luglio), nell'ambito della quale gli operatori sono stati chiamati a presentare i propri piani per i prossimi 5 anni.

Dal perimetro di sicurezza cibernetica alla nascita dell'Agenzia per la cybersicurezza nazionale. L'ecosistema italiano della cybersecurity

Il processo di sviluppo delle infrastrutture non necessita soltanto di risorse ma anche di certezza normativa ed elevati standard di **sicurezza**.

A tale riguardo, il percorso intrapreso dal nostro Paese si sta caratterizzando per una serie di iniziative tese, da un lato, alla semplificazione delle procedure necessarie per realizzare le reti (da ultimo con il D.L. 77/2021, convertito con modificazioni dalla Legge 29 luglio 2021, n. 108, c.d. decreto Semplificazioni bis) con particolare attenzione per fibra e 5G e, dall'altro, a costruire un ecosistema normativo a tutela della **cybersecurity**.

A tale riguardo, seppur con ritardi e difficoltà derivanti anche dalla necessità di dedicare massima attenzione al contrasto della pandemia, è in dirittura d'arrivo (mancando all'appello solo un DPCM) la complessa procedura, composta da 5 DPCM e un regolamento governativo di esecuzione, disegnata dal decreto legge n. 105/2019 (convertito con la legge n. 133/2019), per garantire la piena operatività del **perimetro di sicurezza nazionale cibernetica**.

Rispetto al sistema di governance che sovrintende il sistema della sicurezza in Italia, con la legge n. 109 del 4 agosto 2021 che ha convertito il D.L. n. 82/2021 è stata istituita l'**Agenzia per la cybersicurezza nazionale**. Si tratta di un intervento straordinariamente rilevante che, partendo dalla constatazione della centralità assunta dal canale digitale, della crescente e sempre più sofisticata minaccia di attacchi informatici e della estrema complessità del quadro normativo e regolamentare, frutto di una serie di interventi che si sono andati a susseguire - in maniera a volte anche poco organica - negli anni disseminando tra diverse autorità competenze in materia di cybersecurity, persegue una chiara e condivisibile finalità di riordino della materia, attraverso la concentrazione presso un unico soggetto, la neoistituita Agenzia, di tutte le competenze in materia.

Le infrastrutture digitali italiane. Copertura attuale e roll-out della banda ultralarga al 2026

Tra le risorse stanziate nell'ambito del PNRR, 6,7 miliardi di euro sono riservati a 7 progetti che

costituiscono la presente Strategia per la banda ultralarga, in continuità con la Strategia varata nel 2015 e con le iniziative precedenti volte ad incentivare domanda e offerta di servizi di connettività. Sulle reti fisse il principale è il **Piano "*Italia a 1 Giga*"**, che punta a fornire connettività a 1 Gbps in download e 200 Mbps in upload nei numeri civici ubicati nelle aree grigie e nere NGA che, al 2026, non sarebbero raggiunti da connessioni in download ≥300 Mbps.

Al fine di impiegare al meglio le risorse stanziate, il Governo ha assegnato a Infratel il compito di effettuare una nuova consultazione, della quale sono stati pubblicati i dati di copertura al 2026, ma non ancora quelli relativi allo stato della copertura attuale. In assenza di tali dati, un'indicazione di massima può essere estrapolata da quelli contenuti nella ***broadband map*** dell'AGCOM, che mostra lo stato di copertura in termini di famiglie raggiunte. Così calcolata, **la copertura in fibra con reti FTTP (Fiber To The Premise) raggiunge il 34% delle famiglie**. La copertura migliore si ha in **Lazio** (50%), la più bassa in Calabria (10%). Si fa ancora troppo affidamento sull'ADSL in Valle d'Aosta, dove poco più della metà delle famiglie possono contare sulla fibra (FTTC o FTTP), e in Trentino Alto Adige e Molise, dove circa un quarto delle famiglie beneficia solo di quella tecnologia. A livello provinciale, tecnologie a ≥100 Mbps raggiungono almeno l'80% solo Siracusa, Taranto, Trieste, BAT, Roma e Palermo. La copertura in FTTP è ancora appannaggio di pochi, in particolare presso le famiglie di Mantova (77%) di Trieste (76%), Prato (71%), Genova (69%), Milano (65%), Roma (63%) e Napoli (61%).

Per quanto concerne le coperture che – senza le risorse del PNRR - si realizzerebbero nel 2026, il 71% del territorio nazionale beneficerà di una rete con velocità superiore a 300 Mbps, prevalentemente costituita da rete a velocità superiore a 1 Gbps (68%). Il restante 29% del territorio sarà oggetto di intervento.

La prima regione per copertura ad almeno 1 Gbps sarebbe il **Friuli Venezia Giulia** (84%), seguita da Sicilia (79%), Trentino Alto Adige (78%) e Liguria (76%) mentre tra le regioni del Sud solo Puglia (72%) e Molise (71%) figurerebbero al di sopra della media nazionale (68%). In Sardegna e Abruzzo non sarebbe coperto, al 2026, nemmeno la metà del territorio, e la copertura tra i 300 Mbps e 1 Gbps sarebbe pari ad appena il 2%. La fotografia provinciale segnala un'elevata diffusione (maggiore dell'80%) della rete ultra-veloce (≥300 Mbps) in alcune province lombarde e del Nord Est. Per quanto riguarda la copertura alla velocità massima (≥1 Gbps) presentano un dato superiore all'80% gran parte delle province del Nord Est, tra cui Bolzano (87%), Udine (87%), Trieste (83%) Gorizia (82%) e Treviso 81%). Tra le grandi province figurano Palermo (86%), Bari (84%), Cagliari 84%) Genova (83%) e Roma (81%). Nelle province di Oristano, Nuoro, Sud Sardegna, stante la fotografia attuale, l'intervento riguarderà all'incirca 3 civici su 4 mentre nelle aree di Chieti, Vibo Valentia, Sassari, L'Aquila, Catanzaro, Teramo e Potenza l'intervento riguarderà tra il 40% e il 50% degli indirizzi.

Per quanto concerne le **aree bianche**, a fine agosto 2021 sono stati emessi quasi 5.000 ordini di esecuzione per le infrastrutturazioni in fibra FTTH, di cui oltre 3.000 risultano chiusi, ovvero con CUIR, a fronte di oltre 2.000 interventi completati. Per i cantieri FWA si osservano quasi 2.200 ordini emessi, di cui oltre 1.900 con CUIR. L'avanzamento economico del progetto a livello nazionale ha raggiunto attualmente circa il 70% in termini di avanzamento dei lavori, con 1,09 miliardi di euro impiegati su oltre 1,5 miliardi di lavori ordinati a Open Fiber.

Per la **copertura ad almeno 300 Mbps**, il Piano Italia 1 Giga fa riferimento anche al **Fixed Wireless Access (FWA)**, che costituisce un'alternativa più economica e flessibile in particolare per le zone dove non è presente una rete cablata fino a casa dell'utente o in cui sarebbe anti-economico

costruirla. A livello di copertura, i dati riportati da AGCOM indicano che **gli operatori FWA coprono circa il 74% delle famiglie italiane**, in particolare nel Nord Italia. A livello di abbonamenti il FWA è arrivato a servire quasi il 10% del totale delle utenze broadband attive in Italia (8,7% a marzo 2021). La natura ibrida della *tecnologia fixed-wireless* ha introdotto un ulteriore elemento di valutazione all'interno della consultazione del 2021. Nel Piano Italia a 1 Giga si parla di differenza tra utenti raggiunti, ovvero "*passed*", e utenti effettivamente serviti o "*served*", ritenendo ragionevole applicare il **criterio del 10%**, che consiste nel considerare effettivamente serviti con tutta la banda richiesta circa il 10% degli utenti coperti dalle celle elettromagnetiche (o "*passed*"). Dalla consultazione è emerso che, nel 2026, i civici coperti in modalità FWA con capacità ≥300 Mbps arriverebbero a quota 560.000. Allo stato attuale, il Piano sembra prevedere un contributo del Fixed Wireless alla connettività a 300 Mbps pari al 10% dei civici coperti, in attesa degli ulteriori sviluppi e verifiche.

Le reti mobili e l'importanza del 5G

Secondo i dati AGCOM, connettività 3G e 4G hanno da tempo raggiunto oltre il 98% della popolazione. Discorso più complesso per il 5G, rispetto al quale, oltre ad apposite iniziative e stanziamenti di risorse previste nell'ambito del PNRR, nella nuova "*Strategia italiana per la banda ultralarga*" e nel Piano "*Italia 5G*", quest'ultimo ha previsto anche una consultazione *ad hoc* per verificare lo stato delle reti, i cui esiti, al momento della scrittura, non risultano ancora pubblicati. In assenza di dati ufficiali, si riportano i risultati dell'analisi di EY, secondo cui, **a settembre 2021, la copertura 5G avrebbe raggiunto il 95% della popolazione italiana e oltre 7.500 comuni**. Questa tipologia di copertura è effettuata in gran parte con tecnologia 5G NSA (*non stand alone*), un ibrido tra la vecchia rete core 4G e la nuova rete di accesso 5G. A livello di operatori, Wind dichiara una copertura della popolazione in 5G NDA superiore al 95.4% in DSS e del 38% in modalità 5G TDD in banda 3.6 GHz. Vodafone è presente attualmente in 25 città italiane e punta a raggiungere circa 50 città entro la fine del 2021. Iliad copre alcune aree di 27 città, mentre TIM ha dichiarato per il 2021 un sensibile ampliamento della copertura in modalità SA (stand alone) in oltre 20 città. Anche Linkem ha lanciato un servizio 5G commerciale completamente stand alone in tecnologia FWA su frequenze a 26 GHz.

In questo contesto, una chiara mappatura della copertura 5G è fondamentale per due ragioni: individuare le aree cui destinare i fondi a supporto delle aree a fallimento di mercato e, in secondo luogo, favorire il pieno dispiegamento della copertura 5G SA (*stand alone*), poiché solo questa può garantire il conseguimento di tutti i benefici collegati alla sua diffusione, in particolare provenienti dalle c.d. *industrie verticali*.

Per quanto riguarda il primo aspetto, al Piano "*Italia 5G*" sono stati destinati complessivamente 2,02 miliardi di euro, di cui 1 miliardo per la copertura delle aree a fallimento di mercato.

Rispetto ai benefici, GSMA stima una crescita a livello mondiale di circa 2,2 trilioni di dollari tra il 2024 e il 2034, di cui 565 miliardi provenienti dall'utilizzo delle bande sopra i 24 GHz. Le applicazioni che si prevede generino il maggior contributo sono l'automazione industriale, il controllo da remoto dei dispositivi e la realtà virtuale, mentre a livello settoriale, le stime indicano che i maggiori benefici dovrebbero provenire dalla manifattura e dalle utilities (215 miliardi di dollari), dai servizi professionali e finanziari (141 miliardi) e dai servizi pubblici (96 miliardi).

Tuttavia, tale orizzonte di lungo termine non deve far pensare che i tempi non siano sono stringenti. Secondo la ricerca condotta da Interdigital, su 345 professionisti della filiera delle comunicazioni mobili e dei vertical, oltre il 70% intende utilizzare

applicazioni 5G industriali entro due anni. In particolare, poco più di un'impresa su 10 ne fa già uso (12%), circa una su 3 le adotterà entro 12 mesi (32%) e un ulteriore 28% entro 24 mesi.

Per favorire al massimo lo sviluppo dei verticali e il raggiungimento dei benefici auspicati assumono un'importanza centrale i **modelli di business** che prevarranno nell'implementazioni delle nuove applicazioni 5G a livello industriale. È verosimile che la gestione delle nuove reti si focalizzi su un modello in cui la copertura potrebbe divenire sempre più localizzata, destinata a servire imprese o distretti industriali e l'integrazione di reti private aziendali, e con business model primariamente B2B focalizzati sulle applicazioni industriali. Nel progressivo affiancamento tra reti pubbliche e reti private potrebbero emergere diverse soluzioni e modelli di business, che vanno dalla fornitura delle applicazioni industriali da parte degli stessi operatori, da soli o in partnership con terze parti che utilizzano la rete, o con le stesse imprese dei verticali, fino alla creazione e gestione di reti private per le aziende fornite da intermediari o sviluppate in proprio dalle aziende stesse su porzioni di spettro riservato, passando per altre tipologie di modelli ibridi. Proprio al fine di consentire maggiore flessibilità nella gestione dello spettro e dell'affermazione tali nuovi modelli, Paesi come Germania e Regno Unito hanno già previsto policy *ad hoc*, che prevedono l'assegnazione di spettro locale, accesso condiviso e *light licensing*. In Italia, d'altra parte, lo sviluppo di un modello di offerta (o gestione) localizzato potrebbe incontrare delle difficoltà, per via dell'alto costo di assegnazione dei diritti d'uso delle frequenze 5G raggiunto nel Paese e la scarsa domanda di servizio dovuta al tessuto industriale italiano, composto in prevalenza da PMI. A tal proposito, PNRR e Strategia indicano la volontà del Governo di sostenere la domanda di connettività 5G attraverso l'erogazione di **incentivi** per l'adozione di servizi e applicazioni 5G, anche a favore dei settori verticali per lo sviluppo di casi d'uso previsti dall'ITU, inclusi i settori pubblici della sanità, scuola, mobilità e sicurezza. Parallelamente, l'AGCOM ha avviato un'indagine conoscitiva su possibili nuove modalità di utilizzo dello spettro radio per favorire lo sviluppo dei verticali, inclusa la possibilità di riservare porzioni di spettro 5G per reti locali e reti private.

Fintech

Tra i principali *driver* della rivoluzione digitale, un ruolo da protagonista assoluto sarà giocato nei prossimi anni dal Fintech, settore nel quale nei primi sei mesi del 2021 gli investimenti, dopo la flessione dovuta alla crisi pandemica, hanno ricominciato a crescere a ritmo elevato, raggiungendo il valore annuale del 2020, e triplicato il capitale investito nel primo semestre dell'anno precedente (34,4 miliardi di dollari). Le prime dieci società del settore a livello globale hanno un valore superiore ai 2,1 trilioni di dollari. Osservando la classifica, è però possibile notare che a primeggiare sono le società statunitensi, che cubano il **62,5%** della capitalizzazione totale e cinesi (20,5%), mentre l'Europa ha un peso marginale (8,5%).

La trasformazione digitale sta coinvolgendo profondamente anche il **mondo bancario**. Infatti, negli ultimi anni, accanto agli istituti di credito tradizionali, che hanno avviato un processo di digitalizzazione della maggior parte delle proprie attività cercando di offrire ai propri clienti un'esperienza omnichannel, sono nate le cosiddette ***digital bank***, ovvero banche che non hanno una presenza fisica sul territorio ma operano esclusivamente sui canali digitali. Ad ottobre 2020 le dieci principali banche digitali al mondo hanno raccolto complessivamente capitali per oltre 5,6 miliardi di dollari. La tendenza ad avvicinarsi al mondo delle banche digitali, dopo la diffusione del Covid-19, probabilmente anche a causa delle limitazioni alla circolazione e al funzionamento contingentato delle filiali bancarie, è esplosa portando nel 2020 il numero di clienti italiani a 2,37 milioni, con un ulteriore

crescita del 33% prevista per il 2021.

In forte crescita anche i pagamenti digitali che nel 2020 in Italia hanno transato circa 268 miliardi di euro, con una lieve decrescita (-2 miliardi) rispetto all'anno precedente. Il dato, anche se negativo, è comunque estremamente incoraggiante visti i 123 miliardi di euro di consumi totali persi nel 2020 a causa della crisi pandemica. Nel primo semestre del 2021 i pagamenti digitali nella penisola si sono assestati sui 146 miliardi, in netta crescita rispetto allo stesso periodo sia del 2020 (+19%) che del 2019 (+14%). Una forte crescita si è registrata anche nell'utilizzo dei sistemi di pagamento più innovativi come il *contactless* e i *mobile & wearable payment*. Il valore dei pagamenti senza contatto effettuati nei negozi fisici nel primo semestre 2021 (52,1 miliardi di euro) è stato quasi il doppio di quello registrato nel 2019 (27,2 miliardi) e circa il 40% in più rispetto al 2020 (31,4 miliardi). Per quanto riguarda i *mobile & wearable payment*, anche se in valori assoluti i pagamenti nel 2021 hanno raggiunto solo i 2,7 miliardi, è importante sottolineare una crescita del 52% rispetto all'anno precedente e del 74% rispetto al 2019.

Altro ambito del Fintech che sta vivendo una forte fase di crescita è quello delle criptovalute. L'ecosistema delle criptocurrency conta ad ottobre 2021 6.823 monete per una capitalizzazione totale di oltre 2.343 miliardi di dollari. La mancanza di un'autorità centrale, se da una parte rende il sistema più libero e democratico, dall'altro espone le criptovalute ad un'eccessiva volatilità, infatti, la mancanza di un soggetto in grado di intervenire, ad esempio attivando azioni utili a calmierare le oscillazioni, di fatto lascia l'andamento della moneta completamente in balìa delle dinamiche di mercato. Osservando l'andamento del BitCoin negli ultimi dieci anni risulta evidente come il valore della criptovaluta sia caratterizzato da una volatilità estrema. Nel solo periodo che va dal 11 ottobre 2020 allo stesso giorno del 2021 si sono palesate variazioni giornaliere sia positive che negative fino al 19%.

Nonostante questa criticità numerosi Paesi stanno guardando con interesse al mondo delle criptovalute. Lo Stato centramericano di **El Salvador** è stato il primo a scegliere di utilizzare il BitCoin come valuta di corso legale.

Se l'utilizzo di una criptovaluta commerciale come moneta corrente sembrerebbe essere ad oggi eccessivamente rischioso per la solidità economica dei Paesi occidentali, numerosi Stati stanno cominciando a studiare la possibilità di emettere una valuta digitale di stato. Il Paese che attualmente è più avanti su questo tema e ha già iniziato la sperimentazione della propria moneta digitale è la Cina. La sperimentazione dello yuan digitale è stata avviata dalla Banca Centrale Cinese a partire dal mese di aprile del 2021 in 4 città (Shenzhen, Chengdu, Suzhou e Xiongan) e dovrebbe chiudersi entro il 2023 per poi vedere il lancio ufficiale della moneta in tutto il paese tra il 2024 e il 2025.

Le tecnologie emergenti

Intelligenza Artificiale

Nonostante viaggi ancora su cifre inferiori rispetto al resto d'Europa e soprattutto alle grandi potenze del settore, il **mercato italiano dell'intelligenza artificiale (IA)** ha mostrato resilienza durante l'emergenza sanitaria e tanti sono stati i progetti e le iniziative implementate in Italia per affrontare la crisi Covid-19. Soluzioni IA sono state pensate non solo per la diagnosi e predizione degli sviluppi clinici della malattia causata da SARS-CoV-2, oppure per la ricerca in ambito farmaceutico ma anche per combattere la disinformazione su Covid-19, oppure nel marketing per migliorare la *customer engagement* durante la pandemia e continuare a garantire esperienze e comunicazioni efficaci secondo le aspettative degli utenti. Questo interesse, si può dire oramai consolidato, è

testimoniato anche dalla crescita del mercato che, stando ai dati dell'Osservatorio Artificial Intelligence del Politecnico di Milano, nel 2020 ha registrato un incremento del 15% rispetto al 2019 e raggiunto un valore di 300 milioni di euro, di cui il 77% commissionato da imprese italiane (230 milioni) e il 23% come export di progetti (70 milioni).

A trainare il mercato è soprattutto la componente dei software, che vale il 62%, seguita dai servizi e marginalmente dalla componente hardware.

Questa nuova frontiera tecnologica è dunque una leva fondamentale per accelerare la crescita digitale dell'Italia, con benefici che riguardano non solo il mondo industriale ma la società nel suo complesso. Tuttavia, nel PNRR si parla poco di intelligenza artificiale e sembra mancare alla base una strategia complessiva, che indichi come il Paese intenda sfruttarne le potenzialità a 360°per ripartire nella fase post-Covid e anche la **Strategia Nazionale per l'Intelligenza Artificiale**, la cui elaborazione si sarebbe dovuta concludere nel 2019, non ha ancora visto la luce a più di due anni di distanza dalla scadenza prevista.

Blockchain

La **blockchain** costituisce un altro ambito di sviluppo interessante a livello nazionale. Gli investimenti globali in questa tecnologia, secondo un'analisi condotta da IDC, dovrebbero attestarsi sui 6,6 miliardi di dollari nel 2021 e sono destinati a crescere nel prossimo triennio fino a raggiungere i 19 miliardi nel 2024. **Nel 2020 gli investimenti italiani in blockchain si sono attestati sui 23 milioni di euro**, in leggera discesa rispetto ai 30 milioni del 2019. L'effetto di questa flessione è probabilmente addebitabile solo in parte alla crisi pandemica, infatti, con il dissolversi dell'*hype* mediatico che ha caratterizzato questa tecnologia nel 2019, gli innumerevoli annunci, diminuiti del 80%, hanno lasciato il passo ai soli progetti che potevano avere effettivamente un futuro. Questa tesi trova riscontro anche nel monitoraggio effettuato dall'Osservatorio sullo stato di avanzamento dei progetti blockchain sviluppati in Italia. Il 60% degli investimenti effettuati in Italia su questa tecnologia nel 2020 è stato destinato a iniziative già in fase operativa, il 28% a progetti pilota, l'11 % a *proof of concept* e solo l'1% a progetti di formazione.

Cloud Computing

La strategicità del **cloud**, una delle principali piattaforme abilitanti, viene evidenziata anche dalla centralità che le viene assegnata nel quadro del PNRR, che gli assegna 1 miliardo di euro in termini di abilitazione e facilitazione della migrazione e 600 milioni per la digitalizzazione delle grandi amministrazioni centrali, che dovrà seguire un approccio "*cloud first*". A livello di mercato, secondo i dati forniti dal Politecnico di Milano, nel 2020 il cloud ha superato quota 3,34 miliardi, mostrando una crescita del +21% YoY.

Sul piano delle policy, la pubblicazione della **nuova Strategia nazionale sul cloud**, pur non dando formalmente avvio alle attività implementative, ha chiarito alcuni fondamentali aspetti della posizione governativa. Il modello si basa su 3 gambe: la classificazione dei dati e dei servizi; la qualificazione dei servizi cloud; il polo strategico nazionale. In particolare, dati e servizi di grado diverso verranno essere affidati a *provider* che garantiscono livelli di sicurezza diversi. I **cloud pubblici non criptati**, pur se qualificati, potranno ospitare solo dati e servizi ordinari, mentre i servizi di **cloud pubblico criptato**, privato/ibrido su licenza e privato qualificato potranno ospitare dati e servizi sia critici che ordinari. Quelli strategici potranno essere localizzati solo sugli ultimi due. Secondo la pianificazione italiana questo processo dovrà culminare nella realizzazione di un nuovo *marketplace* che guidi le pubbliche amministrazioni nella scelta e nell'acquisto del

servizio cloud più adatto alle proprie esigenze.
Il PSN previsto dal piano italiano dovrà offrire garanzie di affidabilità, resilienza e indipendenza. Verrà gestito da un fornitore identificato sulla base di opportuni requisiti tecnico-organizzativi, che sarà tenuto a garantire il controllo sui dati in conformità con la normativa in materia, e offrirà sia servizi di cloud pubblico criptato (IT), sia tutta la gamma di servizi cloud privato/ibrido (cloud privato/ibrido su licenza e il cloud privato qualificato). Allo scadere di settembre 2021, così come auspicato dal Ministro Colao, sono pervenute due proposte per la realizzazione e la gestione del **Polo Strategico Nazionale per il cloud**, da parte di due cordate. Una **proposta di partenariato pubblico-privato** per la creazione del Psn proviene dalla cordata costituita da TIM (45%), Leonardo (25%), CDP (20%) e Sogei (10%). Un'altra **proposta per la realizzazione e gestione del Polo Strategico Nazionale** è stata presentata dalla cordata Almaviva-Aruba, sempre in regime di partenariato pubblico-privato. In termini di tempistiche, il documento pubblicato individua tre fasi: entro il 2021 è prevista la conclusione della cosiddetta "*Fase 1*", ovvero la pubblicazione del bando per la realizzazione del PSN. La Fase 2, che si sostanzia nell'aggiudicazione e nella realizzazione fisica del PSN, dovrà finire entro il 2022. Infine, la Fase 3 prevede la migrazione di tutto l'ecosistema IT della PA italiana in cloud entro il 2025.

Nonostante il piano sia apprezzabile per chiarezza e sinteticità rispetto ai tradizionali *benchmark* italici, rimangono almeno tre dubbi principali.

Innanzitutto, la classificazione dei dati si richiama esplicitamente all'esperienza del Regno Unito, dove la *Data Classification Strategy*, basata su tre livelli di sicurezza, ha distinto informazioni classificate come "*secret*" e "*top secret*" dalle cosiddette "*official*". Il risultato è che le prime due categorie corrispondono a non più del 5% del totale dei dati in possesso della pubblica amministrazione britannica. Che ha dunque adottato un criterio realmente selettivo, lasciando la stragrande maggioranza dei dati al mercato e al cloud pubblico, più performanti sia sotto il criterio tecnologico che economico. È legittimo chiedersi se la PA italiana saprà fare lo stesso. È chiaro che dovranno essere stabiliti criteri stringenti, validati *ex post*. In questo senso, preoccupa che le amministrazioni centrali che dovranno occuparsene siano oggi ampiamente sottodimensionate (il Dipartimento per la trasformazione digitale) oppure addirittura nascenti (l'Agenzia per la cybersicurezza nazionale).

Inoltre, il fatto che anche per i dati ordinari la Strategia consigli le pubbliche amministrazioni centrali di adottare il cloud pubblico criptato con chiave di accesso in Italia appare un criterio forse troppo sbilanciato verso le ragioni della sicurezza, laddove evidentemente occorre tenere conto in maniera sufficientemente equilibrata del *trade-off* con la competitività.

Infine, non è chiaro se il Polo Strategico Nazionale si sostituirà di fatto al *marketplace* per le tre tipologie di servizio che fornirà oppure ne avrà solo una quota parte (con l'esclusione evidentemente dei dati più sensibili). Una scelta troppo dirigista rischierebbe di portare l'Italia in una direzione diversa da quella percorsa da altri Paesi, riducendo concorrenza e innovazione rispetto a un approccio di mercato.

CAPITOLO 1

IL DIGITALE NELLE POLITICHE DELL'UNIONE EUROPEA

1.1 IL DIGITAL DECADE E GLI OBIETTIVI FUTURI

Il biennio 2020-2021 rappresenta un momento di straordinaria rilevanza per la definizione del quadro normativo europeo di riferimento per il digitale. Ed infatti, in concomitanza e successivamente alla pubblicazione, nel febbraio 2020, della Comunicazione "*Plasmare il futuro digitale dell'Europa*" nella quale la Commissione europea ha declinato una serie di importanti macro-obiettivi da perseguire – sviluppo di tecnologie al servizio degli individui, creazione di un'economia digitale trasparente e competitiva e realizzazione di una società aperta, democratica e sostenibile – con relative azioni, sono state numerose le iniziative e le proposte adottate dalla stessa Commissione al fine di modernizzare il set di regole in vigore, rimuovere gli ostacoli allo sviluppo delle tecnologie e dei servizi digitali, favorire le dinamiche concorrenziali e creare un ecosistema normativo quanto più possibile chiaro e *future proof*.

Nel discorso sullo stato dell'Unione di settembre 2020, in un contesto, quello creato dalla pandemia, sempre più consapevole dell'assoluta irrinunciabilità delle tecnologie digitali e dell'importanza di garantirne ampia accessibilità in un clima di fiducia e sicurezza, la presidente von der Leyen ha annunciato che l'Europa dovrebbe garantire una sovranità digitale con una visione comune dell'UE per il 2030 ponendo particolare attenzione al cloud europeo, alla leadership nel settore dell'intelligenza artificiale etica, all'identità digitale, alle infrastrutture di dati, supercomputer e connettività. In linea con tali considerazioni, il Consiglio europeo ha invitato la Commissione a presentare entro marzo 2021 una bussola per il digitale globale che definisca le ambizioni digitali per il 2030, istituisca un sistema di monitoraggio e delinei le tappe fondamentali e le azioni da mettere in atto per realizzare tali ambizioni.

Ebbene, dando seguito a tale richiesta, il 9 marzo scorso la Commissione europea ha pubblicato la Comunicazione **"*Bussola per il digitale 2030: il modello europeo per il decennio digitale*"** proponendo di istituire una bussola per il digitale per tradurre le ambizioni digitali dell'UE per il 2030 in obiettivi concreti e garantirne il raggiungimento. Il percorso dell'UE, in particolare, sarà mappato con riguardo a quattro punti cardinali, due incentrati sulle capacità digitali a livello di infrastrutture e di istruzione e competenze e due focalizzati sulla trasformazione digitale delle imprese e dei servizi pubblici.

Rispetto al **tema infrastrutturale**, la comunicazione enfatizza l'importanza di assicurare una connettività sicura e di altissima qualità per tutti e ovunque in Europa, fissando come obiettivo al 2030 la copertura Gigabit per tutte le famiglie europee e lo sviluppo di reti 5G in tutte le zone abitate e precisando che tale obiettivo può essere perseguito con qualsiasi combinazione di tecnologie, con particolare enfasi però sulla connettività satellitare, fissa e mobile di prossima generazione più sostenibile. Se la connettività viene indicata come una condizione preliminare per la trasformazione digitale, molta attenzione è riservata ai microprocessori, quali elementi da cui iniziano quasi tutte le catene del valore strategiche più importanti, quali i veicoli connessi, i telefoni, l'Internet delle cose, i computer ad alte prestazioni, i sistemi di *edge computing* e l'intelligenza artificiale (con la conseguente necessità per l'UE di colmare le attuali lacune nella fabbricazione e progettazione per giungere a raddoppiare la quota dell'UE nella produzione mondiale), alla mancanza di grandi imprese europee che offrano cloud ed alla necessità investire nelle tecnologie quantistiche (annunciando la disponibilità per l'UE entro il 2025 del suo primo computer con accelerazione quantistica).

Quanto invece alla **digitalizzazione delle imprese**, la Commissione ha decritto il potenziale della trasformazione digitale in cinque ecosistemi

chiave (settore manifatturiero, sanità, costruzioni, agricoltura e mobilità) fissando come obiettivi al 2030 l'utilizzo, da parte del 75% delle imprese europee di servizi di *cloud computing*, big data e intelligenza artificiale, il raggiungimento, da parte di oltre il 90% delle PMI europee di almeno un livello di base di intensità digitale, l'incremento del numero di scale-up innovative ed il raddoppio del numero di imprese "*unicorno*"[1] in Europa.

Cruciale, nell'agenda dell'UE, la **digitalizzazione dei servizi pubblici** rispetto alla quale gli obiettivi da raggiungere entro il 2030 sono il 100% dei servizi pubblici principali disponibili online per le imprese e i cittadini europei, l'accesso alle cartelle cliniche elettroniche per il 100% dei cittadini europei e l'utilizzo dell'identificazione digitale da parte dell'80% dei cittadini.

Se questi sono gli obiettivi, la Commissione ha anche enucleato una serie di **principi digitali guida** tra cui il concetto di cittadinanza digitale e l'importanza di garantire che nell'ecosistema digitale i diritti trovino opportunità e tutele analoghe a quelle garantite offline, il diritto ad una connettività sicura, di alta qualità e a prezzi abbordabili, la promozione di un ambiente digitale antropocentrico che rispetti i dritti fondamentali e favorisca l'inclusione ed il rispetto dell'ambiente.

Dal punto di vista operativo, la Commissione ha proposto una serie di obiettivi concreti per ciascuno dei quattro punti cardinali ed un sistema di monitoraggio (anche mediante un ripensamento delle variabili dell'indice DESI) che vede nella stessa Commissione il soggetto responsabile dell'analisi e della segnalazione complessiva dei progressi compiuti a livello europeo al fine di individuare i settori in cui si registrano ritardi ed apprestare le conseguenti misure e raccomandazioni a livello europeo e/o nazionale. Sulla base dell'analisi effettuata, la Commissione pubblicherà ogni anno la relazione sullo stato del decennio digitale europeo destinata al Consiglio e al Parlamento europeo che determinerà l'avvio di un'analisi collaborativa tra la Commissione e gli Stati membri volta a individuare soluzioni per ovviare alle carenze e proporre azioni mirate per rimedi efficaci.

Al fine di raggiungere gli obiettivi fissati la Commissione propone anche meccanismi che consentano agli Stati membri di organizzare quei progetti multinazionali necessari per costruire la transizione digitale dell'Europa nei settori critici e di costruire solidi partenariati digitali internazionali corrispondenti ai quattro pilastri della nostra bussola (competenze, infrastrutture, trasformazione delle imprese e dei servizi pubblici) così da rafforzare la capacità dell'UE di affermare i propri interessi e fornire soluzioni globali, combattendo nel contempo le pratiche sleali e abusive e garantendo la sicurezza e la resilienza delle catene di approvvigionamento digitali dell'UE.

1.2 IL RIPENSAMENTO DEL QUADRO NORMATIVO EUROPEO. STRATEGIA SUI DATI, IL PACCHETTO DSA E DMA E IL REGOLAMENTO AI

Una delle esigenze emerse con maggior forza negli ultimi anni ed in particolar modo da quando è esplosa la pandemia che ancora purtroppo ci troviamo a fronteggiare, è quella di favorire l'ampia disponibilità di reti e servizi digitali, assicurare un mercato digitale competitivo nel quale riescano a fiorire ed affermarsi eccellenze europee e garantire un set di tutele e regole uniformi all'interno dell'UE in grado di assicurare

[1] Il termine "*unicorno*" indica: 1) le imprese unicorno "*realizzate*", ossia le società costituite dopo il 1990 che hanno effettuato un'IPO o un'operazione di trade sale superiore a un miliardo di USD e 2) le imprese unicorno "*non realizzate*", vale a dire le società che sono state valutate almeno un miliardo di USD nel loro ultimo round di finanziamenti privati in capitale di rischio (il che significa che la valutazione non è stata confermata in un'operazione secondaria).

un ecosistema improntato a certezza e fiducia nelle tecnologie digitali e, dunque, favorevole agli investimenti ed al progresso.

In tale logica ed al fine di perseguire obiettivi di armonizzazione massima, la Commissione europea ha lanciato una serie di proposte di regolamento. Scopo di tale paragrafo sarà dunque analizzare le iniziative messe in campo dalla Commissione nell'ultimo anno in materia di dati ed intelligenza artificiale, nonché il pacchetto Digital Services Act (DSA) e Digital Market Act (DMA) che, insieme alle iniziative in materia di cybersecurity, costituiscono la cornice normativa europea in materia digitale.

1.2.1 Dalla strategia sui dati al Data Governance Act

Considerando che le tecnologie digitali hanno trasformato l'economia e la società, influenzando tutti i settori di attività e la vita quotidiana di tutti gli europei e che i dati sono al centro di questa trasformazione, la comunicazione "*Una strategia europea per i dati*" del febbraio 2020 ha delineato una strategia articolata in una serie di misure ed investimenti tesi ad abilitare l'economia dei dati per i prossimi cinque anni.

La Commissione, in particolare, partendo dalla convinzione che le imprese e il settore pubblico nell'UE possano riuscire, attraverso l'accesso e l'utilizzo dei dati, a prendere decisioni migliori, maggiormente efficaci ed efficienti, intende creare uno spazio unico europeo dei dati – un vero mercato unico dei dati, aperto ai dati provenienti da tutto il mondo – dove i dati personali e non personali, compresi i dati aziendali sensibili, siano sicuri e le imprese possano avere un facile accesso a una quantità quasi infinita di dati industriali di alta qualità, stimolando la crescita e creando valore ed al contempo riducendo l'impatto sull'ambiente.

Per raggiungere questo ambizioso obiettivo, la strategia evidenzia la necessità di affrontare e risolvere una serie di criticità riguardanti:

a) **la disponibilità dei dati**. Considerando che il valore dei dati sta nel loro utilizzo e riutilizzo e che attualmente non ci sono abbastanza dati disponibili per un riutilizzo innovativo, la strategia sottolinea l'importanza di garantire la condivisione dei dati *government-to-business* (G2B) (per assicurare che i dati generati dal settore pubblico, così come il valore creato, siano disponibili per il bene comune garantendo, anche attraverso un accesso preferenziale, che questi dati siano utilizzati da ricercatori, altre istituzioni pubbliche, PMI o start-up), la condivisione dei dati *business-to-business* (B2B) (eliminando l'attuale mancanza di fiducia tra gli operatori economici sul fatto che i dati saranno utilizzati in linea con gli accordi contrattuali, gli squilibri nel potere negoziale, il timore di appropriazione indebita dei dati da parte di terzi e la mancanza di chiarezza giuridica circa i possibili usi dei dati), la condivisione dei dati tra imprese e governi (B2G) (per migliorare l'elaborazione di politiche e servizi pubblici basati su dati concreti, come la gestione della mobilità o il miglioramento della portata e della tempestività delle statistiche ufficiali) e la condivisione dei dati tra autorità pubbliche (per migliorare l'elaborazione di politiche e servizi pubblici, ma anche per ridurre gli oneri amministrativi delle imprese che operano nel mercato unico);

b) **squilibri nel potere di mercato, nella fornitura di servizi cloud e infrastrutture di dati, ma anche in relazione all'accesso e all'uso dei dat**i;

c) **interoperabilità e qualità dei dati**, incoraggiando l'applicazione di formati e protocolli standard e condivisi compatibili per la raccolta e l'elaborazione dei dati

provenienti da diverse fonti in modo coerente e interoperabile attraverso i settori e i mercati verticali;

d) **governance dei dati**, per rafforzare ulteriormente la governance dell'uso dei dati nella società e nell'economia;

e) **le infrastrutture e le tecnologie dei dati**, sottolineando diverse questioni critiche sia sul lato dell'offerta che su quello della domanda di cloud, dato che i fornitori di cloud con sede nell'UE hanno solo una piccola quota del mercato del cloud con una visibilità insufficiente, e i fornitori di servizi che operano nell'UE possono anche essere soggetti alla legislazione di paesi terzi (con il rischio che i dati dei cittadini e delle imprese dell'UE possano essere accessibili da giurisdizioni di Paesi terzi che sono in contraddizione con il quadro di protezione dei dati dell'UE). Inoltre, c'è una bassa diffusione del cloud in Europa e le imprese europee spesso sperimentano problemi con l'interoperabilità multi-cloud (in particolare la portabilità dei dati);

f) **l'abilitazione degli individui a esercitare i loro diritti**, sottolineando che anche se gli individui apprezzano l'alto livello di protezione garantito dal GDPR e dalla legislazione ePrivacy, soffrono dell'assenza di strumenti tecnici e standard che rendono l'esercizio dei loro diritti semplice e non eccessivamente oneroso;

g) **le competenze e l'alfabetizzazione sui dati**, evidenziando che l'alfabetizzazione generale sui dati nella forza lavoro e in tutta la popolazione è relativamente bassa con lacune che devono essere affrontate per padroneggiare le sfide dell'economia e della società dei dati;

h) **la sicurezza informatica**.

In una logica di superamento delle criticità appena descritte, la Commissione ha delineato una strategia incentrata su **quattro pilastri** e **diverse azioni chiave** tese a istituire un quadro di governance intersettoriale per l'accesso e l'uso dei dati, agire sui fattori abilitanti, attraverso investimenti nei dati e mediante il rafforzamento delle capacità e delle infrastrutture europee per ospitare, elaborare e utilizzare i dati, l'interoperabilità, rafforzare le competenze e responsabilizzare gli individui, e le imprese, creare spazi comuni europei dei dati in settori strategici e domini di interesse pubblico (industria manifatturiera, Green Deal, Mobilità, Salute, Finanza, Energia, Agricoltura, Pubblica Amministrazione e Competenze).

Ebbene, in attuazione della strategia, il 25 novembre 2020 la Commissione ha pubblicato la propria **proposta di regolamento relativo alla governance europea dei dati (Data Governance Act)** al fine di disciplinare la messa a disposizione dei dati del settore pubblico per il riutilizzo qualora tali dati siano oggetto di diritti di terzi, la condivisione dei dati tra le imprese, dietro compenso in qualsiasi forma, il consenso all'utilizzo di dati personali con l'aiuto di un "*intermediario per la condivisione dei dati personali*", il cui compito consiste nell'aiutare i singoli individui a esercitare i propri diritti a norma del regolamento generale sulla protezione dei dati (GDPR) ed il consenso all'utilizzo dei dati per scopi altruistici.

In particolare, la proposta di regolamento istituisce un meccanismo per il riutilizzo di determinate categorie di dati protetti detenuti da enti pubblici, che è subordinato al rispetto dei diritti di terzi (in particolare per motivi di protezione dei dati personali, ma anche di protezione dei diritti di proprietà intellettuale e riservatezza commerciale), non creando il diritto di riutilizzo dei dati, ma istituendo una serie di condizioni armonizzate di base che consentano il riutilizzo di tali dati (ad es. il requisito di non esclusività).

Nello specifico, il regolamento proposto prescrive agli enti pubblici che consentono il riutilizzo di attrezzarsi in maniera da garantire la piena tutela della protezione dei dati, della privacy e della riservatezza ed agli Stati membri di istituire un punto di contatto unico a sostegno dei ricercatori e delle imprese innovative per l'identificazione dei dati idonei e creare strutture per sostenere gli enti pubblici con mezzi tecnici ed assistenza giudiziaria.

Rispetto alla condivisione dei dati tra imprese (B2B) e da consumatore a impresa (C2B), al fine di garantire un funzionamento aperto e collaborativo dei servizi di condivisione dei dati e rafforzare il ruolo delle persone fisiche e giuridiche attraverso una maggiore conoscenza ed un maggiore controllo sui dati, il regolamento fissa una serie di **requisiti** che i fornitori di servizi di condivisione dei dati devono soddisfare (innanzitutto quello di rimanere neutrali in merito ai dati scambiati, al quale si aggiunge il divieto di utilizzare i dati per altri scopi e, nel caso di fornitori di servizi di condivisione dei dati che offrono i loro servizi a persone fisiche, l'obbligo di assunzione degli obblighi fiduciari nei confronti di chi li utilizza) e prevede un **regime di notifica** per i fornitori di servizi di condivisione dei dati. Lo stesso regolamento dispone l'individuazione di un'autorità competente designata dagli Stati membri responsabile del monitoraggio della conformità ai requisiti connessi alla fornitura di tali servizi.

Rispetto all'altruismo dei dati e, dunque, per i dati messi a disposizione su base volontaria da parte di individui o imprese per il bene comune, il regolamento proposto da un lato riconosce la possibilità per le organizzazioni che praticano l'altruismo dei dati di registrarsi in qualità di *"organizzazioni per l'altruismo dei dati riconosciute nell'UE*" annunciando anche lo sviluppo di un modulo europeo comune di consenso all'altruismo dei dati per ridurre i costi della raccolta dei consensi e facilitare la portabilità dei dati (qualora i dati da mettere a disposizione non siano detenuti dai singoli individui); dall'altro, fissa i requisiti per il funzionamento delle autorità competenti incaricate del monitoraggio e dell'attuazione del quadro di notifica per i fornitori di servizi di condivisione dei dati e per gli enti che praticano l'altruismo dei dati e disciplina il diritto di presentare reclami contro le decisioni di tali enti nonché i mezzi di ricorso giurisdizionale.

Dal punto di vista dell'assetto istituzionale, la proposta della Commissione istituisce un gruppo formale di esperti, il "***Comitato europeo per l'innovazione in materia di dati***", di cui descrive composizione e funzionamento, con funzioni di supporto e consulenza in favore della Commissione e con il compito di supportare la Commissione agevolare lo sviluppo di migliori prassi da parte delle autorità degli Stati membri, in particolare per quanto riguarda il trattamento delle domande di riutilizzo di dati oggetto dei diritti di terzi, la garanzia di una prassi coerente in merito al quadro di notifica per i fornitori di servizi di condivisione dei dati e l'altruismo dei dati.

L'impianto normativo proposto dalla Commissione è stato oggetto di un'ampia consultazione pubblica, avviata il 3 giugno e conclusasi lo scorso 3 settembre 2021, tesa a raccogliere i pareri delle autorità pubbliche competenti degli Stati membri, delle istituzioni accademiche e di ricerca, delle associazioni imprenditoriali, dei distretti industriali, delle imprese/imprese, delle organizzazioni dei consumatori, delle ONG, dei sindacati e dei cittadini.

1.2.2 Digital Markets Act (DMA)

Nel dicembre 2020, a seguito di un'ampia consultazione pubblica, la Commissione europea ha presentato il **Digital Markets Act (DMA)** con il fine di disciplinare quelle piattaforme che agiscono sempre più come *gateway* o *gatekeeper*

tra utenti commerciali e utenti finali, godono di una posizione consolidata e duratura e si trovano nella possibilità di fare usi impropri dei dati degli utenti, rafforzare le barriere all'ingresso nel mercato e porre in essere comportamenti scorretti nei confronti degli utenti commerciali e deli utenti finali. All'esigenza di fornire risposte efficaci a tali fenomeni, la Commissione ha proposto un regolamento contenente una serie di obblighi e divieti ex ante che scattano in capo ai soggetti muniti di determinati requisiti.

In particolare, la proposta va a toccare otto diversi **"*core platform services*"** e, specificatamente, servizi di intermediazione B2C online, motori di ricerca online, social network, piattaforme di condivisione video, servizi di comunicazione interpersonale indipendenti dal numero, sistemi operativi, servizi di *cloud computing* e servizi pubblicitari, compresi eventuali reti pubblicitarie, scambi pubblicitari e altri servizi di intermediazione pubblicitaria, offerti da un fornitore di uno dei servizi di cui sopra.

Ai fini della definizione dei requisiti indispensabili a qualificare un *provider* come *gatekeeper*, la proposta di regolamento richiede la sussistenza delle seguenti condizioni:

1) **significativo impatto sul mercato interno** che si presume tutte le volte in cui l'impresa realizzi un fatturato annuo nello Spazio Economico Europeo pari o superiore a 6,5 miliardi di euro negli ultimi tre esercizi finanziari (o qualora la capitalizzazione media di mercato sia stata pari ad almeno 65 miliardi di EUR nell'ultimo esercizio finanziario) ed offra il servizio in almeno tre Stati membri;

2) **possesso di una forte posizione di intermediazione**, che si verifica quando il provider collega una grande base di utenti a un gran numero di imprese (nello specifico più di 45 milioni di utenti finali attivi mensili stabiliti o situati nell'Unione e più di 10.000 utenti commerciali attivi all'anno stabiliti nell'Unione nell'ultimo esercizio finanziario);

3) **possesso** (o prevedibile possesso in un prossimo futuro) **di una posizione consolidata e duratura nelle proprie attività**. Tale requisito si presume sussistente quando le soglie di cui alla lettera b) sono state raggiunte in ciascuno degli ultimi tre esercizi finanziari.

Il possesso dei requisiti appena descritti fa scattare in capo al provider l'obbligo di notifica nei confronti della Commissione, ferma restando la facoltà della Commissione, in via autonoma, di identificare come *gatekeeper* il fornitore inadempiente rispetto a tale obbligo di notifica (alla Commissione è comunque affidato il compito di verificare, almeno ogni due anni, la conservazione dei requisiti fissati dal regolamento da parte dei *gatekeeper* e l'eventuale presenza di ulteriori providers nelle medesime condizioni).

L'**art. 5** fissa, ex ante, una serie di obblighi e di divieti in capo ai controllori dell'accesso. In particolare, sarà obbligatorio per le piattaforme *gatekeeper*:

a) consentire a terzi di interagire con i servizi del *gatekeeper* in determinate situazioni specifiche;

b) consentire agli utenti aziendali di accedere ai dati che generano nell'uso della piattaforma del *gatekeeper*;

c) fornire alle aziende pubblicitarie sulla loro piattaforma gli strumenti e le informazioni necessarie affinché gli inserzionisti e gli editori possano effettuare la propria verifica indipendente dei loro annunci ospitati dal *gatekeeper*;

d) consentire agli utenti commerciali di

promuovere la loro offerta e concludere contratti con i loro clienti al di fuori della piattaforma del *gatekeeper*;

e) consentire agli utenti finali di disinstallare qualsiasi applicazione software preinstallata sul proprio servizio di piattaforma di base, tranne nel caso in cui sia essenziale per il funzionamento del sistema operativo o del dispositivo e la cui fornitura come applicazioni software autonome di terzi è impossibile a livello tecnico;

f) consentire agli utenti commerciali e ai fornitori di servizi ausiliari l'accesso allo stesso sistema operativo e alle stesse componenti hardware o software disponibili o utilizzati nella fornitura di servizi ausiliari da parte del *gatekeeper* e l'interoperabilità con gli stessi;

g) garantire l'effettiva portabilità dei dati generati attraverso l'attività di utenti finali o business.

Sarà invece **vietato** a queste piattaforme:

a) trattare i servizi e i prodotti offerti dal *gatekeeper* stesso più favorevolmente rispetto a servizi o prodotti simili offerti da terzi sulla piattaforma del *gatekeeper*;

b) impedire ai consumatori di collegarsi con le imprese ospitate al di fuori delle piattaforme dei *gatekeeper*;

c) impedire agli utenti di disinstallare qualsiasi software o applicazione preinstallata, se lo desiderano;

d) usare i dati degli utenti commerciali al fine di competere con gli stessi.

In un'ottica di garanzia di trasparenza, è previsto a carico dei *gatekeeper* l'obbligo di sottomettere alla Commissione, entro 6 mesi dalla designazione, una descrizione, sottoposta a verifica da parte di un soggetto indipendente, di tutte le tecniche di profilazione dei consumatori che il *gatekeeper* applica a o attraverso i propri servizi.

La proposta di regolamento riconosce un ruolo centrale alla Commissione, alla quale conferisce la facoltà di richiedere informazioni, condurre ispezioni, ordinare misure temporanee, rendere vincolanti impegni proposti dal *gatekeeper*, svolgere attività di monitoraggio sull'osservanza degli obblighi di cui al regolamento proposto, adottare decisioni attestanti infrazioni da parte dei *gatekeeper* e comminare sanzioni. Queste ultime, in particolare, sono quantificate fino al 10% del fatturato annuo totale mondiale dell'azienda e fino al 5% del fatturato medio giornaliero. Nello svolgimento delle attività disciplinate nel DMA, la Commissione è assistita dal **Digital Markets Advisory Committee**. Le decisioni della Commissione e le sanzioni dalla stessa comminate sono sottoposte alla giurisdizione della Corte di Giustizia dell'UE che può cancellarle, ridurle o incrementarle.

All'indomani del lancio della proposta è stato immediato l'avvio di un ampio e acceso dibattito tra gli stakeholder e tra Stati membri e Commissione sulle scelte di impianto generale nonché sulla struttura di governance da mettere in campo per assicurare che una volta conclusa la procedura legislativa di approvazione della proposta, l'UE e gli Stati membri siano davvero in grado di garantire un'efficace applicazione del nuovo set di regole. E infatti, se è diffusa la consapevolezza circa la necessità di ripensare il set di regole vigenti per offrire risposte ed apprestare rimedi alle criticità concorrenziali esistenti negli ecosistemi digitali, sono molti i profili oggetto di dibattito.

In particolare, è in discussione la capacità di un sistema normativo improntato ad una logica ex

ante di far fronte alle sfide del futuro in un settore ad elevatissima rapidità di innovazione, così come la scelta di dettare regole uniformi per soggetti con modelli di business ed organizzazioni profondamente diverse cui si contrappone, almeno parzialmente, l'esigenza di garantire certezza, prevedibilità e uniformità.

Rispetto ai contenuti degli obblighi e dei divieti previsti, è stato inoltre rilevato il rischio che la proposta della Commissione risulti eccessivamente focalizzata sulle criticità del presente e sulla necessità di porvi rimedio e meno attenta all'impatto che il nuovo set di obblighi e divieti potrebbe produrre sui modelli di business e sulle leve competitive degli operatori oltre che sulla privacy e sulla sicurezza. In tale logica andrebbe valorizzato il ricorso al dialogo regolatorio che potrebbe consentire, in parte, di mitigare le conseguenze di una rigorosa ed indiscriminata applicazione del nuovo quadro normativo. Il ricorso al dialogo regolatorio - con deadline precise che non ritardino oltremodo l'intervento della Commissione - potrebbe risultare particolarmente utile anche al fine di garantire che i poteri particolarmente pervasivi riconosciuti alla Commissione trovino mitigazione e correttivo così da assicurare un'adeguata ponderazione della singola situazione oggetto di analisi. Non meno importanti i rilievi concernenti la necessità, al fine di garantire l'efficacia della normativa proposta, di assicurare un'efficace cooperazione tra Commissione e Stati Membri anche mediante una maggior valorizzazione del ruolo delle autorità nazionali di regolamentazione.

1.2.3 Digital Services Act (DSA)

A seguito di un'ampia e partecipata consultazione incentrata su temi quali la sicurezza online, la libertà di espressione, l'equità e condizioni di parità nell'economia digitale che ha registrato 2.863 risposte e circa 300 position papers da parte di diversi gruppi di stakeholder, il 15 dicembre 2020 la Commissione europea ha pubblicato la proposta di regolamento per l'adozione del **Digital Services Act (DSA)** con cui offrire una risposta normativa agli enormi cambiamenti - cui si accompagnano non solo grandi opportunità ma anche nuovi rischi e criticità - determinati dalla crescente diffusione di servizi digitali ad elevata innovatività che hanno rivoluzionato il modo di comunicare, interagire, consumare e fare business.

La proposta, articolata in **cinque capitoli**, introduce un quadro orizzontale per tutte le categorie di contenuti, prodotti, servizi e attività sui servizi di intermediazione, ma allo stesso tempo delinea un regime di responsabilità diversificato in base ai servizi offerti ed alla dimensione del fornitore. Per quanto riguarda la governance, la proposta di regolamento prevede a carico degli Stati membri specifici obblighi di verifica della compliance di fornitori di servizi operanti nei rispettivi territori rispetto alle previsioni contenute nel regolamento proposto, istituisce nuovi soggetti (i **Coordinatori per i Servizi Digitali**) e delinea meccanismi di enforcement e cooperazione tra gli Stati.

Destinatari della nuova disciplina sono **i prestatori di servizi della società dell'informazione** così come definiti nella direttiva n. 1535/2015 e, dunque, coloro che forniscono qualsiasi servizio normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi. Nel distinguere le varie tipologie di providers e fissare i relativi regimi di responsabilità, il regolamento riproduce la distinzione già fissata nella direttiva e-commerce, distinguendo servizi "*mere conduit*", servizi di "*caching*" e servizi di "*hosting*" e ricollega alle diverse ipotesi i presupposti per l'esclusione della responsabilità a carico dei fornitori.

Per quanto concerne gli **obblighi di due diligence**, la proposta di regolamento ne fissa vari e di complessità crescente. In particolare, se a carico

di tutti i fornitori di servizi di intermediazione, indipendentemente dalle dimensioni e dal servizio offerto, è posto l'obbligo di istituire un singolo punto di contatto per la comunicazione diretta con le autorità degli Stati membri, individuare per iscritto, nel caso di fornitori non stabiliti nell'Unione, un legale rappresentante in uno degli Stati membri in cui offre i propri servizi, includere nei propri termini e condizioni, in un linguaggio chiaro e disponibile pubblicamente, le informazioni riguardanti eventuali restrizioni imposte all'utilizzo del servizio, incluse quelle relative a politiche, procedure, misure e strumenti utilizzati per la moderazione dei contenuti, compreso il processo decisionale algoritmico e la revisione umana e pubblicare, almeno una volta all'anno, un report, facilmente comprensibile e dettagliati su qualsiasi moderazione di contenuto operata, tali obblighi si arricchiscono nel caso di fornitori di servizi di *hosting*, incluse le piattaforme online.

A questi ultimi, infatti, è prescritta la predisposizione di meccanismi di notifica ed azione che consentano a individui ed enti di segnalare la presenza sui servizi degli intermediari di specifiche informazioni ritenute di contenuto illegale e l'invio di un'informativa circostanziata e motivata ai destinatari del servizio circa la decisione di rimuovere o disabilitare l'accesso a determinate informazioni.

Con riguardo alle **piattaforme online** (con esclusione di quelle qualificate come micro o piccole imprese), gli obblighi di due diligence raggiungono una complessità ancora maggiore, richiedendo la predisposizione di un sistema interno di gestione dei reclami contro decisioni di rimozione o disabilitazione dell'accesso all'informazione, sospensione, interruzione o chiusura dell'account dei destinatari, la previsione di misure tecniche ed organizzative idonee ad assicurare che le segnalazioni provenienti da "*segnalatori di fiducia*" siano processate e decise con priorità, la tempestiva informazione, per le piattaforme che abbiano appreso notizie che fanno sorgere il sospetto che un grave reato penale implichi una minaccia per la vita o la sicurezza di persone ha avuto luogo, sta avendo luogo o è probabile che abbia luogo, in favore delle autorità incaricate dell'applicazione della legge o le autorità giudiziarie dello Stato membro o degli Stati interessati, la redazione di un report che includa il numero di controversie sottoposte agli organismi, le decisioni ed il tempo medio di risoluzione di tali controversie, il numero di sospensioni etc., la predisposizione di sistemi in grado di garantire che gli utenti possano identificare, per ogni specifico annuncio visualizzato, in modo chiaro e inequivocabile e in tempo reale, che l'informazione visualizzata è una pubblicità, la persona fisica o giuridica per conto della quale viene visualizzato l'annuncio ed informazioni significative sui principali parametri utilizzati per individuare il destinatario della pubblicità e l'acquisizione di specifiche informazioni da mettere a disposizione dei consumatori ai quali viene consentito concludere contratti a distanza con i venditori (tracciabilità dei venditori).

Rispetto alle **grandi piattaforme online**, ossia quelle che offrono i propri servizi ad un numero di utenti pari ad almeno il 10% della popolazione dell'UE (45 milioni di utenti), la proposta prescrive obblighi di controllo dei propri rischi e di adozione di misure di mitigazione dei rischi individuati, la sottoposizione delle grandi piattaforme, a proprie spese, ad un audit almeno annuale da parte di un'organizzazione indipendente dalla piattaforma che verifichi l'osservanza degli obblighi sulla stessa gravanti e stili un report, l'inserimento, in un archivio di dedicato, di una serie di informazioni relative alla pubblicità online, l'obbligo di ostensione dei dati richiesti dalla Commissione e dal **Coordinatore per i Servizi Digitali** per attività di verifica dell'osservanza delle obbligazioni previste dal regolamento, l'individuazione di responsabili della conformità e l'osservanza di specifici obblighi di reporting in favore della

Commissione e del Coordinatore.

Per quanto attiene la **governance**, oltre a istituire la figura del Coordinatore dei Servizi Digitali (di cui prevede i poteri minimi e le competenze) e il **Board europeo per i Servizi Digitali**, di cui disciplina la composizione e le funzioni, la proposta di regolamento attribuisce importanti e pervasivi poteri alla Commissione. A quest'ultima, infatti, sono attribuiti poteri di monitoraggio, avvio del procedimento, indagine, ispezione, nonché il potere di prescrivere misure temporanee, adottare decisioni attestanti il mancato rispetto della disciplina di cui al regolamento o tese a rendere vincolanti gli impegni proposti dalla piattaforma e comminare sanzioni alle grandi piattaforme nella misura massima del 6% del fatturato realizzato nell'anno precedente a quello in cui volontariamente o negligentemente ha violato il regolamento, una decisione contenente misure temporanee o inosservanza degli impegni assunti (a ciò si aggiunge la possibilità di comminare penalità di mora non superiori al 5% del fatturato medio giornaliero dell'esercizio precedente, calcolato a partire dalla data stabilita dalla decisione, il tutto entro 5 anni dalla data di commissione della violazione).

L'importanza delle innovazioni proposte ha ragionevolmente sollevato una vasta e vivace discussione che sicuramente accompagnerà tutte le fasi dell'articolata procedura legislativa di adozione del regolamento e che, sebbene abbia alla base l'unanime consapevolezza circa la necessità di rivedere il quadro normativo vigente, si concentra su molti aspetti della disciplina proposta.

E infatti, se da un lato viene espressa, soprattutto da parte degli Stati membri, la necessità di chiarire meglio i meccanismi di cooperazione e coordinamento con la Commissione al fine di garantire **efficacia di azione**, dall'altro, sono state formulate richieste di ripensamento della tipologia di obblighi previsti a carico dei fornitori in considerazione della loro praticabilità e sostenibilità, di estensione di alcuni obblighi, soprattutto quelli a tutela dei consumatori, anche alle PMI, di rafforzamento ed estensione di alcune prescrizioni in materia di pubblicità online, di rafforzamento dell'obbligo di tracciabilità dei commercianti mediante l'estensione della portata di alcune disposizioni a tutti i servizi di intermediazione e attraverso l'introduzione di nuove disposizioni rivolte ai mercati online, di fissazione di tempistiche più stringenti per agire sui contenuti ad alto impatto e di chiarificazione del concetto di contenuto illecito al fine di non vanificare gli sforzi di armonizzazione compiuti con la disciplina proposta.

1.2.4 Artificial Intelligence Act

L'**intelligenza artificiale** (IA) rappresenta uno dei fattori tecnologici dai quali dipenderà, in larga parte, la competitività dell'UE e dei singoli Stati membri. L'uso dell'IA, infatti, assicurando migliori capacità predittive, consentendo l'ottimizzazione delle operazioni e dell'assegnazione delle risorse e la personalizzazione dell'erogazione di servizi, contribuirà in maniera straordinaria al conseguimento di benefici enormi dal punto di vista sociale ed ambientale oltre che alla fruizione di vantaggi competitivi per le imprese e l'economia europea nella competizione globale.

Conscia di tale opportunità, la Commissione europea sin dal 2018, con la **comunicazione "*AI per l'Europa*"** ha dato avvio ad una serie di iniziative da parte dell'UE nel campo dell'intelligenza artificiale tra cui la pubblicazione, nel febbraio 2020, del **Libro Bianco sull'IA**, fino a giungere al lancio, il 21 aprile 2021, di una proposta di regolamento AI intitolato ***"Il regolamento del Parlamento europeo e del Consiglio che stabilisce norme armonizzate in materia di intelligenza artificiale e che modifica alcuni atti legislativi dell'Unione"***, con il quale si istituisce un quadro di riferimento legale volto a

normare il mercato dell'UE dell'IA.

Tale proposta, in particolare, si inquadra nell'ambito di un pacchetto più ampio che comprende anche una comunicazione sulla promozione di un **approccio europeo all'intelligenza artificiale ed il Piano Coordinato con gli Stati membri**: aggiornamento 2021, con cui si va ad istituire la nuova cornice normativa europea in materia e a perseguire gli obiettivi strategici fissati dalla Commissione che consistono nella definizione delle condizioni abilitanti per lo sviluppo e la diffusione dell'IA, nella costruzione di una leadership strategica nei settori ad impatto elevato, nella creazione di un ecosistema favorevole al prosperare dell'IA e nella garanzia che le tecnologie di IA siano al servizio delle persone.

Entrando nell'analisi della proposta, l'ambito applicativo del regolamento comprende i **fornitori che immettono sul mercato o mettono in servizio sistemi di IA nell'UE**, indipendentemente dal luogo di stabilimento, agli utenti dei sistemi di IA situati nell'Unione e ai fornitori ed utenti di sistemi di IA situati in un Paese terzo, laddove l'output prodotto dal sistema sia utilizzato nell'UE.

Quanto alle **finalità** perseguite, la disciplina proposta mira ad accrescere la fiducia dei cittadini europei nell'IA mediante la previsione di obblighi diversificati che seguono un approccio basato sul rischio, che distingue tra usi dell'IA che creano (i) un rischio inaccettabile, (ii) un rischio elevato e (iii) un rischio basso o minimo. Il regolamento va conseguentemente a vietare quelle pratiche considerate inaccettabili in quanto contrarie ai valori dell'Unione, ad esempio perché violano i diritti fondamentali (ad es. pratiche manipolative dei minori o dei disabili o che prevedono l'uso di tecniche subliminali che sfruttano l'inconsapevolezza degli individui etc.), mentre per i sistemi di IA ad alto rischio, il regolamento distingue le principali tipologie di sistemi che rientrano in tale categoria (i sistemi di IA destinati ad essere utilizzati come componenti di sicurezza di prodotti soggetti a valutazione della conformità ex ante da parte di terzi ed altri sistemi di IA indipendenti che presentano implicazioni principalmente in relazione ai diritti fondamentali esplicitamente elencati nell'allegato III), individua i criteri da seguire per valutare se un sistema di IA presenta alti rischi e fissa una serie di requisiti obbligatori oltre a subordinare l'accesso al mercato europeo di tali sistemi ad una valutazione della conformità ex ante di cui il regolamento disciplina dettagliatamente le procedure tese ad ottenere la marcatura CE di conformità.

Nello specifico, il regolamento prescrive l'istituzione, la conservazione e la dimostrazione di un **sistema di gestione dei rischi che sia frutto di un processo di aggiornamento costante e sistematico** nel corso dell'intero ciclo di vita del sistema, l'adozione di adeguate misure di gestione dei rischi da adottare secondo una serie di criteri e principi dettagliatamente enucleati e a seguito di specifiche prove dirette a misurarne l'appropriatezza, la predisposizione e conservazione della documentazione tecnica a supporto, una progettazione tesa ad assicurare un adeguato livello di accuratezza, robustezza e cibersicurezza, obblighi di monitoraggio successivo all'immissione in commercio e di segnalazione di incidenti gravi o malfunzionamenti e garanzie di collaborazione con le autorità competenti.

Specifici obblighi sono posti a carico di importatori e distributori di sistemi di IA ad alto rischio.
La proposta di regolamento si premura di definire obblighi anche in capo agli utilizzatori di sistemi di IA ad alto rischio, prescrivendo, in particolare, l'utilizzo di tali sistemi conformemente alle istruzioni per l'uso, la garanzia che i dati di input siano pertinenti con la finalità del sistema di IA e la conservazione dei *log* generati automaticamente dai sistemi di AI ad alto rischio, nella misura in cui tali log sono sotto il loro

controllo, per un periodo adeguato alla luce della finalità prevista del sistema di IA.

Specifici **obblighi di trasparenza** sono previsti con riferimento a sistemi di IA destinati a interagire con le persone fisiche, sistemi di riconoscimento delle emozioni o di categorizzazione biometrica e sistemi che generano o manipolano immagini o contenuti audio o video rispetto ai quali è necessario garantire che gli utenti siano consapevoli.

Oltre agli obblighi imposti per lo sviluppo, la distribuzione e l'uso di sistemi di IA, **l'AI Act contiene diverse misure volte a sostenere l'innovazione in questo settore**. Il regolamento, infatti, incoraggia le autorità nazionali competenti a creare sandbox di regolamentazione e stabilisce un quadro di base in termini di governance, supervisione e responsabilità, nonché misure per ridurre gli oneri a carico di PMI e start-up.

Per quanto riguarda gli aspetti di governance, il regolamento proposto istituisce a livello dell'Unione un **Comitato europeo per l'intelligenza artificiale** composto dalle autorità nazionali di controllo, rappresentate dal capo di tale autorità o da un alto funzionario di livello equivalente e dal Garante europeo della protezione dei dati e presieduto dalla Commissione, con il compito di raccogliere e condividere conoscenze e migliori pratiche tra gli Stati membri e contribuire all'uniformità delle pratiche amministrative negli Stati membri, formulare pareri, raccomandazioni o contributi scritti su questioni relative all'attuazione del regolamento.
A ciascun Stato membro è rimessa invece la designazione di un'autorità competente al fine di garantire l'applicazione e l'attuazione del regolamento (con il compito, anche, di fornire orientamenti e consulenza sull'attuazione dello stesso regolamento) e la formulazione di una relazione annuale da trasmettere alla Commissione.

Il regolamento incoraggia, infine, l'adozione di **Codici di condotta** elaborati da singoli fornitori di sistemi di IA o da organizzazioni che li rappresentano o da entrambi, anche con la partecipazione degli utenti e di tutti gli altri portatori di interessi e delle loro organizzazioni rappresentative tesi a promuovere l'applicazione volontaria ai sistemi di IA dei requisiti relativi, ad esempio, alla sostenibilità ambientale, all'accessibilità per le persone con disabilità etc.

A garanzia dell'osservanza delle regole contenute nel regolamento, la proposta declina un **set di sanzioni** rispetto alle varie possibili violazioni rimettendo agli Stati membri la fissazione delle regole relative alle sanzioni a patto che esse siano effettive, proporzionate e dissuasive e tengano conto in particolare degli interessi dei fornitori di piccole dimensioni e delle start-up e della loro sostenibilità economica.

Se questa è la cornice normativa disegnata con il regolamento, il piano coordinato intende coordinare i finanziamenti stanziati attraverso i programmi Digital Europe e Horizon, nonché il Recovery and Resilience Facility (che prevede un obiettivo di spesa digitale del 20%), nonché i programmi della politica di coesione, per:

a) creare condizioni abilitanti per lo sviluppo e l'adozione dell'IA;

b) promuovere l'eccellenza dell'IA attraverso un partenariato pubblico-privato;

c) garantire che l'IA sia incentrata sulle persone ed operi come forza positiva nella società;

d) costruire una leadership strategica in settori e tecnologie ad alto impatto, concentrandosi sul contributo dell'IA alla produzione sostenibile, alla salute, al settore pubblico, alla mobilità, all'agricoltura e alla robotica.

Anche tale proposta della Commissione sta animando un ampio dibattito a livello internazionale. Ed infatti, sebbene sia ampio l'apprezzamento per la scelta di stabilire un quadro armonizzato nel campo dell'IA ed aderire ad un approccio basato sul rischio e focalizzato sulla tutela dei diritti e degli interessi degli individui, non mancano le richieste di chiarificazione circa i contenuti di alcuni obblighi, di riservare maggior attenzione alle possibili applicazioni ed usi delle tecnologie IA piuttosto che alle tecnologie in sé di valutare l'entità dei costi gravanti soprattutto sulle PMI e le start-up ed il potenziale ostacolo alla concorrenza e l'innovazione che essi rappresentano.

1.3 LA CYBERSECURITY NELL'ECOSISTEMA NORMATIVO EUROPEO

Come componente essenziale della strategia digitale dell'UE ***"Plasmare il futuro digitale dell'Europa"***, del piano per la ripresa dell'Europa e della strategia dell'UE per l'Unione della sicurezza, il 16 dicembre 2020 la Commissione e l'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno presentato la ***"Strategia dell'UE in materia di cibersicurezza per il decennio digitale"*** al fine di rafforzare la resilienza collettiva dell'Europa contro le minacce informatiche e contribuire a garantire che tutti i cittadini e tutte le imprese possano beneficiare al meglio di servizi e strumenti digitali affidabili.
Si tratta di una strategia straordinariamente importante che rientra nel "*Cybersecurity package*", pacchetto che comprende anche una nuova direttiva sulla resilienza delle entità critiche e una proposta di direttiva relativa alle misure necessarie per conseguire un elevato livello comune di cibersicurezza in tutta l'Unione (direttiva NIS rivista) e che rappresenta un nuovo insieme di azioni ed iniziative, in parte già effettive ed in parte ancora solo proposte, per indirizzare la sicurezza cibernetica dell'Unione nel prossimo decennio.

La strategia, in particolare, contiene proposte concrete di iniziative politiche, di regolamentazione e di investimento in tre aree d'azione dell'UE:

1) RESILIENZA, SOVRANITÀ TECNOLOGICA E LEADERSHIP. In questa linea d'azione, in particolare, la Commissione propone di:

a) riformare le norme sulla sicurezza delle reti e dei sistemi informatici nell'ambito di una direttiva NIS riveduta;

b) creare una rete di centri operativi per la sicurezza all'interno dell'UE;

c) prevedere un sostegno dedicato alle piccole e medie imprese (PMI) nel quadro dei poli dell'innovazione digitale e maggiori sforzi per migliorare le competenze della forza lavoro, attirare e trattenere i migliori talenti in materia di cibersicurezza e investire per una ricerca e un'innovazione aperta, competitiva e basata sull'eccellenza;

d) realizzare un'infrastruttura di comunicazione quantistica sicura per l'Europa;

e) garantire reti mobili di ultima generazione sicure attraverso il completamento dell'attuazione del pacchetto di strumenti per il 5G entro il secondo trimestre del 2021;

f) apprestare nuove norme orizzontali volte a migliorare la cibersicurezza di tutti i prodotti connessi e servizi associati presenti nel mercato interno;

g) creare una presenza rafforzata lungo la catena di approvvigionamento tecnologico per promuovere la propria strategia industriale e la propria leadership in materia di tecnologie digitali e cibersicurezza lungo la catena di approvvigionamento digitale

(comprendente dati e cloud, tecnologie dei processori di nuova generazione, connettività ultra sicura e reti 6G), in linea con i propri valori e priorità;

h) migliorare le competenze della forza lavoro, per attrarre e trattenere i migliori talenti in materia di cibersicurezza e per investire nella ricerca e nell'innovazione di livello mondiale.

2) SVILUPPO DI CAPACITÀ OPERATIVE DI PREVENZIONE, DISSUASIONE E RISPOSTA. Nell'ambito di tale linea d'azione, invece, la Commissione propone:

a) la predisposizione di un'unità congiunta per il ciberspazio con la funzione di piattaforma virtuale e fisica per la cooperazione tra le varie comunità di cibersicurezza all'interno dell'UE, con particolare attenzione al coordinamento tecnico e operativo volto a contrastare gravi minacce e incidenti informatici di natura transfrontaliera;

b) ampliare e migliorare la capacità delle forze dell'ordine di indagare sulla criminalità informatica, rispettando pienamente i diritti fondamentali e perseguendo il necessario equilibrio tra i vari diritti e interessi, attuando pienamente una legislazione adatta allo scopo;

c) aggiornare le linee guida di attuazione del pacchetto di strumenti della diplomazia informatica anche al fine di aumentare l'efficienza del processo decisionale e continuare ad organizzare regolarmente esercitazioni e valutazioni sul pacchetto di strumenti della diplomazia informatica stesso;

d) promuovere le capacità di ciberdifesa presentando una revisione del quadro strategico in materia di ciberdifesa al fine di migliorare ulteriormente il coordinamento e la cooperazione tra attori dell'UE;

e) facilitare lo sviluppo di una "*visione e strategia militari dell'UE sul ciberspazio come dominio operativo*" per le missioni e le operazioni militari della PSDC, sostenere sinergie tra l'industria civile, della difesa e dello spazio e rinforzare la cibersicurezza delle infrastrutture spaziali critiche nell'ambito del programma spaziale.

3) PROMOZIONE DI UN CIBERSPAZIO GLOBALE E APERTO. Nella terza linea d'azione, la Commissione mira a:

a) rafforzare la cooperazione con i Paesi terzi, le organizzazioni internazionali e la comunità multi-partecipativa;

b) promuovere comportamenti responsabili degli Stati nel ciberspazio, promuovendo, coordinando e consolidando le posizioni degli Stati membri presso le sedi internazionali, sviluppando una posizione dell'Unione sull'applicazione del diritto internazionale nel ciberspazio, guidando la protezione e la promozione dei diritti umani e delle libertà fondamentali online e completando il secondo protocollo aggiuntivo alla convenzione di Budapest;
c) promuovere con forza il modello multi-partecipativo per la governance di Internet consolidando scambi regolari e strutturati con il settore privato, il mondo accademico e la società civile.

Sempre nella logica di garantire risposte efficaci alle nuove minacce, il 14 aprile 2021 la Commissione ha presentato **una nuova strategia dell'UE per contrastare la criminalità organizzata**, con la quale mira a rafforzare la cooperazione tra autorità di contrasto e autorità giudiziarie offrendo, rispetto a reati di particolare rilevanza,

risposte adeguate agli sviluppi tecnologici. La strategia definisce gli strumenti e le misure da introdurre nei prossimi cinque anni per smantellare il modello operativo e le strutture delle organizzazioni criminali a livello transfrontaliero, sia online che offline.

Successivamente, il 20 maggio 2021 è stato adottato **il Regolamento numero 887/2021 che istituisce il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento**. Tale regolamento, in particolare, mira a rafforzare le capacità europee di sicurezza informatica, promuovere l'eccellenza della ricerca ed accrescere la competitività dell'industria dell'Unione in questo campo.

L'UE si è impegnata a sostenere la nuova strategia per la cibersicurezza nei prossimi sette anni con poderosi investimenti nella transizione digitale dell'UE, attraverso il prossimo bilancio a lungo termine dell'UE, in particolare tramite il **programma Europa digitale, Orizzonte Europa e il piano per la ripresa dell'Europa**. Gli Stati membri sono pertanto incoraggiati a utilizzare appieno il dispositivo per la ripresa e la resilienza dell'UE per rafforzare la cibersicurezza e a fare investimenti a pari livello di quelli dell'Unione con l'obiettivo di raggiungere fino a 4,5 miliardi di euro di investimenti combinati da parte dell'UE, degli Stati membri e dell'industria, in particolare nell'ambito del Centro di competenza sulla cibersicurezza e della rete dei centri di coordinamento e garantire che una parte importante di questi investimenti sia effettivamente attribuita alle PMI.

1.3.1 La proposta di modifica della direttiva NIS: le principali novità

Come anticipato nel paragrafo precedente, **la proposta lanciata a dicembre 2020 va a modificare ed abrogare la direttiva 2016/1148 (la cosiddetta direttiva NIS) del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione**, con la quale le istituzioni europee hanno affrontato le sfide in materia di cyber security, e, per la prima volta, hanno disciplinato in maniera organica il tema della sicurezza, delineando la cornice normativa ed organizzativa dell'UE e rinsaldando la cooperazione tra Stati membri ed istituzioni.

Tale direttiva, in particolare, ha obbligato gli Stati membri ad adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi (di cui la stessa direttiva, all'art. 7, ha individuato i contenuti essenziali), ha individuato sette settori strategici strettamente legati alla dimensione della sicurezza, ossia energia, trasporti, banche, mercati finanziari, sanità, fornitura e distribuzione di acqua potabile e infrastrutture digitali, oltre a motori di ricerca, cloud e piattaforme online, ha istituito un gruppo di cooperazione (composto da rappresentanti degli Stati membri, della Commissione e dell'ENISA) con il compito di svolgere i propri compiti (in quattro ambiti, e nello specifico, pianificazione, guida, segnalazione e condivisione) sulla base di programmi di lavoro biennali, ha istituito una rete di gruppi di intervento per la sicurezza informatica, ha fissato obblighi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali (tra cui l'obbligo di dotarsi di misure di sicurezza che comprendono prevenzione dei rischi, garanzia circa la sicurezza dei sistemi, delle reti e delle informazioni e capacità di gestire gli incidenti cui si aggiunge, per i secondi, la sicurezza dei sistemi e degli impianti, la gestione della continuità operativa, il monitoraggio e i test e la conformità a norme internazionali).

Ebbene, partendo dalla constatazione della trasformazione digitale della società (intensificata dalla crisi COVID-19) che ha ampliato e aggravato il panorama delle minacce imponendo nuove sfide, in anticipo rispetto alla roadmap tracciata

che fissava al 9 maggio 2021 la formulazione della prima relazione a Parlamento europeo e Consiglio, **il 25 giugno 2020 la Commissione europea ha ufficialmente aperto la consultazione pubblica relativamente alla futura revisione della direttiva NIS**, conclusasi il 2 ottobre 2020, al fine di valutare il livello di funzionamento della Direttiva NIS all'interno di ciascun Paese dell'Unione, attraverso lo studio del livello qualitativo e quantitativo della sicurezza delle reti e dei sistemi informativi degli Stati membri, la determinazione dell'efficacia, efficienza, coerenza e pertinenza della Direttiva NIS in considerazione dei progressi tecnologici e dell'evoluzione delle relative minacce informatiche, l'individuazione e la quantificazione dei costi e dei benefici, diretti e indiretti, derivanti dal processo di revisione della normativa nonché l'individuazione delle questioni chiave esistenti e di quelle potenzialmente emergenti a livello di sicurezza in grado di impattare sul funzionamento della direttiva.

Entrando ora nel merito delle innovazioni previste dalla proposta della Commissione, una tra le più rilevanti concerne senza dubbio l'**estensione di specifici obblighi in materia di cyber security a soggetti ulteriori** rispetto a quelli attualmente rientranti nell'ambito applicativo della direttiva NIS e la **puntuale identificazione delle tipologie di soggetti operanti nei vari settori e sotto-settori indicati** che rientrano nella definizione di "*soggetto essenziale*" e "*soggetto importante*", che confluiscono, secondo quanto previsto dalla proposta di direttiva, in un apposito registro creato e tenuto dall'ENISA e sono sottoposti a regimi di vigilanza parzialmente diversi.

In una logica di modernizzazione, la proposta prevede la divulgazione coordinata delle vulnerabilità mediante attribuzione, da parte di ciascuno Stato membro, del ruolo di **coordinatore a uno dei propri CSIRT (Computer Security Incident Response Team)** che agisce da intermediario di fiducia e l'istituzione del registro europeo delle vulnerabilità, la cui tenuta è affidata all'ENISA, che contiene informazioni circa la vulnerabilità, i prodotti TIC o i servizi TIC interessati, la gravità della vulnerabilità e le possibili modalità di attenuazione dei rischi derivanti dalle vulnerabilità divulgate.

Rispetto agli Stati membri, la normativa proposta arricchisce i contenuti da inserire nella strategia nazionale, prescrive l'adozione di un piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala in cui sono stabiliti gli obiettivi e le modalità della gestione delle crisi e degli incidenti di cibersicurezza, la designazione di una o più autorità competenti responsabili della gestione delle crisi e degli incidenti su vasta scala e l'assegnazione a tali autorità di risorse adeguate per svolgere la propria attività. A livello UE, al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cibersicurezza su vasta scala e di garantire il regolare scambio di informazioni tra gli Stati membri e le istituzioni, gli organismi e le agenzie dell'UE, la stessa proposta istituisce la **Rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe)** definendone la composizione e declinandone i compiti.

Oltre a confermare l'obbligo di individuazione dei punti di contatto unici nazionali, la proposta di direttiva introduce una specifica disposizione (l'art. 10) che declina in dettaglio **i requisiti e i compiti dei CSIRT**, mentre nel disciplinare la cooperazione a livello nazionale, introduce ulteriori commi tesi a garantire che ciascuno Stato membro assicuri un'adeguata cooperazione tra le autorità competenti e i punti di contatto unici e le autorità di contrasto, le autorità di protezione dei dati, le autorità responsabili delle infrastrutture critiche e le autorità finanziarie nazionali designate e prescriva la comunicazione periodica, da parte delle autorità competenti designate a norma della direttiva sulla resilienza dei soggetti critici, di informazioni sui rischi di cibersicurezza, sulle minacce informatiche e sugli incidenti che interessano i soggetti essenziali

identificati come critici, o come soggetti equivalenti ai soggetti critici, a norma della direttiva sulla resilienza dei soggetti critici, nonché sulle misure adottate dalle autorità competenti in risposta a tali rischi e incidenti.

Per quanto riguarda, invece, il **Gruppo di cooperazione**, la proposta di direttiva, da un lato, estende la possibilità di partecipare alle attività del gruppo (composto da rappresentanti degli Stati membri, della Commissione e dell'ENISA), in qualità di osservatore, al servizio europeo per l'azione esterna, nonché alle autorità europee di vigilanza (AEV) conformemente all'articolo 17, paragrafo 5, lettera c), del regolamento DORA in materia Fintech, dall'altro, ne arricchisce l'ambito operativo.

Per assicurare un monitoraggio efficace, la proposta di direttiva **affida all'ENISA il compito di redigere una relazione biennale sullo stato della cibersicurezza nell'Unione** in cui valutare il livello di maturità delle capacità di cibersicurezza ed istituisce una procedura di revisione tra pari. La Commissione, in particolare, previa consultazione del gruppo di cooperazione e dell'ENISA, è chiamata a stabilire una metodologia nonché i contenuti di un sistema di revisioni condotte da esperti tecnici di cibersicurezza provenienti da Stati membri diversi da quello oggetto di revisione per valutare l'efficacia delle politiche di cibersicurezza degli Stati membri.
Quanto invece alle **misure di gestione dei rischi di cibersicurezza**, se la direttiva NIS lasciava agli Stati membri provvedere affinché gli operatori di servizi essenziali adottassero misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, la proposta in esame elenca i contenuti minimi che le misure adottate dai soggetti essenziali e importanti devono contenere e, andando parzialmente ad arricchire quanto già previsto indicando il ricorso a specifiche misure, prevede:

a) analisi dei rischi e politiche di sicurezza dei sistemi informatici;

b) gestione degli incidenti (prevenzione e rilevamento degli incidenti e risposta agli stessi);

c) continuità operativa e gestione delle crisi;

d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi fornitori o fornitori IT 49 IT di servizi, quali i fornitori di servizi di conservazione ed elaborazione dei dati o di servizi di sicurezza gestiti;

e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;

f) strategie e procedure (test e audit) per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;

g) uso della crittografia e della cifratura.

Per quanto attiene agli **obblighi di segnalazione** gravanti sui soggetti essenziali ed importanti, la proposta di direttiva prescrive la notifica degli incidenti con impatto significativo sulla fornitura dei loro servizi alle autorità competenti o al CSIRT, fornendo una definizione chiara di incidente significativo e definendo tempistiche e modalità della procedura di notifica.

Molto rilevante la facoltà riconosciuta agli Stati membri di imporre ai soggetti essenziali e importanti di certificare determinati prodotti TIC, servizi TIC e processi TIC nell'ambito di specifici sistemi europei di certificazione della cibersicurezza (con possibilità per la Commissione di richiedere all'ENISA di predisporre una proposta di sistema nel caso in cui non siano

disponibili sistemi di certificazione europei adeguati).

Specifica attenzione è riservata alla c**ondivisione delle informazioni tra soggetti essenziali ed importanti**, nell'ambito di comunità fidate e secondo procedure specificate dagli Stati membri, comprese quelle relative a minacce informatiche, vulnerabilità, indicatori di compromissione, tattiche, tecniche e procedure, allarmi di cibersicurezza e strumenti di configurazione nella logica di prevenire, rilevare ed attenuare gli incidenti ed aumentare il livello di cibersicurezza, cui si aggiunge la possibilità, già prevista dalla direttiva NIS in vigore, per i soggetti non rientranti nell'ambito di applicazione della direttiva, di effettuare una notifica volontaria di incidenti significativi, minacce informatiche o quasi incidenti (senza che da tale notifica consegua la nascita di obblighi ulteriori).

Rispetto ai **poteri di vigilanza e di esecuzione**, la proposta di modifica della direttiva NIS distingue le misure di vigilanza o di esecuzione imposte ai soggetti essenziali e ai soggetti importanti prescrivendo agli Stati membri di provvedere affinché le autorità competenti abbiano il potere di compiere ispezioni ed audit, formulare richieste di informazioni ed accesso a dati e documenti, da un lato, e di emanare avvertimenti, istruzioni vincolanti ed ingiunzioni, imporre la designazione di un funzionario addetto alla sorveglianza con compiti ben definiti nell'arco di un periodo di tempo determinato, rendere una dichiarazione pubblica che identifica le persone fisiche e giuridiche responsabili della violazione di un obbligo stabilito dalla presente direttiva e illustra la natura di tale violazione, imporre a tali soggetti di informare le persone fisiche o giuridiche cui forniscono servizi o attività potenzialmente interessati da una minaccia informatica significativa in merito alle eventuali misure protettive o correttive che possano essere adottate da tali persone fisiche o giuridiche in risposta a tale minaccia, dall'altro.

A ciò si aggiunge la possibilità, offerta dalla direttiva, in relazione ai soggetti essenziali, di sospendere o chiedere a un organismo di certificazione o autorizzazione di sospendere un certificato o un'autorizzazione relativi a una parte o alla totalità dei servizi o delle attività forniti da un soggetto essenziale e di imporre o chiedere l'imposizione, da parte degli organismi o degli organi giurisdizionali pertinenti secondo le legislazioni nazionali, di un divieto temporaneo nei confronti di qualsiasi persona che svolga funzioni dirigenziali a livello di amministratore delegato o rappresentante legale in tale soggetto essenziale, e di qualsiasi altra persona fisica ritenuta responsabile della violazione, di svolgere funzioni dirigenziali in tale soggetto nel caso in cui e fino a quando il soggetto non abbia adottato le misure necessarie a porre rimedio alle carenze o a conformarsi alle prescrizioni dell'autorità competente per le quali le sanzioni sono state applicate.

Quanto alle **sanzioni**, la proposta detta i criteri e le condizioni generali per imporre sanzioni amministrative e sebbene confermi il potere degli Stati membri di procedere alla fissazione delle stesse, stabilisce che esse siano pari ad un massimo di almeno **10 milioni di euro** o **fino al 2% del fatturato totale annuo mondiale** dell'impresa interessata. Specifiche disposizioni sono dettate in relazione alle ipotesi di violazione dei dati personali.

La proposta disciplina, infine, le **procedure di assistenza reciproca** attivabili ogniqualvolta un soggetto essenziale o importante fornisca servizi in più di uno Stato membro o abbia lo stabilimento principale o un rappresentante in uno Stato membro, ma i suoi sistemi informatici e di rete siano ubicati in uno o più altri Stati membri prevedendo forme di cooperazione reciproca in funzione delle necessità del caso.

Come anticipato nel paragrafo precedente, nel pacchetto di proposte del 16 dicembre 2020 è

stata presentata anche una **proposta di direttiva sulla resilienza dei soggetti critici** che va a modificare la direttiva sulle infrastrutture critiche europee del 2008 estendendone sia l'ambito di applicazione, sia la profondità. Tale direttiva, in particolare, prescrive agli Stati membri l'adozione di una strategia nazionale, individua 10 settori (e sottosettori) di base da considerare (energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione e spazio) e prescrive una valutazione di tutti i rischi rilevanti, naturali e di origine umana, compresi i sinistri, le catastrofi naturali, le emergenze di sanità pubblica e le minacce antagoniste, inclusi i reati di terrorismo.

Nell'individuare i soggetti critici la normativa proposta fissa dei criteri e, in particolare, prescrive di valutare se il soggetto fornisce uno o più servizi essenziali, se la fornitura di tale servizio dipende da un'infrastruttura situata nello Stato membro e se un incidente avrebbe effetti negativi rilevanti sulla fornitura del servizio o di altri servizi essenziali nei settori indicati che dipendono da tale servizio.

Oltre a individuare i soggetti critici, gli Stati membri devono provvedere affinché questi predispongano e applichino un piano di resilienza o un documento o documenti di cui specifica i contenuti, oltre a fornire alla Commissione, entro tre anni dall'entrata in vigore della direttiva, e successivamente quando necessario e almeno ogni quattro anni, una relazione contenente i dati sui tipi di rischi individuati e sui risultati delle valutazioni dei rischi, per settore e sottosettore (prevedendo la possibilità di sviluppare un modello comune volontario per la presentazione di tali relazioni). A carico dei soggetti critici sono invece posti specifici obblighi di notifica nei confronti delle autorità competenti aventi ad oggetto il numero di utenti interessati dalla perturbazione o dalla potenziale perturbazione, la durata della perturbazione o la durata prevista di una potenziale perturbazione e l'area geografica interessata dalla perturbazione o dalla potenziale perturbazione.

Quanto al **modello di governance**, la proposta prescrive agli Stati membri la designazione di una o più autorità competenti responsabili della corretta applicazione e, se necessario, dell'esecuzione delle norme della direttiva a livello nazionale e l'individuazione di un punto di contatto unico che eserciti una funzione di collegamento per garantire la cooperazione transfrontaliera con le autorità competenti di altri Stati membri (ed invii annualmente una relazione di sintesi in merito alle notifiche ricevute, compresi il numero di notifiche e la natura degli incidenti notificati, e alle azioni intraprese alla Commissione e al gruppo per la resilienza dei soggetti critici) e con il gruppo per la resilienza dei soggetti critici, istituito da tale direttiva al fine di agevolare la cooperazione strategica e lo scambio di informazioni su questioni attinenti alla stessa direttiva.

1.3.2 Le iniziative per lo sviluppo e la sicurezza delle reti 5G

Se la crescente centralità assunta dai servizi digitali – alla quale peraltro la pandemia ancora in atto ha impresso una forza ed un vigore senza precedenti – ha posto l'accento sull'esigenza ormai davvero improcrastinabile di garantire lo sviluppo e l'ampia disponibilità di reti sicure e performanti, il 5G, quale attore abilitante un'ampia e variegata gamma di servizi di rilevanza straordinaria dal punto di vista economico e sociale (v. capitolo seguente), rappresenta una priorità assoluta per la Commissione. Tanto che la comunicazione "*Bussola digitale 2030: la via europea per il decennio digitale*" del marzo 2021 fissa come obiettivi di connettività al 2030 connessioni Gigabit per tutte le famiglie europee e lo sviluppo di reti 5G in tutte le zone abitate.

Nella logica di accelerare lo sviluppo delle

infrastrutture digitali, il 18 settembre 2020 la Commissione ha pubblicato la **Raccomandazione n. 2020/1307**, relativa a un pacchetto di strumenti comuni dell'Unione per ridurre i costi di installazione di reti ad altissima capacità e garantire un accesso allo spettro radio 5G tempestivo e favorevole agli investimenti, al fine di promuovere la connettività a sostegno della ripresa economica dalla crisi di COVID-19 nell'Unione.

Si tratta di un documento importante che, partendo dalla constatazione della necessità di garantire reti performanti e di sviluppare un approccio comune dell'Unione, persegue l'obiettivo di **incentivare lo sviluppo tempestivo di reti ad altissima capacità, comprese le reti in fibra ottica e le reti senza fili di prossima generazione** concentrandosi, in particolare, su tre finalità:

a) **ridurre il costo e accelerare le procedure di installazione delle reti di comunicazione elettronica** (in particolare di reti ad altissima capacità), razionalizzando le procedure di rilascio delle autorizzazioni, accrescendo la trasparenza e migliorando l'attività degli sportelli unici istituiti dalla direttiva sulla riduzione dei costi della banda larga, ampliando i diritti di accesso all'infrastruttura fisica esistente controllata da enti pubblici e individuando misure che contribuirebbero a ridurre l'impatto ambientale delle reti;

b) **fornire, ove opportuno, un accesso tempestivo allo spettro radio 5G** mediante incentivi destinati agli investimenti per l'uso dello spettro radio, come pure procedure tempestive di assegnazione dello spettro radio per le bande pioniere 5G;

c) **definire un processo di coordinamento più solido per l'assegnazione dello spettro radio**, che agevoli altresì la prestazione transfrontaliera di servizi 5G innovativi.

Nella logica di favorire lo scambio delle migliori pratiche tra gli Stati membri, dal punto di vista delle procedure, la raccomandazione:

1) incentiva il rispetto del termine di 4 mesi per il rilascio o il rifiuto delle autorizzazioni;

2) propone l'introduzione del principio del silenzio-assenso nonché l'istituzione di procedure accelerate di rilascio delle autorizzazioni e/o deroghe (definendo le tipologie di reti che ne potrebbero beneficiare);

3) incentiva l'istituzione e il rafforzamento del ruolo dello sportello unico quale unico canale di presentazione (telematica) delle domande.

Quanto allo **spettro e agli incentivi agli investimenti**, la raccomandazione invita da un lato a ridurre al minimo i rinvii delle procedure per la concessione dei diritti d'uso dello spettro radio e, dall'altro, evidenzia l'opportunità che gli Stati membri riferiscano su tutte le misure tese, tra l'altro, a combinare gli incentivi finanziari con obblighi o impegni formali per accelerare o ampliare la copertura senza fili di alta qualità e quelle tese a garantire, nel rispetto del diritto della concorrenza, la possibilità di condivisione delle infrastrutture attive e passive, nonché il dispiegamento congiunto delle infrastrutture. In relazione, infine, al miglioramento del coordinamento, a livello di Unione, la stessa raccomandazione pone l'attenzione sull'importanza di individuare casi d'uso di carattere transfrontaliero come trasporti e impresa manifatturiera e di coordinare le politiche di rilascio delle autorizzazioni nella logica di assicurare la continuità transfrontaliera del servizio (entro il 30 marzo 2022).

Rispetto alla roadmap da seguire, la raccomandazione ha fissato al **20 dicembre 2020** il termine per l'individuazione e la condivisione,

ad opera degli Stati membri, delle migliori pratiche e al 30 marzo 2021 la data entro cui finalizzare un accordo sul pacchetto di strumenti. La Commissione ha fissato, infine, al **30 aprile 2021** il termine per ciascuno Stato membro per trasmettere una tabella di marcia per l'attuazione del pacchetto di strumenti e al **30 aprile 2022** il termine per gli stessi Stati per riferire in merito all'attuazione degli stessi.

Nel rispetto della roadmap descritta, il 25 marzo 2021 gli Stati membri, in stretta collaborazione con la Commissione, hanno concordato un pacchetto di strumenti per la connettività a livello di Unione (***"Connectivity Toolbox"***) nel quale vengono indicate una serie di migliori pratiche per ridurre questi costi, promuovere l'accesso alle infrastrutture fisiche e snellire le procedure di concessione delle autorizzazioni per eseguire lavori civili. Nello specifico, il Toolbox incoraggia:

a) ad accrescere la disponibilità di informazioni sull'infrastruttura fisica esistente, le opere civili pianificate e le procedure di autorizzazione attraverso i punti di informazione unici o piattaforme equivalenti, nonché a promuovere la gestione elettronica di tutte le procedure di domanda di rilascio delle autorizzazioni;

b) a semplificare le procedure per l'installazione di elementi di rete, in particolare rilevanti per il 5G, prevedendo il meccanismo del silenzio-assenso ed offrendo agli operatori un accesso più ampio alle infrastrutture pubbliche (in linea con quanto già previsto dal codice europeo delle comunicazioni elettroniche per le *small cells*);

c) a rendere più trasparenti ed efficienti i meccanismi di risoluzione delle controversie tra gli attori coinvolti;

d) ad intraprendere iniziative per limitare gli effetti ambientali negativi e migliorare la sostenibilità delle reti;

e) a realizzare regolari revisioni delle strategie nazionali di gestione dello spettro ed accelerare la conclusione delle procedure di assegnazione delle bande destinate al 5G e la promozione di misure che incentivino l'uso dello spettro ed il lancio del 5G;

f) ad adottare misure coordinate che supportano la connettività wireless per casi d'uso industriali, anche con una dimensione transfrontaliera;

g) a promuovere regimi autorizzatori flessibili sulla banda 26 GHz con particolare attenzione per le licenze locali e la condivisione delle infrastrutture;

h) a combinare incentivi finanziari con obblighi di copertura in considerazione delle specifiche esigenze dello Stato membro e della relativa situazione del mercato;

i) promuovere a livello nazionale e di UE ricerca scientifica e campagne informative al fine di contrastare a resistenza sociale allo sviluppo delle reti 5G; l) implementare le misure contenute nel Toolbox (è fissato al 30 aprile 2022 il termine per l'invio di un report sui progressi nell'implementazione stessa).

Se queste iniziative sono tese ad accelerare lo sviluppo delle reti, non sono mancati interventi tesi ad accrescere **la sicurezza delle reti 5G**. Ed infatti, nel febbraio 2020 la Commissione ha pubblicato la Comunicazione "*Dispiegamento del 5G sicuro - Attuazione del pacchetto di strumenti dell'UE*" e del pacchetto di strumenti dell'UE (Toolbox sul 5G) che, come noto, affronta tutti i rischi individuati nella relazione coordinata sulla loro valutazione, individuando e descrivendo una serie di misure strategiche e tecniche, nonché di corrispondenti azioni di sostegno volte a

rafforzare la loro efficacia e che possono essere attuate per attenuarli.

Quanto alle misure, il pacchetto ha identificato:

1) **8 misure strategiche**, comprendenti il rafforzamento dei poteri normativi delle autorità per l'esame dell'approvvigionamento e dello spiegamento della rete, misure specifiche per affrontare i rischi legati a vulnerabilità non tecniche (ad esempio, rischio di interferenza da parte di un Paese terzo o rischi di dipendenza), nonché possibili iniziative per promuovere una catena di approvvigionamento e di valore 5G sostenibile e diversificata, al fine di evitare rischi sistemici di dipendenza a lungo termine;

2) **11 misure tecniche**, comprendenti misure per rafforzare la sicurezza delle reti e delle attrezzature 5G e, in particolare, la sicurezza delle tecnologie, del software, dei processi, delle persone e dei fattori fisici.

A sostegno di tali misure, lo stesso documento ha individuato **una serie di azioni di supporto** che si sostanziano, tra le altre, nel rivedere o sviluppare linee guida e best practice sulla sicurezza della rete, rinforzare le capacità di test e controllo a livello nazionale ed europeo, supportare la standardizzazione, scambiare le migliori pratiche sull'attuazione delle misure strategiche (in particolare le discipline nazionali per la valutazione del profilo di rischio dei fornitori), garantire che i progetti di implementazione del 5G sostenuti con finanziamenti pubblici tengano conto dei rischi per la sicurezza informatica e assicurare l'applicazione di misure di sicurezza tecniche e organizzative standard attraverso uno specifico schema di certificazione a livello europeo. La sezione certamente più complessa del documento è rappresentata dal paragrafo 4.2 dove per ciascuna delle nove aree di rischio identificate nella relazione sulla valutazione coordinata a livello di UE dei rischi, il pacchetto individua dei **piani di mitigazione del rischio**, consistenti nella combinazione di misure strategiche e/o tecniche (insieme ad appropriate azioni di supporto) che vengono classificate in quattro livelli, sulla base di una valutazione che considera il rischio da fronteggiare e il rischio persistente dopo l'applicazione della misura stessa.

Nel tracciare le conclusioni, il pacchetto ha invitato gli Stati membri ad attuare misure e disporre di poteri per attenuare i rischi, rafforzando i requisiti di sicurezza per gli operatori delle reti mobili, valutando il profilo di rischio dei fornitori, applicando restrizioni adeguate ai fornitori considerati ad alto rischio, comprese le necessarie esclusioni per gli asset critici, garantendo che ogni operatore disponga di un'adeguata strategia multifornitore per evitare o limitare l'eventuale forte dipendenza da un unico fornitore ed evitare la dipendenza da fornitori considerati ad alto rischio.

A luglio 2020 è stato pubblicato da parte del gruppo di cooperazione NIS, con il sostegno della Commissione e dell'ENISA, un report sui progressi degli Stati membri nell'attuazione del toolbox sulla sicurezza 5G in cui si fa il punto sul livello di maturità raggiunto dai vari Paesi nell'implementazione delle misure contenute nel Toolbox. Ciò che è emerso, dal report, è che sebbene tutti gli Stati membri abbiano iniziato a rivedere e rafforzare le loro misure di sicurezza in vista del 5G, in alcuni paesi questo lavoro è ancora in corso e, pertanto, non sono ancora state adottate misure definitive.

A livello generale, il rapporto evidenzia che **i tre principali rischi individuati sono l'errata configurazione delle reti, la mancanza di controllo degli accessi e le interferenze statali attraverso la catena di fornitura del 5G**. Per quanto riguarda quest'ultimo, evidenzia la convinzione, diffusa tra gli Stati, della mancanza di misure adeguate esistenti.

Per quanto riguarda la dipendenza dai singoli fornitori, il rapporto evidenzia la necessità di comprendere il coinvolgimento dei diversi fornitori nei singoli elementi della rete, la difficoltà tecnica e operativa di applicare una strategia multi-vendor in alcuni punti della rete, il numero limitato di fornitori 5G, le maggiori criticità per i paesi più piccoli, i possibili effetti sugli operatori derivanti dalla formulazione di richieste diversificate ai fornitori e la necessità di individuare specifiche basi normative che consentano di imporre determinati obblighi ai fornitori.

Interessanti anche le considerazioni relative all'implementazione di misure per garantire la sicurezza delle reti 5G. Su questo specifico punto, il documento, dopo aver definito il livello medio-basso di maturità raggiunto nell'implementazione di tali misure, descrive un panorama piuttosto diversificato dove, tuttavia, emerge la richiesta da parte di molti Stati membri di un approccio coordinato agli standard UE. Il termine per stabilire se siano necessarie ulteriori azioni per gli Stati, in collaborazione con la Commissione, è scaduto il 1° ottobre 2020.

1.3.2.1 La tutela della sicurezza delle reti nei maggiori Paesi europei

La recente accelerazione del digitale, non solo in quanto mercato ma anche come fattore trasversale di trasformazione delle economie nazionali e globali, lo ha elevato ad elemento necessario ed abilitante per la crescita e lo sviluppo. La complessità delle tecnologie utilizzate, gli ingenti investimenti necessari per sostenere un'adeguata infrastruttura, l'elevato dinamismo e il grado di innovazione del mercato contribuiscono a rendere questo settore di grande valore strategico nella definizione degli equilibri economici e politici mondiali.

In questa prospettiva si cala l'iniziativa regolatoria e legislativa dell'Unione europea, che punta a supportare la formazione di un ambiente sicuro e stabile per lo sviluppo florido del settore digitale continentale. Quello della **sicurezza** è infatti un tema particolarmente sensibile poiché, nella definizione dei requisiti richiesti per poter operare nei vari Paesi, si mescolano istanze di natura geopolitica ad interventi che influiscono direttamente sulle dinamiche del mercato.

Al fine di comprendere a pieno le politiche messe in atto dall'Unione europea risulta dunque importante comprendere quali sono i contesti nazionali in cui le iniziative continentali dovranno essere applicate e quali invece le posizioni assunte dai principali Paesi al di fuori dall'Unione.

Dall'analisi del contesto relativo alla sicurezza cibernetica di Francia, Germania, Spagna e Regno Unito si osserva come l'architettura nazionale dei singoli Paesi comprenda attori di diversa natura, che vanno dagli organi governativi agli istituti di intelligence, e come il panorama regolatorio continentale sia ancora in fase di definizione, in particolare in relazione alle iniziative legislative in materia di tecnologie di quinta generazione.

Francia

Nel 2015, la Francia si è dotata di una **strategia nazionale di sicurezza cibernetica** con l'obiettivo di facilitare la transizione digitale e permettere al tessuto imprenditoriale di innovarsi in un contesto protetto da minacce esterne, al passo con la digitalizzazione e all'altezza del resto dell'economia globalizzata.

Nel 2017, il Primo Ministro ha affidato al **Segretariato Generale per la Difesa e la Sicurezza Nazionale** (SGDSN, organo interministeriale alle dipendenze del Primo Ministro Francese) il compito di integrare il documento precedente con una strategia di respiro internazionale che confermasse la centralità del ruolo del Governo.

Nello specifico, in seno all'SGDSN si trova l'**ANSSI,**

ovvero l'Agenzia Nazionale della Sicurezza delle reti e dell'informazione, organo istituito nel 2009 che occupa un ruolo pivotale nell'architettura francese di cybersecurity. L'Agenzia è responsabile della prevenzione e della reazione ad incidenti informatici ai danni delle istituzioni sensibili e contribuisce all'orientamento della ricerca nazionale ed europea nel campo della sicurezza dei sistemi informativi. Inoltre, dal 2013 l'ANSSI ha la possibilità di imporre misure di sicurezza e controlli sui sistemi di informazione sensibili degli operatori di Importanza di Vitale (OIV).

I compiti dell'ANSSI in materia di Lotta Informatica Difensiva dello Stato (LID) sono limitati dallo spazio di azione del Ministero della Difesa attraverso il COMCYBER, un comando operativo composto da tutte le forze di cyber defence degli eserciti, delle direzioni e dei servizi, sulle quali effettua una supervisione organica o funzionale. A loro volta, le competenze del COMCYBER in ambito militare sono limitate dai servizi di intelligence del Ministero delle Forze Armate e dell'Interno. Le operazioni di ANSSI e COMCYBER, e quindi dei domini civili e militari, sono coordinate dal Centro di Coordinamento delle Crisi Cyber (C4), che riunisce tutti i soggetti interessati, consente di condividere quotidianamente l'analisi delle minacce e permette di attuare la risposta più consona in relazione all'entità dell'attacco.

Per quanto riguarda le **infrastrutture di rete**, la legge n.2019-810 modifica il modo in cui gli operatori di rete mobili (MNO) possono gestire le reti 5G ed interviene sulla regolamentazione delle autorizzazioni intorno ad esse, in particolare imponendo che, per poter usare apparecchiature hardware e software per la connessione alla rete radiomobile francese, gli operatori coinvolti nei settori critici debbano ottenere un'autorizzazione preventiva da parte del Presidente del Consiglio dei Ministri.

Per quanto concerne l'**impatto della regolamentazione** sulle dinamiche del mercato è importante sottolineare che, nonostante la norma sia da applicare solo relativamente alle reti 5G, i vincoli tecnici che derivano dalla compatibilità di queste ultime con le infrastrutture legacy costituiscono un fattore determinante per il deployment delle nuove reti.

Germania

L'architettura istituzionale di sicurezza cibernetica approvata nel 2016 assegna ampie responsabilità all'**Ufficio Federale per la Sicurezza Informatica (BSI)** e al **Ministero dell'Interno**. Il BSI agisce sul piano operativo per la protezione dei network federali, conduce le indagini relative agli attacchi informatici e si occupa di mettere in atto le strategie difensive. Parallelamente, il MAD, ovvero il servizio di controspionaggio militare, gestisce la reazione ad eventuali eventi malevoli e crisi del dominio cibernetico nazionale ed ha inoltre la possibilità di ricorrere ad azioni di natura offensiva.

Per quanto riguarda l'impianto legislativo, centrale importanza ha **la legge IT SiG 2.0 (IT Sicherheitsgesetz)**, approvata dal Parlamento tedesco nell'aprile del 2021, che da una parte aggiorna il precedente IT Security Act, e dall'altra armonizza la realtà tedesca alla direttiva europea NIS sulla sicurezza informatica.

La nuova norma identifica ed amplia il perimetro delle cosiddette **infrastrutture critiche**, prendendo in considerazione non soltanto quelle di particolare interesse pubblico, ma anche i cyber-critical operators, ovvero tutti quegli istituti il cui malfunzionamento causerebbe, seppur in maniera indiretta, problemi alle infrastrutture critiche.

Con l'introduzione dell'IT SiG 2.0, inoltre, il BSI acquista ulteriori poteri di consulenza e controllo, tra cui la possibilità di stabilire dei requisiti minimi per la sicurezza informatica, di pubblicare

standard tecnici per i prodotti digitali e di svolgere test di sicurezza con l'obiettivo di garantire ai consumatori un livello di rischio basso nell'utilizzo di prodotti e sistemi IT.

Un'ulteriore novità è rappresentata dall'introduzione di un meccanismo di **assesment sulla sicurezza dei componenti delle infrastrutture critiche**. La Germania non prevede l'esclusione ex-ante di alcun vendor, ma lascia in capo al BMI, presso il Ministero dell'Interno, il potere di richiedere un periodo di valutazione delle apparecchiature di 2 mesi, consentendo anche la rimozione delle apparecchiature ex-post qualora queste rappresentino un pericolo per l'ordine pubblico o per la sicurezza della Repubblica Federale.

Spagna

Il sistema istituzionale di sicurezza cibernetica spagnolo si regge da una parte sulla figura del Primo Ministro, il quale detiene la presidenza del **Consiglio di Sicurezza Nazionale (CSN)**, e dall'altra delega i compiti operativi ai ministeri, differenziando le responsabilità in base agli ambiti di competenza. In particolare, il **Ministero degli Affari Economici e della Trasformazione Digitale** opera attraverso l'**Incibe-Cert** come centro di risposta per incidenti di sicurezza digitale a cittadini e imprese, mentre il **Ccn-Cert**, nell'ambito del Ministero della Presidenza, si occupa degli attacchi diretti alle istituzioni governative. A questi si aggiungono l'**Espdef-Cert**, operante nell'ambito del Ministero della Difesa, che gestisce un team di risposta alle emergenze informatiche, e l'**OCC**, che agisce in seno al Ministero dell'Interno e svolge attività di coordinamento dei Cert nazionali.

Per quanto riguarda l'ambito normativo, in Spagna vige il **Regio Decreto Legislativo 14/2019**, il quale regola, in materia di amministrazione digitale, la tutela della pubblica sicurezza. In particolare, l'articolo 6 della legge conferisce al Governo speciali poteri di intervento sulle infrastrutture, le risorse ed ogni elemento associato alle reti e ai servizi di comunicazione elettronica in caso di minaccia all'ordine pubblico o alla sicurezza nazionale.

Inoltre, in Spagna è attualmente in discussione il **disegno di legge sulla Cybersecurity 5G**, che ha l'obiettivo di garantire la sicurezza dell'infrastruttura legata alla nuova tecnologia specialmente per quanto riguarda la manipolazione dei dati e le intercettazioni da parte di agenti esterni. Il disegno di legge prevede anche nuovi obblighi in capo agli operatori di rete, tra cui condurre di un'analisi del rischio ogni due anni, esaminare le pratiche di sicurezza adottate dai propri fornitori, lavorare su un sistema di misure tecniche e organizzative per la gestione del rischio e adottare una strategia di differenziazione della fornitura.

L'approccio spagnolo sembra voler subordinare l'utilizzo di un'apparecchiatura, programma o servizio 5G esterno al previo conseguimento di una certificazione prevista dal regolamento europeo sulla sicurezza informatica, mantenendo un approccio neutrale nei confronti dei fornitori.

Regno Unito

Fuoriuscita dall'Unione europea, la Gran Bretagna sembra spingersi sempre di più verso la sfera d'influenza statunitense, anche (forse soprattutto) sul versante della Difesa, sia fisica (si veda Aukus), sia cibernetica.

Per quanto concerne il secondo ambito, il **National Cyber Security Centre (NCSC)** è uno dei principali attori istituzionali in materia di sicurezza cibernetica del Regno Unito. L'NCSC è un'agenzia governativa alle dipendenze del Government Communication Head Quarter (GCHQ), ne ha assorbito le competenze relative allo spazio cibernetico ed è responsabile della protezione delle reti IT, della riservatezza dei dati e del contrasto degli attacchi cyber. Opera nell'ambito

dei 13 settori critici[2] per il funzionamento dei servizi essenziali all'ordine pubblico ed è supportato a livello operativo dal CNI Hub.

Attualmente è in discussione in Parlamento un **rafforzamento delle misure in materia di cybersecurity**, in particolare attraverso il Telecommunication (Security) Bill, una legge che ha l'obiettivo di riformare l'impianto di sicurezza delle reti di telecomunicazione sul territorio nazionale nell'ottica di imporre requisiti all'entrata e rigidi controlli di sicurezza.

Il dibattito che ha portato alla stesura del disegno di legge è iniziato nel luglio 2019, con la pubblicazione della **Telecom Supply Chain Review**, un documento che consiste in una valutazione degli accordi di fornitura esistenti, e che ha posto l'accento sulle problematiche relative alla sicurezza e resilienza, specialmente riguardo alla valutazione dei rischi e al timore di far dipendere l'intero mercato nazionale da un numero troppo ristretto di fornitori.

In questo contesto, l'NCSC ha pubblicato a gennaio 2020 delle **raccomandazioni formali sul ricorso agli High Risk Vendors (HRV)**, suggerendo l'introduzione di un tetto massimo del 35% sulle quote di mercato per il ricorso a HRV e l'esclusione di questi soggetti ad alto rischio dalle parti sensibili delle reti. Successivamente, in linea con la decisione degli Stati Uniti di inserire il fornitore cinese Huawei nell'Entity List , l'NCSC ha presentato una raccomandazione agli operatori TLC del Regno Unito, indicando di interrompere l'acquisto di nuove apparecchiature Huawei entro la fine del 2020 e di rimuoverle del tutto dalle reti del Regno Unito entro la fine del 2027.

Parallelamente, il Segretariato di Stato per il Digitale, Cultura, Media e Sport del Regno Unito ha pubblicato a novembre 2020 la **5G Supply Diversification Strategy**, la quale poggia su alcuni principi chiave, tra cui il disaggregamento della catena di produzione, la promozione dell'interoperabilità delle infrastrutture, la distribuzione della supply chain globale in diverse regioni, la trasparenza degli standard e la priorità della sicurezza e della resilienza delle reti.

Il **Telecommunication (Security) Bill** attualmente in discussione costituisce il dispositivo attraverso cui il Governo intende rafforzare i poteri degli enti già esistenti, coinvolgendo in particolare l'**autorità indipendente di regolamentazione dei servizi di comunicazione (Ofcom)**. L'Ofcom otterrebbe infatti strumenti e responsabilità per garantire il rispetto della normativa di settore, tra cui la possibilità di richiedere ai fornitori di apparecchiature di rete di eseguire specifici test, emettere notifiche di violazione, indicare misure provvisorie per colmare lacune di sicurezza e, in caso di inadempienza, imporre sanzioni pecuniarie, mentre verrebbero spostati dal Parlamento all'Esecutivo alcuni nuovi poteri che consentono di stabilire specifici requisiti di sicurezza e codici di condotta.

[2] Identificati dal CPNI sono: difesa, servizi, emergenze, governo, salute (settori pubblici), chimico, nucleare civile, comunicazioni, energia, finanza, alimentare, trasporti, acqua (settori privati).

CAPITOLO 2

LO SVILUPPO DELLA BANDA LARGA E ULTRA-LARGA FISSA E MOBILE. LO STATO DELL'ARTE DELLE DIVERSE TECNOLOGIE IN EUROPA

2.1 LE INFRASTRUTTURE DI RETE FISSA

L'evoluzione tecnologica che ha caratterizzato gli ultimi anni e la straordinaria diffusione dei servizi digitali che è conseguita alla pandemia e, dunque, alla necessità, da un lato, di fare ricorso in maniera massiccia a smart working, didattica a distanza, telemedicina, approvvigionamento online di beni e servizi essenziali e non, per garantire la continuità delle attività socioeconomiche e, dall'altro, alle mutate abitudini degli individui sempre più orientati alla fruizione online di giochi e contenuti, hanno mostrato con una forza senza precedenti quanto sia indispensabile garantire l'ampia disponibilità per cittadini, imprese e P.A. di reti performanti, in grado di supportare servizi digitali sempre più sofisticati e di sostenere anche repentini incrementi di traffico quali quelli registrati ovunque durante il lockdown.

Nonostante il generale avanzamento del processo di digitalizzazione anche in quei Paesi, come l'Italia, che scontano un tradizionale ritardo nell'utilizzo dei servizi digitali, permangono ancora **importanti differenze** non solo, prevedibilmente, tra le diverse aree del mondo, ma anche all'interno del contesto europeo. Si tratta di diversità che necessitano di essere analizzate soprattutto alla luce degli ambiziosi obiettivi di connettività fissati dall'UE e, a cascata, dai singoli Stati membri.

Risulta cruciale, dunque, nel valutare il grado di maturità digitale raggiunto dai Paesi europei, l'**analisi dei dati concernenti coperture e *take up* delle reti fisse e mobili** la cui disponibilità ed accessibilità rappresentano, evidentemente, una pre-condizione per accedere al mondo digitale ed alle opportunità che esso offre.

Partendo dall'analisi dei dati di copertura e *take up* relativi alle reti fisse, posto che ormai praticamente tutti i Paesi UE hanno completato il processo di sviluppo della banda larga (Fig. 2.1) con la Lituania che, essendosi concentrata sul deployment della banda ultra-larga, si posiziona ultima con l'84,8% delle famiglie coperte, a fronte di una media europea dell'97,4% (99,6% in Italia), la domanda rivela un andamento più lento.

E infatti, la Fig. 2.2 mostra la percentuale di famiglie connesse alla broadband nell'Unione ed il primato dei Paesi Bassi con il 97% delle famiglie connesse alla broadband. All'altro estremo della classifica invece troviamo Lituania e Portogallo con l'82%, seguiti da Grecia e Bulgaria con rispettivamente 80 e 79% di famiglie connesse alla broadband. Il dato italiano - 87% - si rivela sostanzialmente in linea con il dato europeo (89%).

I dati riportati in Fig. 2.3 mostrano, invece, il tasso annuo di crescita composto (CAGR, *Compound*

Figura 2.1 Copertura in banda larga (% famiglie, 2020)

Fonte: Eurostat

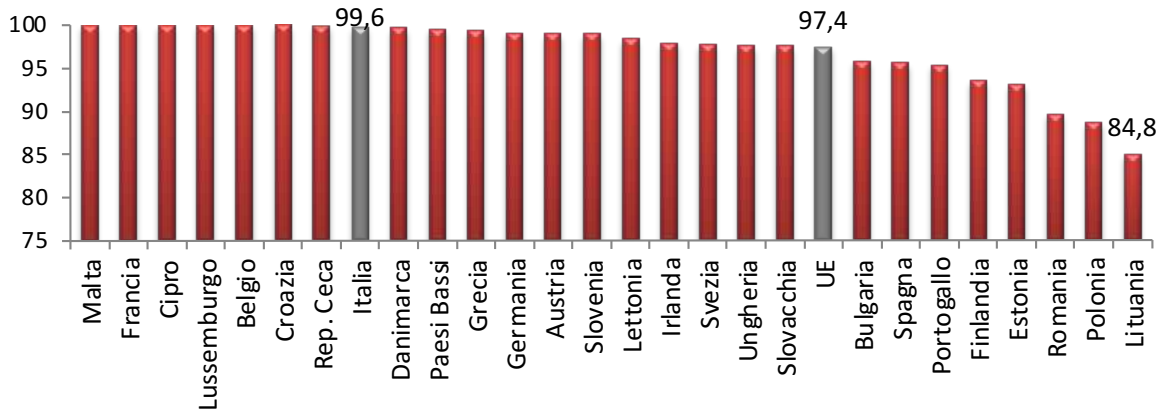


Figura 2.2 Percentuale di famiglie connesse alla banda larga (2020)

Fonte: Eurostat
*dato 2019

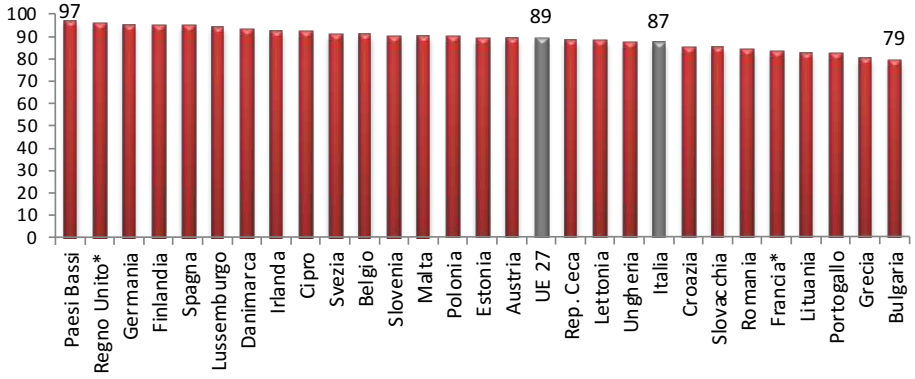
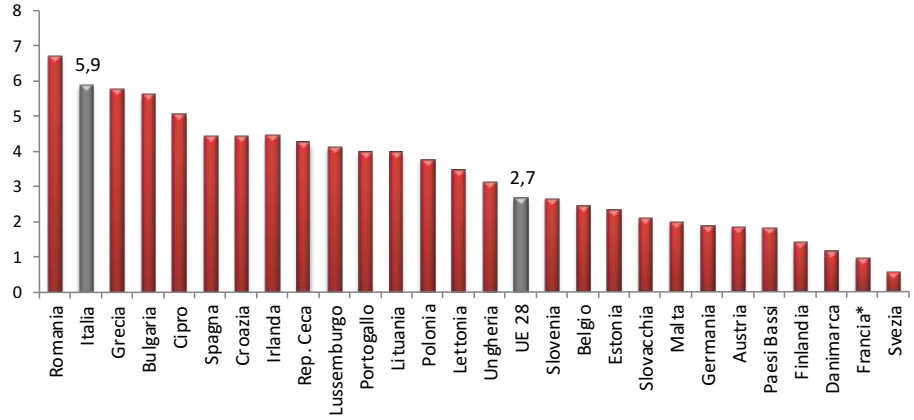


Figura 2.3 Crescita dal 2012 al 2020 (CAGR) della percentuale di famiglie connesse alla broadband a livello UE (%)

Fonte: Elaborazione I-Com su dati Eurostat



Annual Growth Rate) dal 2013 al 2020[3] dei Paesi dell'Unione europea, evidenziando come l'Italia, con il 5,9% presenti un CAGR più del doppio di quello europeo pari al 2,7%, che le consente di posizionarsi seconda a livello europeo.

Ultimi nell'UE, invece, i Paesi nordici che tradizionalmente sono i più digitalizzati e, dunque, inevitabilmente, con tassi di crescita inferiori.

La **positiva performance italiana** emerge manifestamente nella Fig. 2.4 che, mostrando la relazione sussistente tra la percentuale di famiglie connesse alla broadband e tasso annuo di crescita, colloca il nostro Paese decisamente al di sopra della linea di tendenza, a dimostrazione dell'importanza dei progressi compiuti.

Se il dato nazionale rivela progressi incoraggianti, andando ad analizzare i singoli contesti regionali (Fig. 2.5), **il primato nel 2020 spetta ancora una volta alla Provincia autonoma di Trento** con il 93%, seguita da Friuli-Venezia Giulia e Lazio con il 91% ed Emilia Romagna con il 90%.

A chiudere la classifica regionale, invece, le regioni del Sud ed in particolare Puglia e Basilicata (80%), Sicilia e Molise (78%) e Calabria (76%).

[3] Dal punto di vista metodologico si segnala che il dato francese del 2020 non è disponibile e, dunque, si è provveduto ad utilizzare quello del 2019 mentre il dato UE utilizzato per il 2020 è quello UE27.

Figura 2.4 Tasso di crescita delle famiglie connesse alla broadband

Fonte: Elaborazione I-Com su dati Eurostat

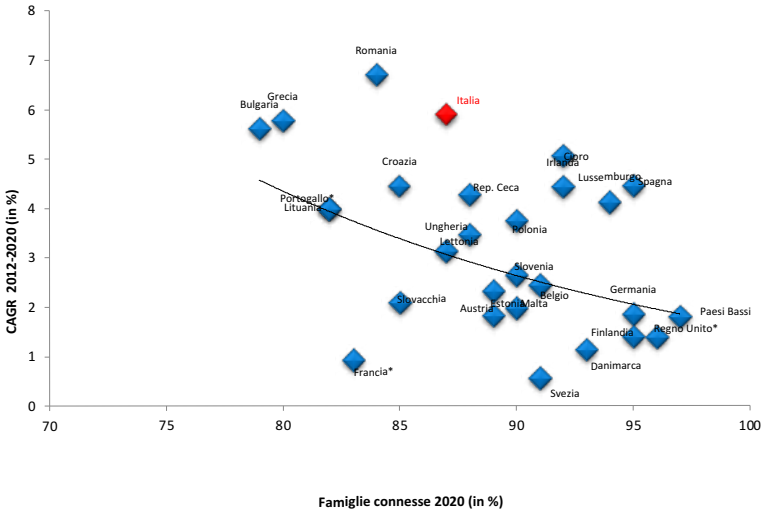
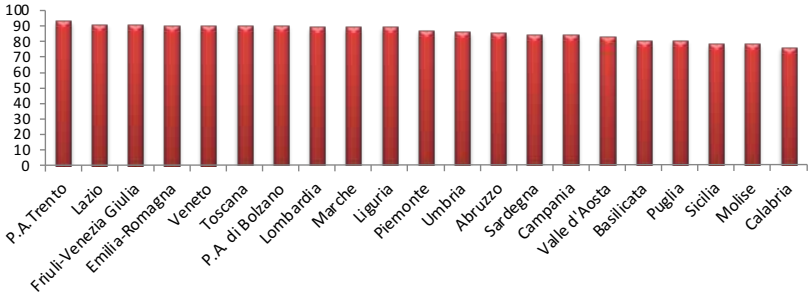


Figura 2.5 Famiglie connesse alla broadband nelle regioni italiane (valori in %, 2020)

Fonte: Istat



Tornando al contesto europeo, alla luce dell'accelerazione impressa all'utilizzo dei servizi digitali dalla pandemia che ha mostrato la praticabilità di soluzioni mai percorse in passato (vedi lo smart working come ordinaria modalità di organizzazione del lavoro) e in considerazione degli ultimi approdi regolamentari (v. Codice europeo delle comunicazioni elettroniche) che iniziano a configurare la connettività come un diritto universale, è interessante verificare il livello di copertura raggiunto nelle **aree rurali**. Queste ultime, in particolare, se da un lato risultano dotate di ottimi livelli di copertura standard, con un dato UE che si attesta all'89,7% (Fig. 2.6), risultano ancora molto indietro se si guarda alla copertura VHCN[4] (Fig. 2.7). E infatti, sebbene vi siano punte di eccellenza europee con Malta – dove la copertura VHCN delle aree rurali è pari al 100% – e Lussemburgo – che segue con l'80,8% – **a livello UE la copertura è ferma al 27,8%**.

L'Italia, in linea con l'andamento generale, registra un ottimo posizionamento rispetto alla copertura standard con una percentuale del 98,2% ben superiore rispetto alla media, mentre sconta un grave ritardo con riguardo alla copertura VHCN rispetto alla quale la percentuale è meno di 1/3 di quella UE (8,4% a fronte del 27,8%).

Considerata la crescente complessità tecnologica e le dinamiche di crescita della domanda di servizi digitali, è indispensabile verificare lo stato di

[4] FTTH, FTTB and Cable Docsis 3.1.

Figura 2.6 Copertura broadband fissa nelle aree rurali (valori in %, 2020)

Fonte: Eurostat

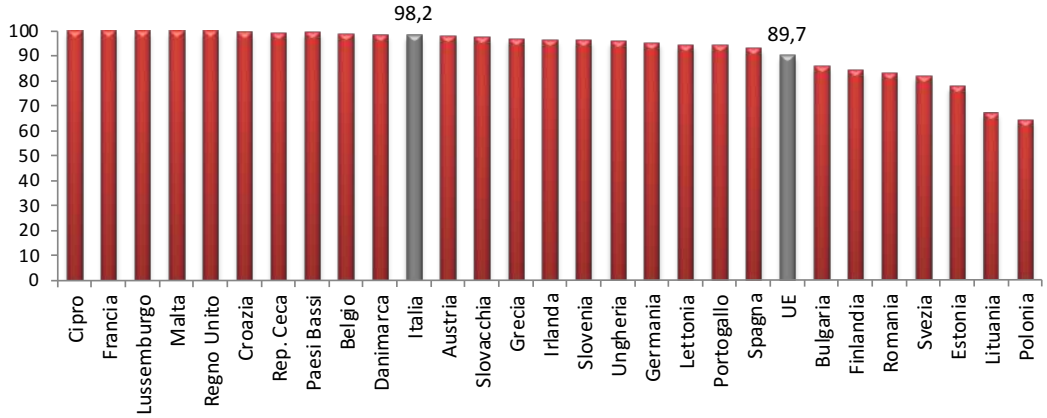
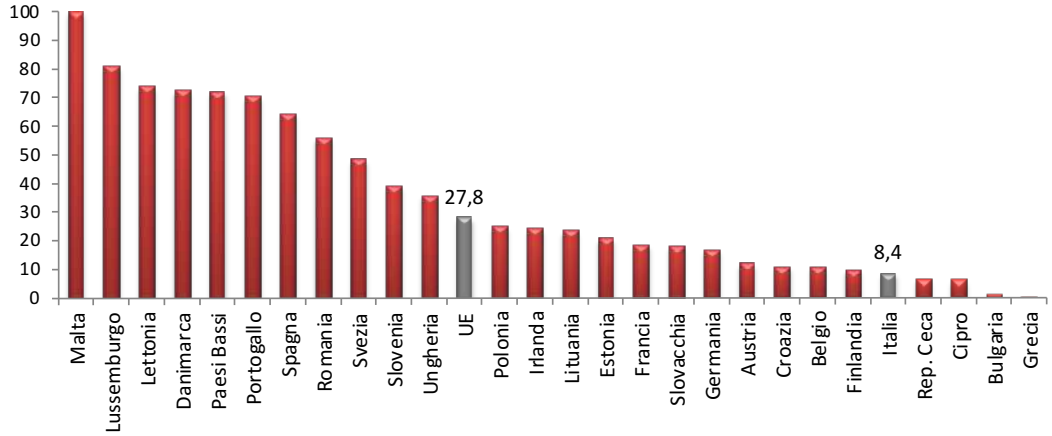


Figura 2.7 Copertura VHCN nelle aree rurali (valori in %, 2020)

Fonte: Eurostat



sviluppo e diffusione della banda ultra larga.

Quando alla **copertura NGA** – che comprende le tecnologie FTTH, FTTB, Docsis 3.0 VDSL ed altre tecnologie che garantiscono almeno 30 Mbps in download – la Fig. 2.8 mostra una grande maturità a livello generale, con un dato UE che si attesta all'87,2% e la metà degli Stati membri che registrano scoperture superiori al 90%. Le percentuali inferiori riguardano Lituania e Francia dove la copertura si attesta al 70,8% e 69%. **L'Italia, con il 92,7% si posiziona oltre 5 p.p. al di sopra della media europea**.

Il dato italiano 2020 di copertura NGA testimonia i grandi progressi realizzati dal nostro Paese grazie agli investimenti messi in campo ed alle politiche adottate dal 2015, anno in cui è stata varata dal Governo la Strategia nazionale per la Banda Ultra Larga, da ultimo sostituita dal Piano Italia 1 Giga, di cui si parlerà approfonditamente nel corso dell'analisi. La percentuale di copertura NGA è infatti più che raddoppiata, passando dal 43,8% al 92,7%, con un incremento di 48,9 punti percentuali.

Tale importante accelerazione può essere espressa dal tasso di crescita: il nostro Paese, infatti, ha registrato, in termini relativi, i maggiori progressi, con un **incremento dell'866%** a fronte

Figura 2.8 Copertura NGA (% di famiglie, 2020)

Fonte: Digital Agenda Scoreboard

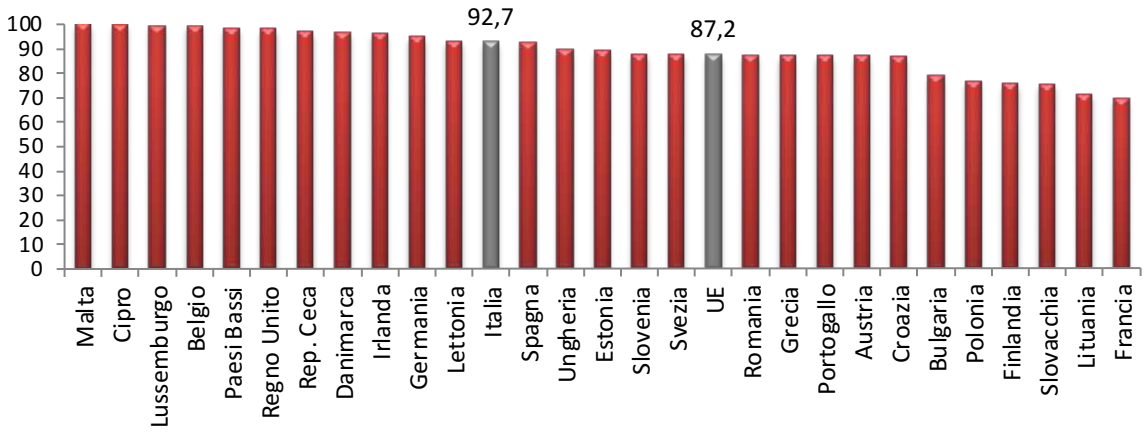
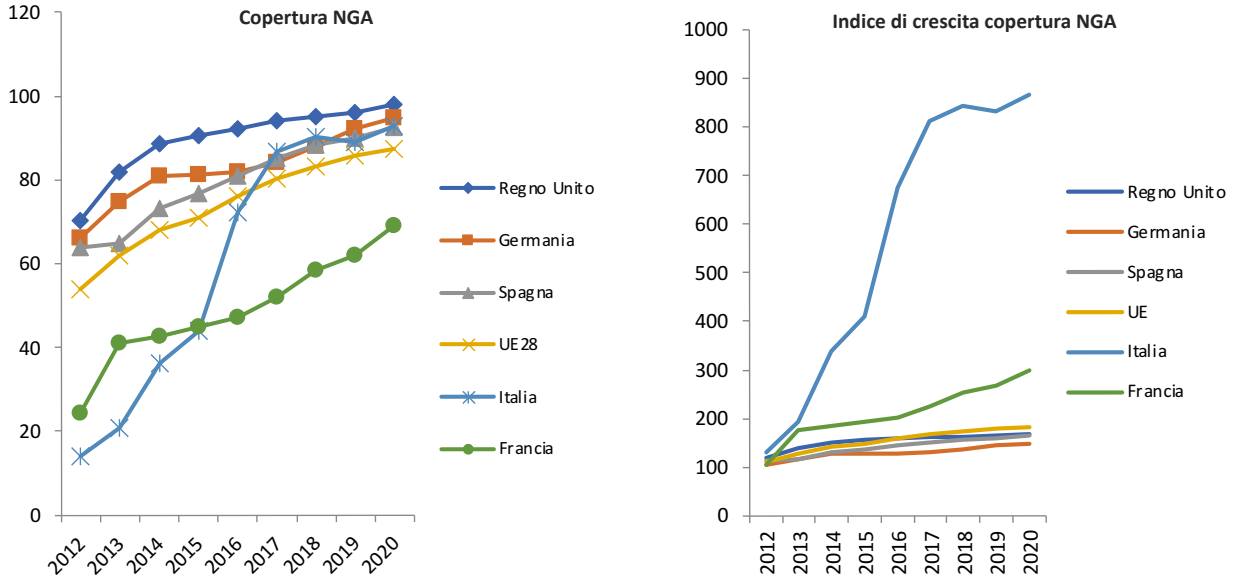


Figura 2.9 Grado di copertura NGA (% famiglie)

Fonte: Elaborazione I-Com su dati Commissione europea



di tassi che non vanno oltre il 297% della Francia (Fig. 2.9).

Sebbene il dato complessivo testimoni uno sforzo significativo nello sviluppo infrastrutturale nel nostro Paese, l'analisi della copertura con tecnologie VHCN (FTTH, FTTB and Cable Docsis 3.1) ed FTTP impone maggiori cautele.

La Fig. 2.10 rivela **una copertura con tecnologie VHCN in Italia nel 2020 ferma al 34%**, al di sotto della media europea del 59% e a distanza siderale dai Paesi best performer Malta, Lussemburgo e Danimarca per i quali le percentuali di copertura si attestano rispettivamente al 100%, 95% e 94%.

Anche i dati relativi all'FTTP rilevano un ritardo del nostro Paese (Fig. 2.11).

La percentuale italiana si ferma al 33,7%, quasi 10 p.p. al di sotto della media europea che si attesta a 42,5%) e lontanissima dalle percentuali registrate in Lettonia, Spagna e Portogallo (rispettivamente 88,1%, 84,9% e 82,3%).

Figura 2.10 Copertura VHCN (% famiglie, 2020)

Fonte: Digital Agenda Scoreboard

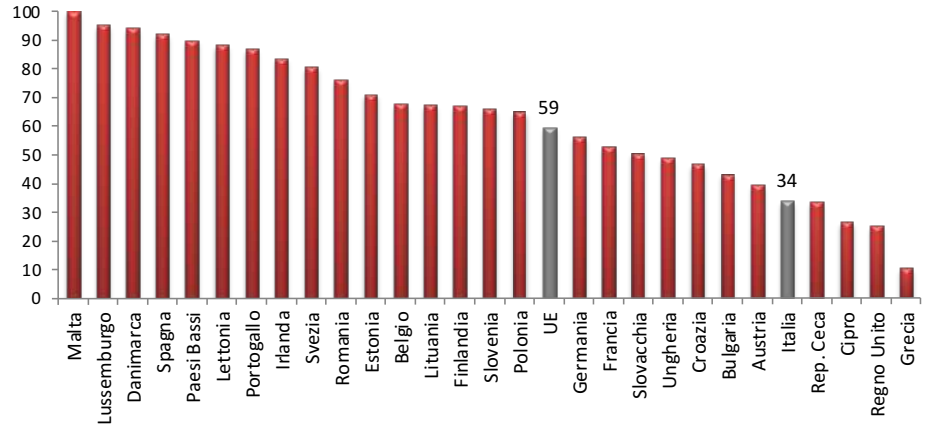
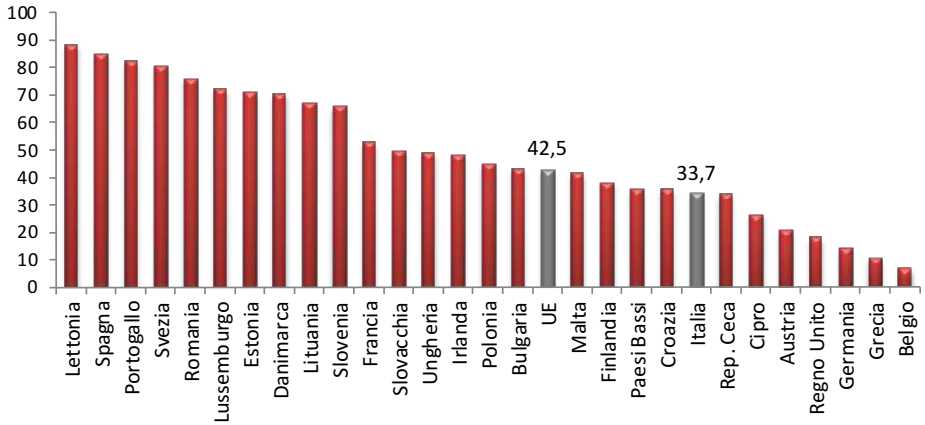


Figura 2.11 Copertura FTTP (% famiglie, 2020)

Fonte: Digital Agenda Scoreboard



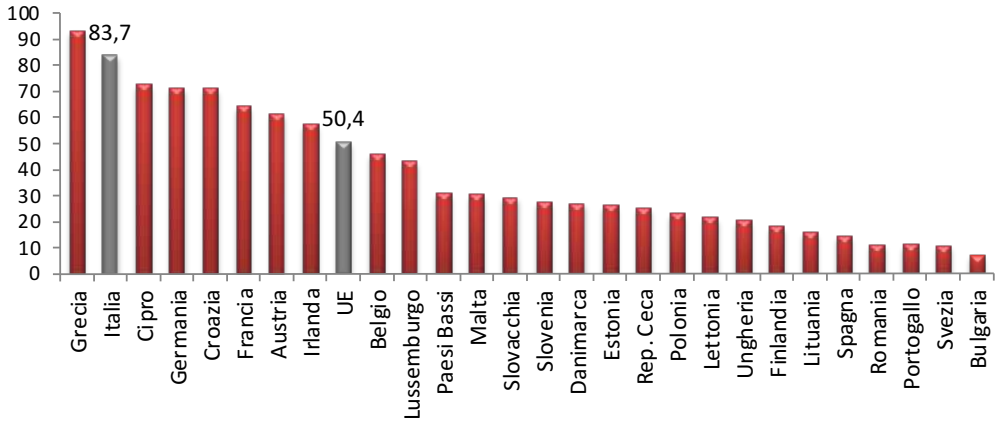
Si tratta di una situazione che, secondo le stime, è destinata ad essere superata nel breve periodo. Infatti, le previsioni dell'FTTH Council Europe, pubblicate a maggio 2021 nello studio "*FTTH/B Market Panorama in Europe*", indicano che, entro il 2026, 197 milioni di abitazioni in UE27+Uk saranno raggiunte dall'Ftth/Fttb, con un incremento del 67% rispetto a quanto si stima per **il 2021 (118 milioni) mentre l'Italia, dal 2020 al 2026, registrerà un +136%**, pari a 26 milioni di case coperte dalla fibra. Questi tassi di crescita consentiranno all'Italia di posizionarsi al quarto posto nell'Europa dei 39 Paesi considerati, dopo il Regno Unito, che viaggia a ritmi del +488%, la Germania (+385%) e i Paesi Bassi (+144%).

Se nel complesso appaiono positivi i progressi in atto nel nostro Paese lato offerta, **le dinamiche della domanda, al contrario, continuano a destare gravi preoccupazioni**.

E infatti, sebbene sia ampia e sempre crescente la disponibilità di reti di ultima generazione, a giugno 2020 in Italia ben l'83,7% degli abbonamenti fissi concerneva ancora linee DSL (Fig. 2.12). Si tratta di una tendenza decisamente più marcata rispetto al resto d'Europa, dove la percentuale si ferma al 50,4%, e che vale al nostro Paese la seconda posizione, dopo la Grecia. Assolutamente marginale, invece, il ruolo del DSL nei paesi del Nord e dell'Est Europa (questi ultimi,

Figura 2.12 Abbonamenti DSL sul totale degli abbonamenti fissi (%, giugno 2020)

Fonte: Digital Agenda Scoreboard



d'altronde, partendo da una situazione iniziale di particolare arretratezza, hanno investito direttamente nelle reti di ultima generazione).

In linea con tale dato la percentuale di abbonamenti in fibra (FTTH, FTTB e FTTP con esclusione di quelli FTTC) sul totale degli abbonamenti (Fig. 2.13) in Italia è pari al 10,1%, molto lontana dal valore OECD (30,6%) e distante anni luce da Finlandia, Portogallo e Lussemburgo dove le percentuali si attestano, rispettivamente, al 57,3%, 55,1% e 50,2%.

Tale dato, secondo le stime dell'FTTH Council Europe, è destinato purtroppo a essere confermato negli anni a venire. Si prevede, infatti, che **nel 2026 ben 19,8 milioni di famiglie non si saranno abbonate alla fibra** nonostante la disponibilità delle nuove reti (a far peggio sarà, secondo le stime, solo la Russia). Questo grave ritardo di adozione si rispecchia nei dati relativi alla velocità degli abbonamenti broadband fissi

Figura 2.13 Percentuale di connessioni in fibra sul totale degli abbonamenti broadband (dicembre 2020)

Fonte: OECD

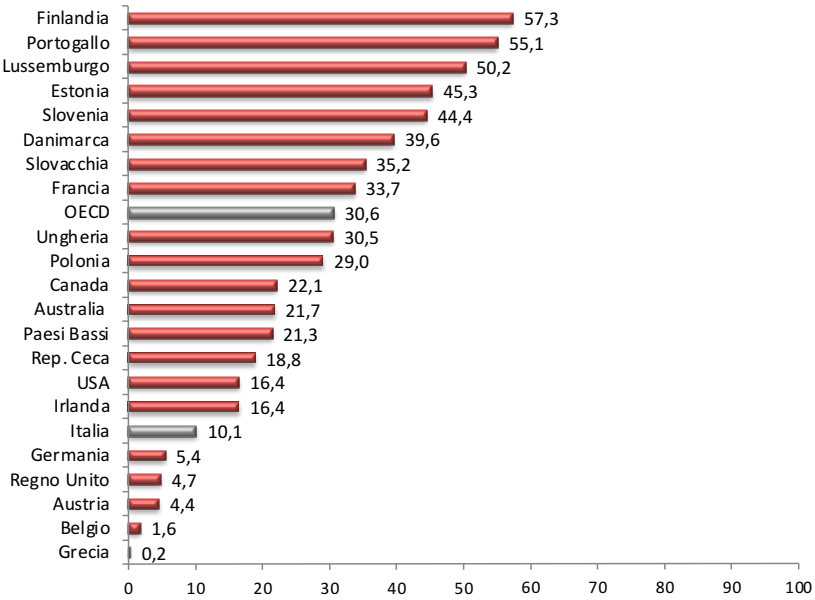
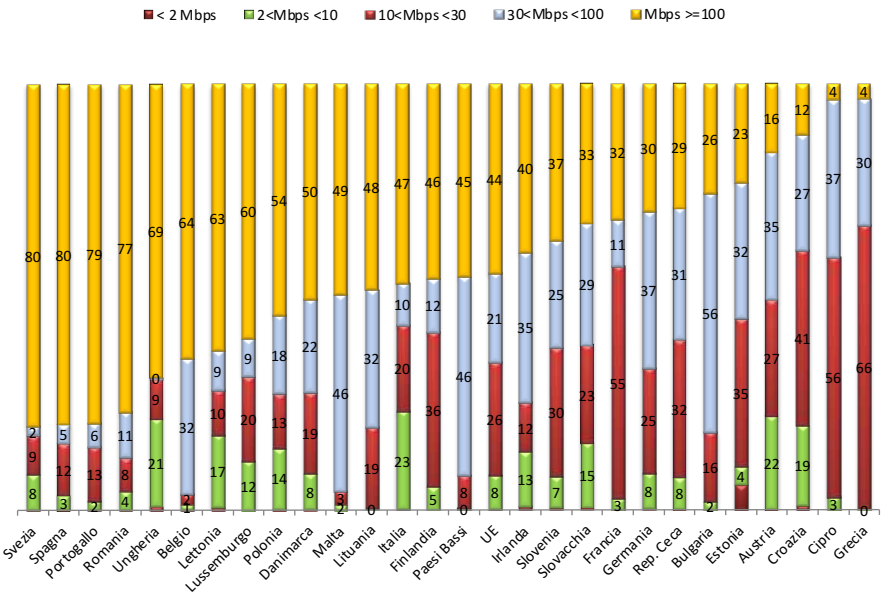


Figura 2.14 Velocità degli abbonamenti broadband (%, 2020)

Fonte: Digital Agenda Scoreboard



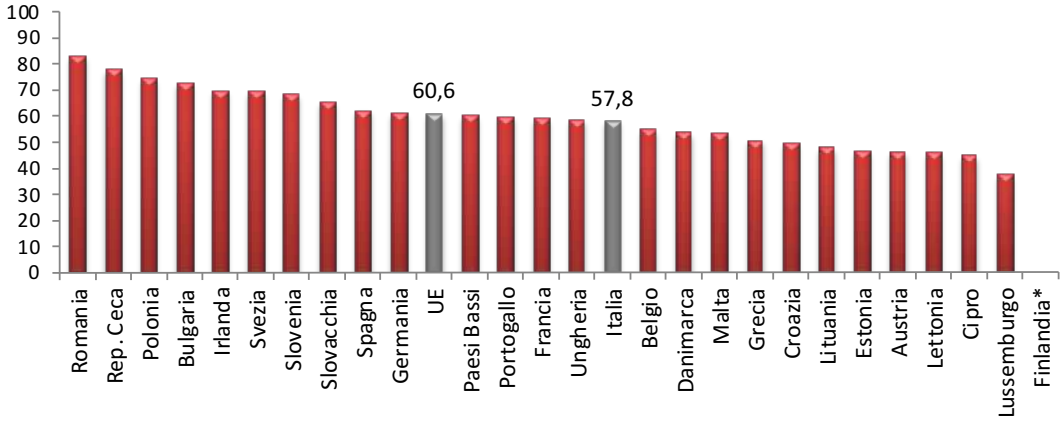
nel 2020 che nel 53% dei casi è in Italia inferiore ai 100 Mbps (Fig. 2.14).

Considerato che la maturità di un Paese si misura anche nella dinamicità del mercato, per completezza è interessante verificare il grado di dinamicità dei singoli mercati nazionali analizzando, nello specifico, le quote di mercato dei nuovi entranti nel **mercato broadband fisso** (Fig. 2.15). I dati aggiornati a giugno 2020 confermano, in particolare, secondo una tendenza consolidata ormai da diversi anni, una buona dinamicità del mercato romeno e quello ceco con valori decisamente superiori alla media europea (82,7% e 78% a fronte del dato UE, 60,6%).

I Paesi che si pongono all'estremo opposto della classifica sono invece Lettonia, Cipro e Lussemburgo, dove le quote di mercato dei nuovi entranti si sono fermate rispettivamente al 45,4%, 44,5% e 37,1% a dimostrazione di quanto forte sia

Figura 2.15 Quote di mercato dei nuovi entranti nel mercato broadband fisso europeo (%, 2019)

Fonte: Fonte: Eurostat
*n.d.



ancora la presenza degli incumbent. Anche l'Italia rivela un dato - 57,8% - sostanzialmente stabile rispetto al 2019 ed ancora al di sotto della media europea.

2.2 LE INFRASTRUTTURE DI RETE MOBILE

Se il processo di diffusione delle reti a banda ultra larga fissa sta raggiungendo un certo grado di maturità nell'Ue, **il segmento mobile sta vivendo un'epoca di profonda trasformazione** grazie allo sviluppo ed alla graduale diffusione delle reti 5G per le quali è enorme l'interesse a livello globale ed europeo.

Si tratta, infatti, di uno standard in grado di assicurare performance inedite in termini di latenza e numero di dispositivi gestibili che, pertanto, si presenta come fattore abilitante un'enorme e variegata gamma di servizi che offriranno a cittadini, imprese e P.A. straordinarie opportunità ed enormi benefici.

Prima di focalizzare l'attenzione sul contesto europeo e verificare la performance italiana, è interessante commentare qualche dato globale che fornisce un'idea di quali sia lo stato dell'arte e le tendenze per il futuro. A tale riguardo, il *Mobility Report* di Ericsson, pubblicato a giugno 2021, fornisce una panoramica molto interessante dell'andamento delle connessioni mobili nel mondo (in particolare 5G).

A livello generale, il report registra circa **8 miliardi di abbonamenti mobili** di cui ben 6, alla fine del 2020, riguardavano smartphone. Tale numero continuerà a crescere, secondo le stime, per attestarsi a 7,7 miliardi nel 2026, con un peso dell'88% sul totale degli abbonamenti mobili.

Lo stesso report quantifica in **160 il numero di fornitori di servizi che hanno lanciato offerte commerciali 5G** e segnala una crescita degli abbonamenti con device 5G nel primo quadrimestre dell'anno di ben 70 milioni (quantificando il numero complessivo in 290 milioni) stimando, per il 2026, 580 milioni di abbonamenti 5G.

Considerate le tendenze mondiali, è interessante ora analizzare le stime relative al mix tecnologico delle reti mobili nel prossimo futuro. A tal fine, i dati contenuti nella Fig. 2.16 offrono una panoramica globale dell'attuale mix tecnologico nonché delle prospettive stimate al 2025.

Il dato che emerge è una **fortissima accelerazione del 5G** che, secondo le stime GSMA, nel 2025 si attesterà a quota 71% nell'aera Asia Pacifico, 48% in Cina, 35% in Europa e addirittura 51%, superando il 4G, in Nord America. Si tratta di numeri importanti, quelli che vedremo affermarsi nei prossimi 5 anni, se si considera che al 2020 la Cina, che rivela il dato migliore, si ferma al 12%.

Stesso trend positivo, anzi ulteriormente rafforzato probabilmente anche dal fatto che la stima guarda al 2026 e, dunque, ai prossimi sei anni, è riportato nel *Mobility Report* di Ericsson dello scorso giugno, nel quale emerge con forza l'affermazione del 5G nelle diverse aree del mondo (Fig. 2.17).

Molto interessanti, soprattutto alla luce degli ambiziosi obiettivi di copertura fissati a livello UE e della necessità, fortemente acutizzata dalla pandemia, di garantire in tempi rapidi e a costi sostenibili, la disponibilità di reti performanti, le evidenze e le stime fornite dal *Mobility Report* rispetto all'**FWA (Fixed Wireless Access)**. Quest'ultima, infatti, è una tecnologia che utilizza un sistema ibrido di collegamenti via cavo e senza fili per offrire servizi di connettività in banda larga e ultra larga. Il cavo, generalmente in fibra ottica, arriva fino alla stazione radio base (detta BTS) che emette un segnale senza fili per raggiungere il terminale ricevente (un'antenna posta in prossimità del domicilio dell'utente) che a sua lo distribuirà all'interno dell'abitazione. La rete mista (fibra/rame da un lato e tecnologia radio

Figura 2.16 Mix tecnologico delle reti mobili per area geografica (2020 - 2025)

Fonte: GSMA, 2020

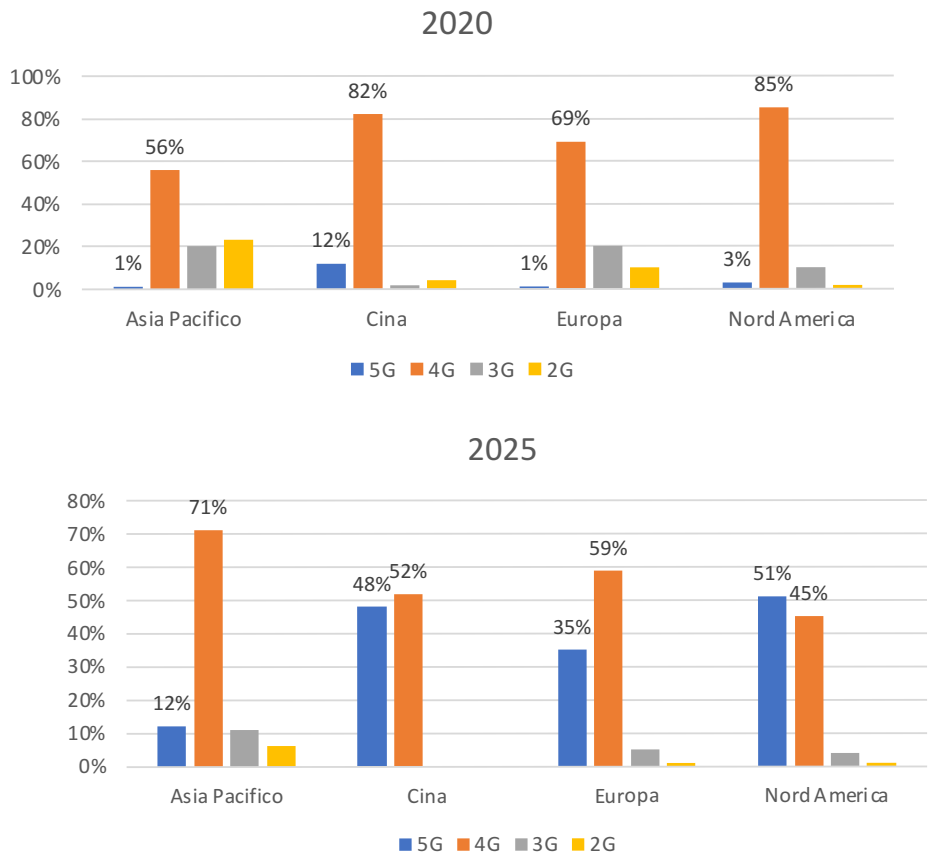
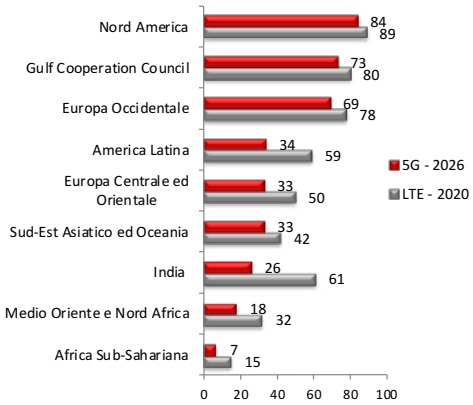


Figura 2.17 Abbonamenti mobili per area geografica (2020 – 2026)

Fonte: Mobility Report, Ericsson



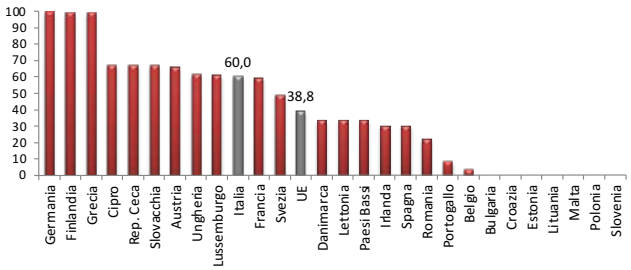
dall'altro) costituisce, dunque, un'alternativa più economica e flessibile rispetto a quella tradizionale, in particolare per le zone montane, rurali e a bassa densità abitativa, non servite da una rete cablata in grado di arrivare fino in casa dell'utente e in cui sarebbe anti-economico costruirla.

Il *Mobility Report* quantifica, in particolare, in oltre 60 milioni le connessioni FWA nel mondo nel 2020, stimando una crescita di circa 20 p.p. annui fino al 2026, anno in cui quando tali connessioni giungeranno quota 180 milioni. Le connessioni FWA 5G, invece, sono stimate salire a 70 milioni entro il 2026. Del traffico mobile globale, quello su reti FWA si attesta al 15% alla fine del 2020 per superare, secondo le stime, il 20% nel 2026.

Le opportunità offerte da tale tecnologia si stanno traducendo in un forte interesse da parte dei fornitori di servizi. Il report in esame, in particolare, riferisce che su 311 fornitori analizzati, 224, ossia il 72%, hanno un'offerta commerciale FWA, con un incremento di 12 p.p.

Figura 2.18 5G readiness (2020)

Fonte: Eurostat

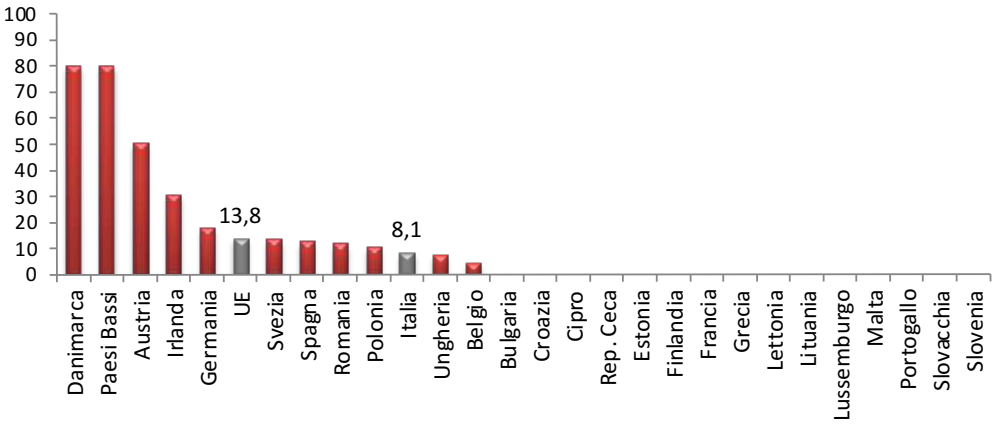


rispetto ai sei mesi precedenti (percentuale raddoppiata rispetto al dicembre 2018). La percentuale sale al 90% nel caso di fornitori che hanno lanciato offerte 5G.

Tornando ora al contesto europeo ed alle prospettive presenti e future di sviluppo del 5G, i dati mostrano, da un lato, un buon grado di "*5G readiness*", essendo in molti casi giunte a completamento le procedure di assegnazione delle frequenze pioniere destinate al 5G (Fig. 2.18); dall'altro, un certo ritardo nella copertura 5G. E infatti, le uniche punte di eccellenza sono rappresentate da Danimarca e Paesi Bassi dove la copertura è già all'80%, seguite da Austria e

Figura 2.19 Copertura 5G (2020)

Fonte: Eurostat



Irlanda con un comunque lodevole 50% e 30%. Per il resto, **ben 15 Paesi risultano sprovvisti di copertura 5G** nel 2020, mentre l'Italia si ferma all'8,1% (Fig. 2.19).

Mentre il processo di sviluppo delle reti 5G in Europa è ancora alle prime battute, il 3G ed il 4G rappresentano, ormai, standard consolidati in tutta l'Ue. **La copertura 4G, in particolare, nel 2020 rasenta il 100%** in quasi tutti gli Stati membri (99,3% in Italia), attestandosi, a livello UE, al 99,7% (Fig. 2.20).

Se i dati appena commentati dimostrano una certa omogeneità dell'offerta in tutti i paesi UE rispetto agli standard più consolidati, lato domanda, al contrario, si registra una maggiore varietà. E infatti, guardando alle SIM attive ogni 100 persone (Fig. 2.21), si passa dalle 190,3, 160,5 e 155,5 rispettivamente di Polonia, Estonia e Finlandia, alle 78,1, 76,4 e 75,2 rispettivamente di Malta, Portogallo ed Ungheria. **L'Italia, con 93,6, si pone al di sotto della media europea di 103,8**.

Anche rispetto al mondo delle **imprese** i dati europei dimostrano diversi gradi di maturità rispetto al tema della connettività. E infatti, gli ultimi dati disponibili – anno 2019 – relativi alla

Figura 2.20 Copertura 4G (LTE), (% di famiglie, 2020)

Fonte: Digital Agenda Scoreboard

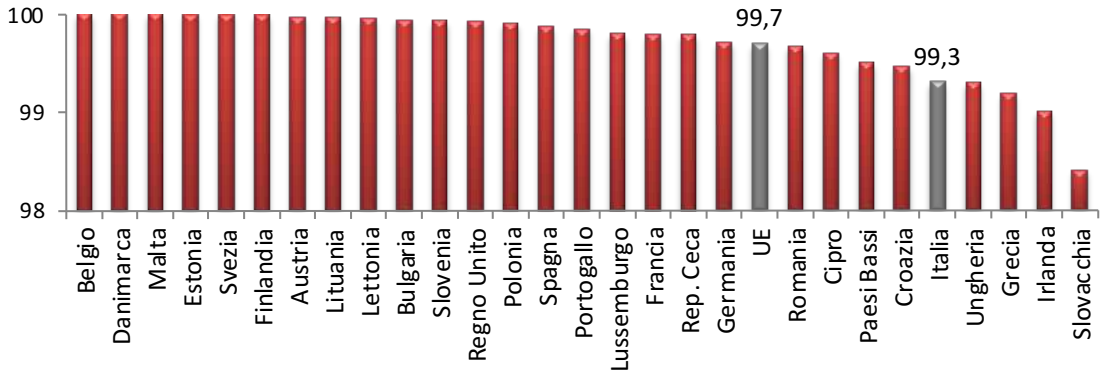


Figura 2.21 Numero di SIM mobili attive ogni 100 persone (giugno 2020)

Fonte: Digital Agenda Scoreboard

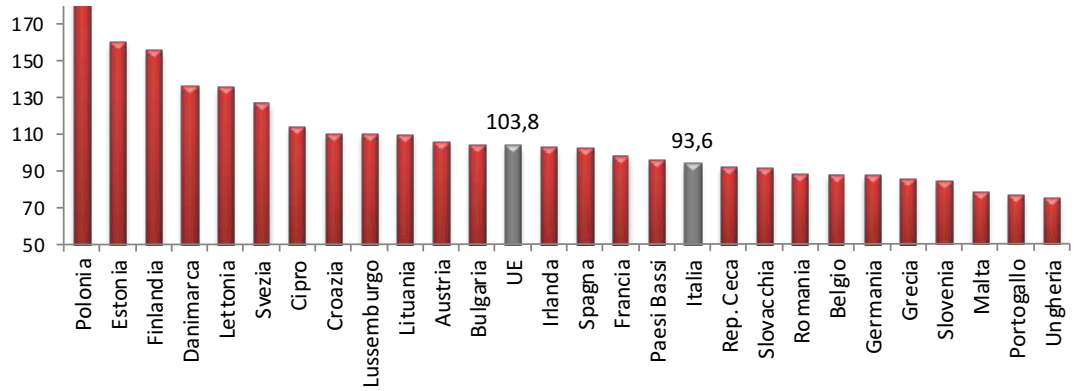
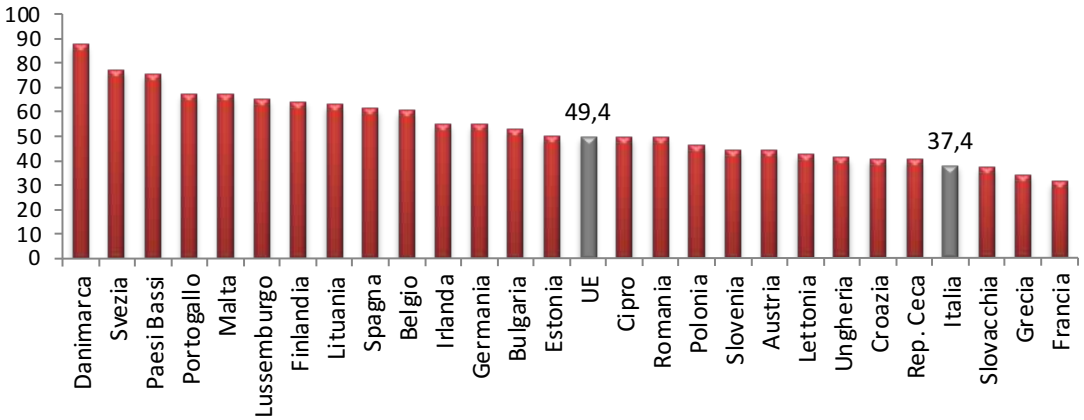


Figura 2.22 Imprese con una connessione fissa veloce (almeno 30 Mbps, 2019)

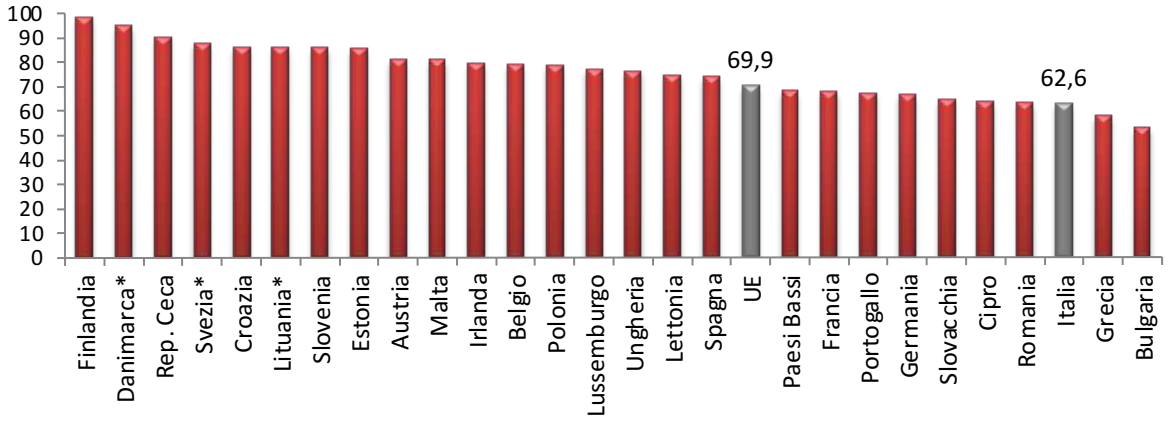
Fonte: Digital Agenda Scoreboard



percentuale di imprese (che impiegano almeno 10 persone e con esclusione del settore finanziario) che hanno una connessione fissa veloce (almeno 30 Mb/s), passano dall'87,1% della Danimarca, best performer, al 30,7% della Francia. La performance italiana non appare particolarmente brillante con una percentuale che si attesta al 37,4% a fronte della media UE del 49,4% (Fig. 2.22).

Figura 2.23 Imprese che dotano parte del personale di device mobili (%, 2020)

Fonte: Digital Agenda Scoreboard



Meno marcate le differenze rispetto alla media europea se si guarda al mobile e, in particolare, alla percentuale di imprese (della medesima tipologia e con le medesime esclusioni riportate in relazione alla figura precedente) che dotano parte del proprio personale di device mobili. Il 62,6% delle imprese italiane rientranti nel campione hanno dotato parte del personale di device mobili, a fronte di una media del 69,9% (Fig. 2.23).

2.2.1 Lo stato dell'arte del 5G a livello internazionale

Nel corso del 2021, l'Europa ha effettuato una serie di passi in avanti nell'ambito del 5G, tra cui l'assegnazione di molteplici frequenze tramite l'indizione di alcune aste nazionali e il lancio del servizio da parte di un gran numero di operatori. Per quanto concerne i secondi, **i servizi 5G risultano attualmente disponibili in tutti i Paesi dell'Europa a 27, a esclusione di Portogallo**[5] **e Lituania**.

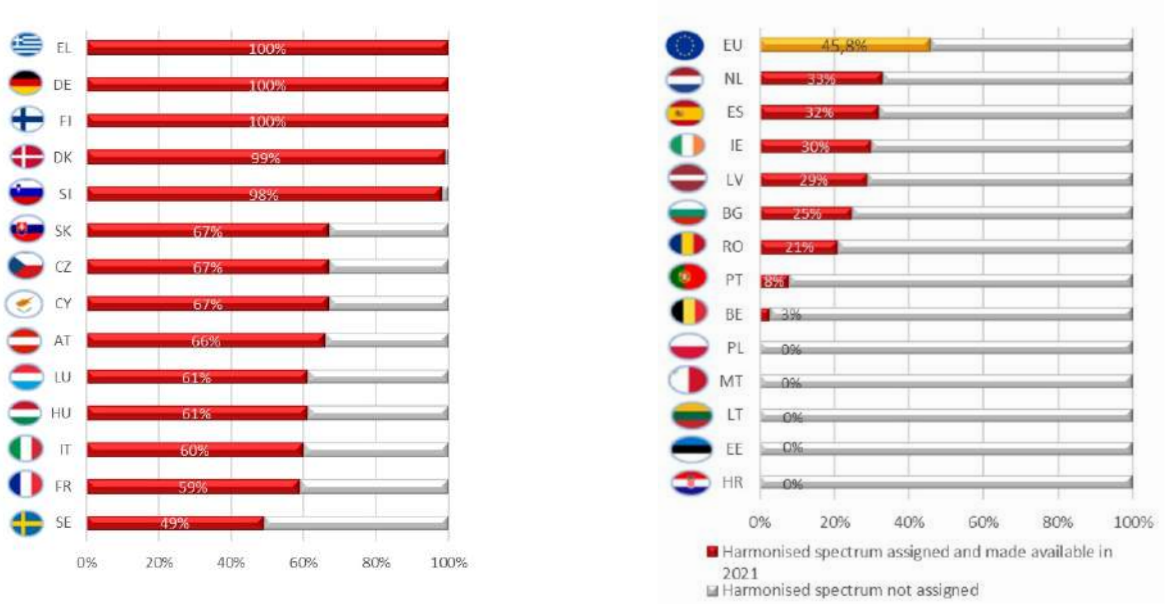
Oltre al Regno Unito, ormai divenuto un Paese extra-UE – e primo Paese con quattro operatori su quattro a fornire servizi 5G – presentano l'*en plein* in termini di offerta (tutte con quattro operatori su quattro) anche la Danimarca, la Francia, l'Italia, la Spagna e la Svezia. Fornitura completa, relativamente ai tre operatori presenti in ognuno di essi, anche per Austria, Finlandia, Grecia, Irlanda, Lussemburgo, Olanda, Repubblica Ceca.

A livello extra-europeo, secondo le stime del *5G Observatory*, a giugno 2021 avevano lanciato servizi 5G oltre **180 operatori** (+100 rispetto a giugno 2020, ad ulteriore riprova del fermento in atto nel settore). Negli Usa i quattro principali operatori hanno lanciato il servizio tra il 2018 e il 2019, mentre in Sud Corea e Cina forniscono connettività 5G i tre maggiori player locali. Anche in Giappone tre operatori "*storici*" (NTT Docomo, KDDI e Softbank) già offrono il servizio da marzo 2020, mentre il newcomer Rakuten ha effettuato il lancio lo scorso settembre.
A livello di policy, alla fine di marzo 2021 la Commissione ha pubblicato un pacchetto di strumenti per la connettività comprendente 39 casi di best practice proposte dagli Stati membri. La roadmap prevedeva l'approvazione di una tabella di marcia da parte di ogni Stato entro aprile 2021 e una comunicazione sullo stato di implementazione del toolbox entro aprile 2022.

[5] L'asta multibanda (700/900/1800/2100/2600/3600 MHz) promossa da Anacom, dopo esser stata rinviata più volte, è iniziata a marzo e, al 29 settembre 2021, risulta ancora in corso di svolgimento. L'Autorità ha modificato le regole per accelerare le procedure, mentre il 27 settembre Vodafone Portugal ha presentato ricorso proprio in relazione a tali modifiche.

Figura 2.24 Indicatore DESI sull'assegnazione delle bande pioniere 5G

Fonte: 5G Observatory, giugno 2021



Scopo dell'iniziativa è facilitare la diffusione dell'infrastruttura 5G riducendo i costi e l'onere normativo.

Per quanto concerne le **sperimentazioni 5G**, alla fine di giugno 2021 la banda di frequenza più testata in Europa è stata di gran lunga la banda da 3.6 GHz (69% dei test).

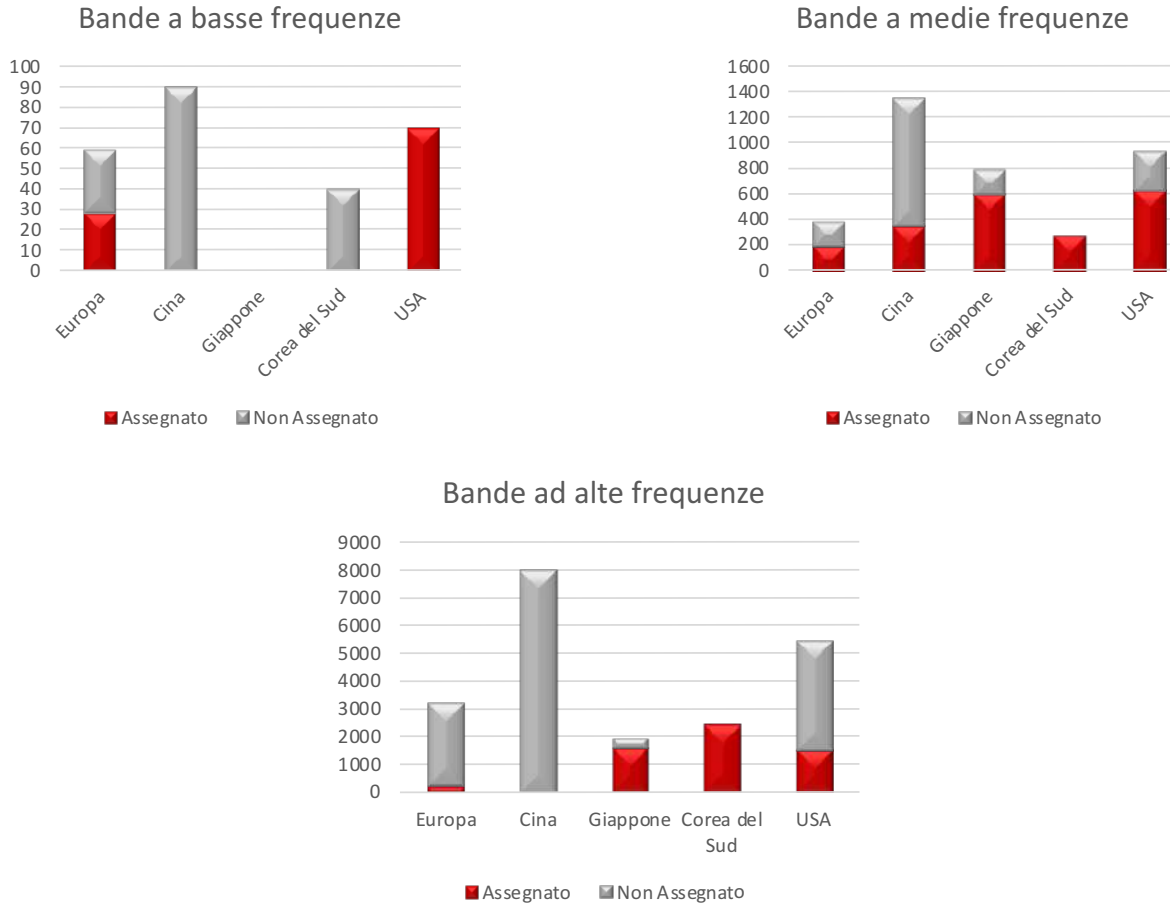
Per quanto concerne lo **stato di assegnazione delle frequenze** (Fig. 2.25), tre Paesi risultavano in testa a giugno 2021, con la totalità delle frequenze pioniere assegnate nelle tre bande individuate (700 MHz, 3.4-3.8 GHz, 26 GHz), ovvero Finlandia, Germania e Grecia, seguite da Danimarca e Slovenia (aprile 2021).
Allo stesso modo sono ormai molti i Paesi ad aver assegnato circa 2/3 delle proprie risorse frequenziali nelle bande indicate, tra cui Cipro, Repubblica Ceca, Austria, Repubblica Slovacca, Lussemburgo e Ungheria. Tra queste figura anche l'Italia che, come noto, ha assegnato da tempo anche la banda a 700 MHz, sebbene con una titolarità prevista da luglio 2022 (data peraltro messa temporaneamente in discussione dal laborioso spostamento degli attuali occupanti[6]).

Tra gli altri grandi Paesi europei, la Francia ha assegnato più della metà delle frequenze individuate, mentre la Spagna appena un terzo. Rispetto a quelli di dimensioni minori, ancora in attesa di assegnazione risultano la Croazia, l'Estonia, la Lituania, Malta e la Polonia. Hanno invece completate le aste nel corso del 2021 la Bulgaria[7], la Danimarca[8], la Spagna[9], la Slovenia[10] e la Svezia[11]. In media, lo spettro individuato a

[6] L'attivazione del Dvbt-2 a livello nazionale sarà disposta a partire dal 1° gennaio 2023, invece che giugno 2022. Ciononostante, è stata confermata la cessione della banda 700 MHz agli operatori di rete, fissata per il 1° luglio 2022.
[7] L'asta per la banda 3.5 GHz è stata completata ad aprile 2021.
[8] L'asta multibanda (1500/2100/2300/3500 MHz and 26 GHz) si è conclusa ad aprile 2021.
[9] I due slot rimanenti nella banda a 3.5 GHz sono stati assegnati a febbraio 2021.
[10] L'asta multibanda su tutte e tre le frequenze individuate (700 MHz/3.5 GHz/26 GHz) si è conclusa ad aprile 2021.
[11] L'asta per le bande 2.3 GHz e 3.5 GHz, inizialmente prevista per marzo 2020, è stata posticipata due volte e si è tenuta a gennaio 2021.

Figura 2.25 Assegnazione bande per regione geografica (2021)

Fonte: 5G Observatory, giugno 2021



livello europeo appare dunque assegnato per il 45,8%.

Sulla scorta della normalizzazione effettuata dal *5G Observatory*, è possibile effettuare un confronto anche con lo stato delle assegnazioni degli altri principali Paesi a livello mondiale. Nel dettaglio, partendo dal presupposto che i Paesi extra-europei non hanno identificato specifiche bande pioniere per il 5G, i grafici mostrano la quantità di spettro individuato e assegnato nelle c.d. bande a basse frequenze, bande a medie frequenze e bande ad alte frequenze.
A livello fisico, una **frequenza bassa** (ovvero una emissione elettromagnetica con una frequenza <1GHz)[12] consente al segnale di arrivare più lontano di una frequenza alta, ma ha la controindicazione di trasportare una minore quantità dati per unità di tempo (calcolati in Mbps o Gbps)[13].

Al contrario una **frequenza alta** (nell'ordine dei GHz, in questo caso il parametro scelto è >6GHz) ha la capacità di trasportare molti dati per unità di tempo ma con un raggio ed un'intensità piuttosto ridotti. Infatti, mentre una frequenza di banda bassa ha una portata più ampia e riesce ad attraversare gli ostacoli fisici, una frequenza di

[12] Valore indicativo utilizzato dal 5G Observatory per la comparazione. Fonte: 5G Observatory, Quarterly report n. 12, giugno 2021.
[13] Fastweb, "*5G: quali differenze tra bande ad alta, media e bassa frequenza*", 17 luglio 2020.

banda alta è molto soggetta a disturbi e distorsioni, che vengono provocati, oltre che dagli ostacoli fisici (abitazioni, alberi) anche dagli agenti atmosferici (pioggia, nuvole). Per tale ragione, per massimizzare i vantaggi del 5G, sono necessari due elementi: l'implementazione di un buon numero di antenna in grado di garantire un'ottima copertura e l'indirizzamento dei device rispetto alle esigenze del servizio richiesto[14].

Per effettuare la comparazione, la classificazione utilizzata dal *5G Observatory* e riportata nella Fig. 2.25 distingue tra le frequenze <1GHz (banda a basse frequenze), tra GHz e 6 GHz (bande a medie frequenze) e sopra i 6 GHz (banda ad alte frequenze). Negli Stati Uniti la banda a bassa frequenza è quella a 600 MHz, le bande a media frequenze sono quelle tra 2,5GHz e 3,5GHz[15] e le bande ad alte frequenze sono quelle tra 24GHz e 48Ghz[16].

Per la Corea del Sud quelle in bassa frequenza sono le bande a 700 Mhz, a media frequenza da 3420-3700 MHz e ad alta frequenza 26500-28900 MHz. In Cina la banda in bassa frequenza è quella a 700 MHz; le bande a media frequenza sono tra 2600 e 5000 MHz[17] e quelle in alta frequenza sono la 24750-27500 e la 37000-42500 MHz.

In Giappone non è stata identificata alcuna banda sotto il Gigahertz, mentre a medie frequenze sono state identificate la 3600-4200 MHz e la 4400-4900 MHz e, tra le bande ad alta frequenza, è stata identificata la 27500-29500 MHz.

Dalla comparazione così composta emergono i risultati illustrati nella Fig. 2.25. Per le bande in bassa frequenza, **l'Europa appare seconda dietro gli Usa**, che hanno assegnato tutto lo spettro individuato, mentre il Vecchio continente ha assegnato circa la metà dei 6 GHz identificati. Tra le bande medie, Cina e Stati Uniti sono i Paesi che intendono dedicare più MHz al 5G (più di 1.300 MHz in Cina e più di 900 MHz negli Usa), sebbene sia il Giappone quello che presenta la porzione più larga di banda assegnata (600 MHz) rispetto a quella individuata (800 MHz). L'Europa presenta in media 200 Mhz assegnati su 400 MHz individuati (nella porzione 3.4-3.8 GHz).

Diverso il discorso per le frequenze in banda alta, dove Corea e Giappone hanno assegnato quasi tutte le porzioni individuate (rispettivamente 2000 MHz e 2300 MHz) mentre gli altri, pur avendone individuate molte di più, ne hanno assegnate ancora poche.

La Cina in particolare non ha ancora assegnato nessuno degli 8.000 Mhz in banda alta e poco meglio ha fatto l'Europa. Infatti, a giugno 2021 la banda a 26 GHz era stata assegnata solo in Italia[18], in Germania[19], in Danimarca[20], in Grecia[21] e in Slovenia[22].

Nel complesso, è evidente come il lockdown abbia determinato un rallentamento nei progressi sia a livello di infrastrutturazione (in particolare relativo al ritardo nella implementazione delle base station) sia a livello amministrativo, anche in

[14] Ad esempio, la banda a basse frequenze è molto più adatta a connessione a bassa intensità di dati come quelle per la smart home, mentre quella alta è decisamente più efficace per le applicazioni data consuming come lo streaming di contenuti audiovisivi.
[15] Nello specifico, le bande 2500 MHz, 3550-3700 (CBRS), 3700-4200 e 3450-3550 MHz.
[16] In particolare, le bande in alta frequenza individuate negli Usa sono: 24250-24450, 24750-25250, 25250-27250, 26500-29500, 31800-33000, 37600- 38600, 38600-40000, 42000-42500, 47200-48200 MHz.
[17] Nel dettaglio, 2600, 3300-3400, 3400-3600, 3600-4200; 4400-4500, 4800-5000 MHz.
[18] Assegnato ad ottobre 2018.
[19] Dal 2020 è disponibile su richiesta a livello locale.
[20] Assegnate ad aprile 2021.
[21] Assegnate a dicembre 2020.
[22] Due blocchi assegnati a gennaio 2018 ma non disponibili per il 5G e c'è stata un'ulteriore assegnazione ad aprile 2021.

termini di assegnazione dello spettro[23].

Tuttavia, la crisi potrebbe aver svolto il ruolo di acceleratore rispetto alla consapevolezza presso la popolazione della necessità di banda e dell'importanza dei servizi avanzati a distanza, in particolare relativi a telemedicina e telelavoro, e dunque il suo impatto potrebbe rivelarsi, nel medio-lungo periodo, positivo in termini di aumento della domanda, che potrebbe ripercuotersi sensibilmente anche sull'accelerazione delle operazioni di infrastrutturazione.

A livello di investimenti (Fig. 2.26), secondo le previsioni di GSMA, nelle reti di trasmissione verranno immessi complessivamente circa 900 miliardi di dollari a livello mondiale entro il 2025, di cui l'80% dedicati all'upgrade verso il nuovo standard 5G[24].

In particolare, GSMA stima quasi 300 miliardi di dollari di investimenti negli Usa, circa 200 miliardi in Asia (sponda Pacifico), oltre 170 miliardi in Europa e più di 200 miliardi di dollari in Cina.

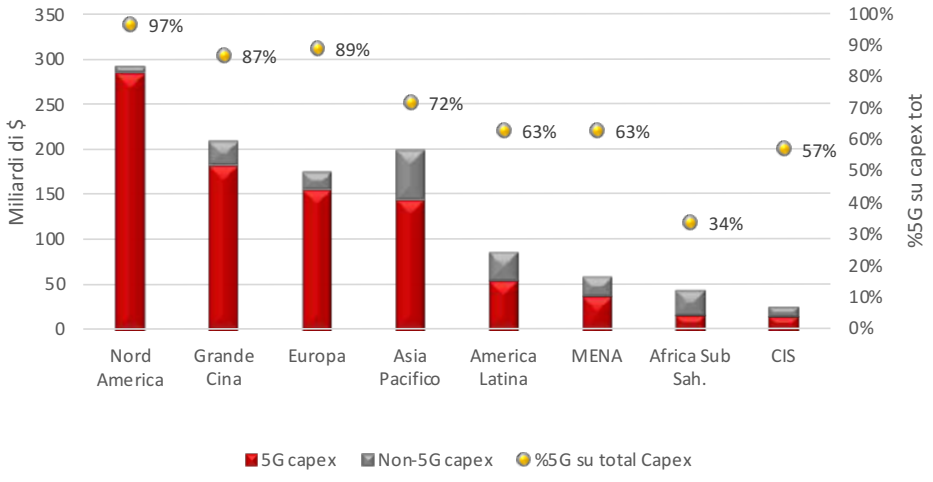
Queste ultime due aree, sono anche quelle in cui gli investimenti in reti 5G dovrebbero avere l'incidenza maggiore, oltre l'85%, rispetto agli investimenti complessivi nelle reti di telecomunicazione, insieme al Nord America, per il quale la quasi totalità degli investimenti avrà come destinazione il nuovo standard di trasmissione.

Più contenuti, seppur significativi, gli investimenti in America Latina (circa 80 miliardi di dollari) e MENA (Medio Oriente e Africa del Nord, circa 60 miliardi di dollari, mentre circa 45 miliardi verranno investiti nell'Africa Sub Sahariana e circa 25 miliardi di dollari nella Comunità degli Stati Indipendenti.

Infine, analizzando il numero di utenze stimate da GSMA al 2025 (Fig. 2.27), si osserva l'inesorabile crescita dei Paesi asiatici, che supereranno quota un miliardo di connessioni (di cui rispettivamente oltre 800 milioni in Cina e oltre 160 milioni nei Paesi asiatici sponda Pacifico), a fronte di circa 240 milioni di connessioni in Europa e circa 220 milioni negli Usa.

Figura 2.26 Investimenti globali in 5G da parte degli operatori rispetto alle altre reti (miliardi di $, 2021 - 2025)

Fonte: GSMA, Mobile Economy Report 2020

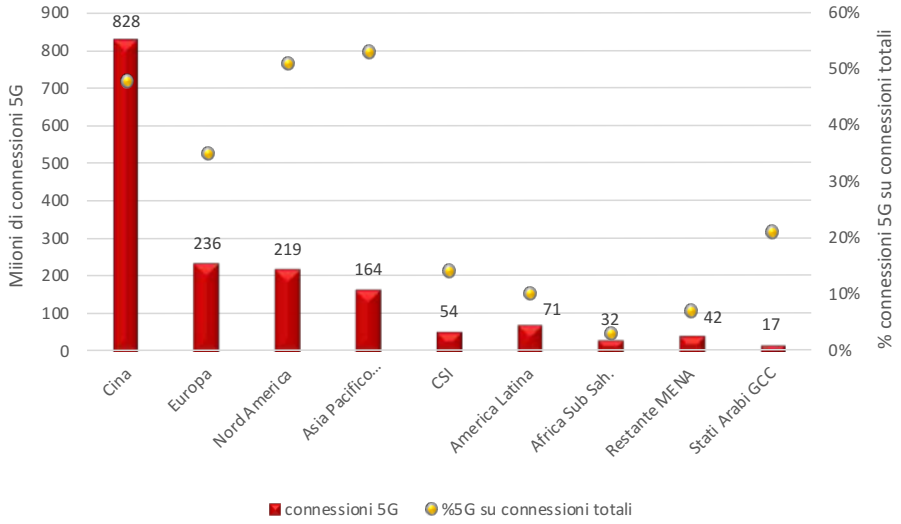


[23] In particolare, le aste per le frequenze in alcuni Paesi sono state rimandate, tra cui quella francese, che si è conclusa il 2 ottobre 2020, raggiungendo un totale complessivo di 2.786 milioni per 310 MHz nella banda pioniera 3.4-3.8 GHz.
[24] GSMA, Mobile Economy, giugno 2021.

Si osserva inoltre come **la percentuale di adozione del 5G sarebbe sensibilmente inferiore in Europa** (circa il 35% delle utenze telefoniche totali) rispetto agli Usa e alle tigri asiatiche (fino ad oltre il 50% delle utenze), a fronte di una media mondiale del 21%.

Figura 2.27 Connessioni 5G per area continentale (in milioni, stima al 2025)

Fonte: GSMA, Mobile Economy Report 2021, giugno 2021
*Il dato sulla Cina include anche Hong Kong, Macao e Taiwan



CAPITOLO 3

IL RUOLO E L'UTILIZZO DEI SERVIZI DIGITALI NELL'UNIONE EUROPEA

3.1 LA PENETRAZIONE DI INTERNET NEL CONTESTO GLOBALE ED EUROPEO

Il 2020 si è caratterizzato per essere un anno all'insegna dell'accelerazione digitale. Le forti limitazioni che la pandemia ci ha imposto nell'ottica di ridurre i contagi limitando le occasioni di contatto sociale hanno determinato il graduale trasferimento in rete di moltissime attività e l'esercizio di diritti di primaria importanza come quello al lavoro e all'istruzione, dimostrando come il canale online rappresenti un alleato indispensabile per assicurare la continuità delle relazioni sociali e delle attività economiche.

Si tratta di una tendenza all'**accelerazione del processo di digitalizzazione** che, sebbene sia stata originata dalla necessità, ineludibile, di gestire un evento straordinario come la pandemia da Covid-19, ha di fatto rappresentato l'occasione per ripensare, ad esempio, le tradizionali modalità organizzative del lavoro favorendo, in particolare, l'affermazione dello smart working come nuova opportunità - peraltro anche molto importante in termini di sostenibilità ambientale e conciliabilità vita-lavoro - per lavoratori e imprese.

Sebbene si tratti di tendenze che hanno riguardato tutte le aree del mondo, **permangono ancora diversi gradi di maturità e sensibilità sia con riguardo allo sviluppo delle infrastrutture e tecnologie abilitanti i servizi digitali** (come emerso dall'analisi condotta nel cap. 2), sia con riferimento alla fruizione di tali servizi da parte di cittadini/consumatori, imprese e PA.

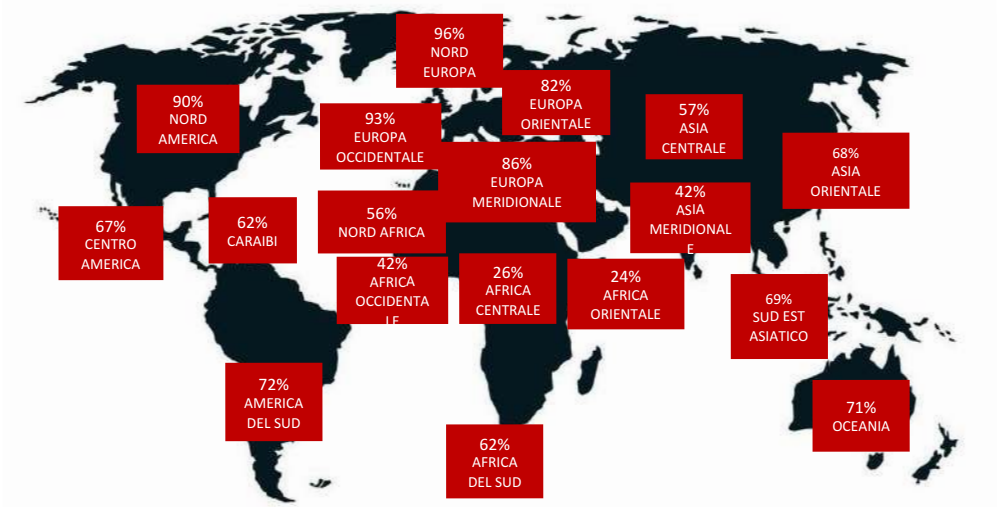
Scopo di tale paragrafo e di quelli che seguiranno sarà, dunque, analizzare sinteticamente i trend di utilizzo di alcuni dei principali servizi digitali da parte di cittadini, imprese e PA al fine di fare il punto sullo stato dell'arte e le prospettive future.

A tale riguardo l'annuale report "*Digital in 2021*", pubblicato da WeAreSocial, offre molte indicazioni e spunti di riflessione. A livello globale, su un totale di quasi 8 miliardi di individui (7,83 miliardi per l'esattezza), gli utenti di Internet, a gennaio 2021, ammontavano a **4,66 miliardi, pari al 59,5% della popolazione mondiale**, con un incremento rispetto all'anno precedente del 7,3% (pari a 316 mln).

Dal punto di vista territoriale (Fig. 3.1), se Europa e Nord America primeggiano con percentuali di utenti di Internet sul totale della popolazione che arrivano al 96% nell'Europa del Nord, esistono

Figura 3.1 Penetrazione di Internet per regione (gennaio 2021)

Fonte: We Are Social, "*Digital in 2021*"

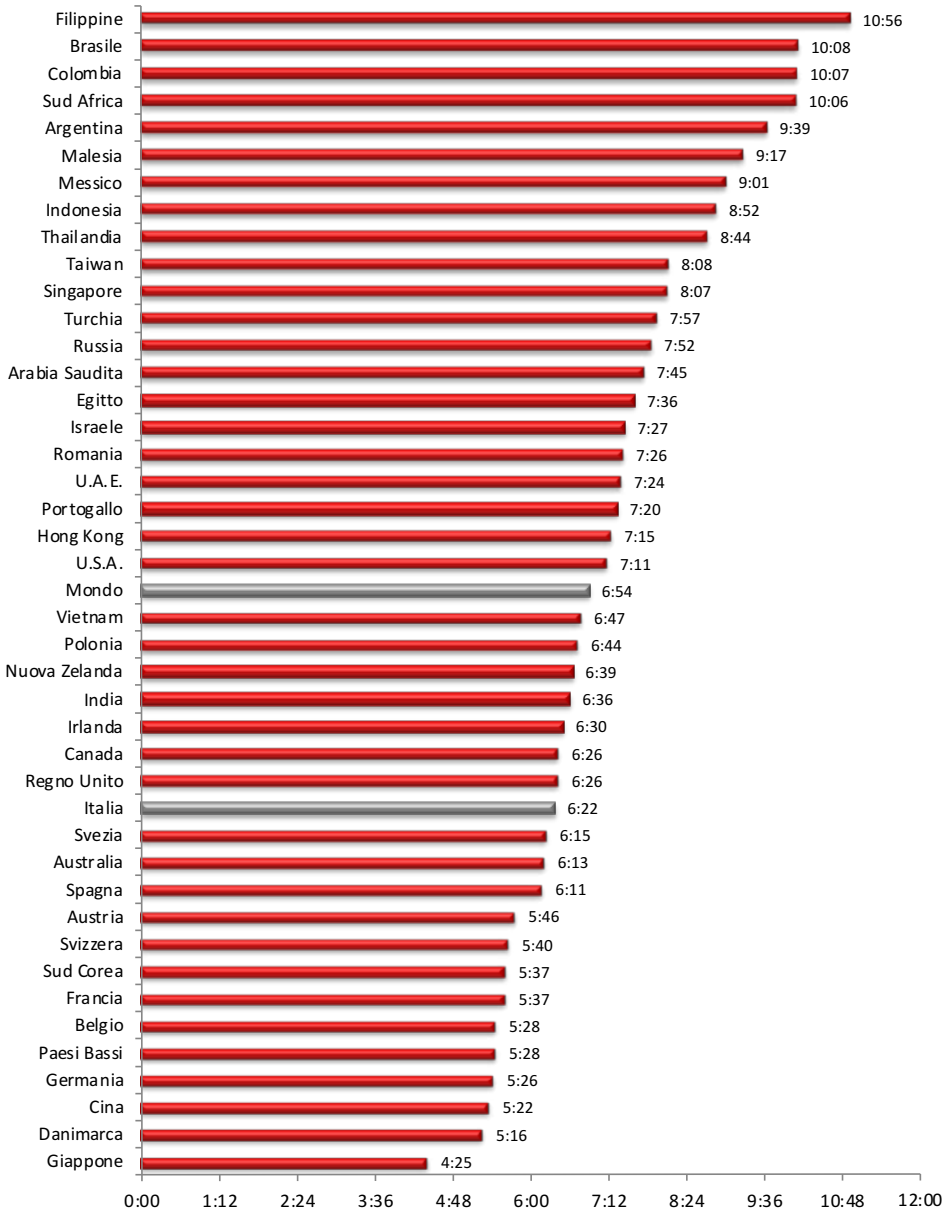


ancora aree del mondo – l'Africa, in particolare – in cui la percentuale di penetrazione si attesta su valori decisamente troppo bassi (addirittura non oltre il 26% nelle nazioni centrali africane) per riuscire ad assicurare alle popolazioni la necessaria inclusione e ai governi di accedere ed assicurare ai propri cittadini i benefici connessi alla digitalizzazione.

Quanto al tempo trascorso su Internet quotidianamente, se a livello mondiale si attesta sulle 6 ore e 54 minuti, il primato spetta alle Filippine con 10 ore e 56 minuti (in aumento rispetto alle 9 ore e 45 minuti di gennaio 2020). A chiudere la classifica, invece, secondo una tendenza consolidata e stabile rispetto al 2020, il Giappone con 4 ore e 25 minuti. Nella classifica mondiale l'**Italia figura quinta tra i Paesi europei**, dopo Romania, Portogallo, Irlanda e Regno Unito, con 6 ore e 22 minuti (Fig. 3.2).

Figura 3.2 Tempo trascorso su Internet quotidianamente (numero medio di ore, gennaio 2021)

Fonte: We Are Social



Nonostante le tendenze globali dimostrino una sempre crescente penetrazione di Internet nelle abitudini degli individui, non mancano le preoccupazioni circa le possibili criticità connesse all'utilizzo online dei dati personali e al fenomeno della disinformazione che trova nella rete uno strumento straordinariamente efficace di diffusione.

A tale riguardo, la Fig. 3.3 rivela una certa varietà di percezione a livello globale rispetto alle potenziali criticità connesse al **tema privacy**, frutto, presumibilmente, della coesistenza, seppur con intensità differente a seconda dei contesti nazionali, di un diverso grado di consapevolezza degli utenti, di fiducia degli stessi negli strumenti digitali e di percezione circa l'efficacia delle regole a tutela dei dati personali e del relativo *enforcement*. Gli utenti europei, mostrano, a livello generale, una più marcata preoccupazione che deriva, certamente, dalle numerose iniziative messe in campo dalle istituzioni europee e nazionali a presidio della privacy e, dunque, dell'elevata maturità del dibattito nel contesto UE.

Figura 3.3 Preoccupazioni degli utenti di Internet relative all'utilizzo online di dati personali da parte delle imprese (% rispondenti, 2021)

Fonte: We Are Social

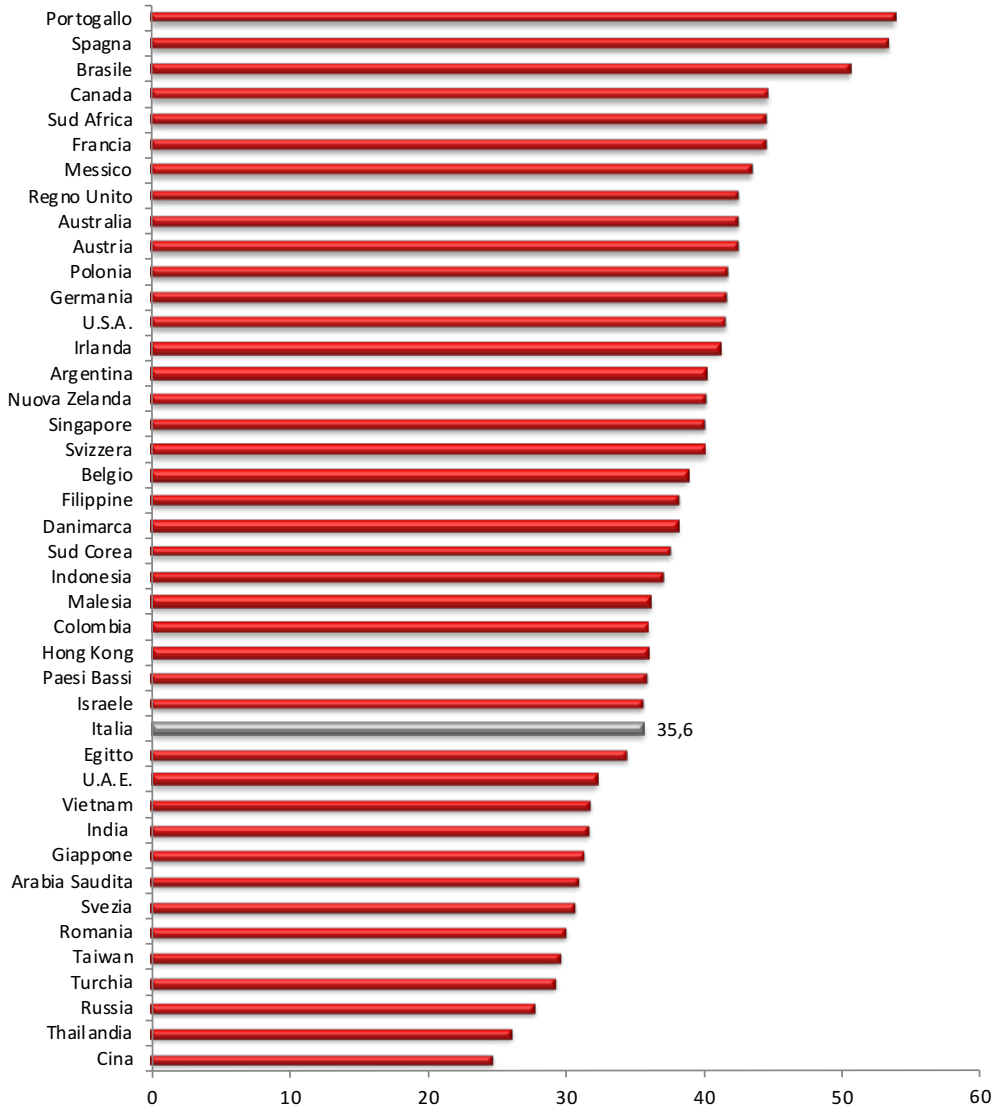
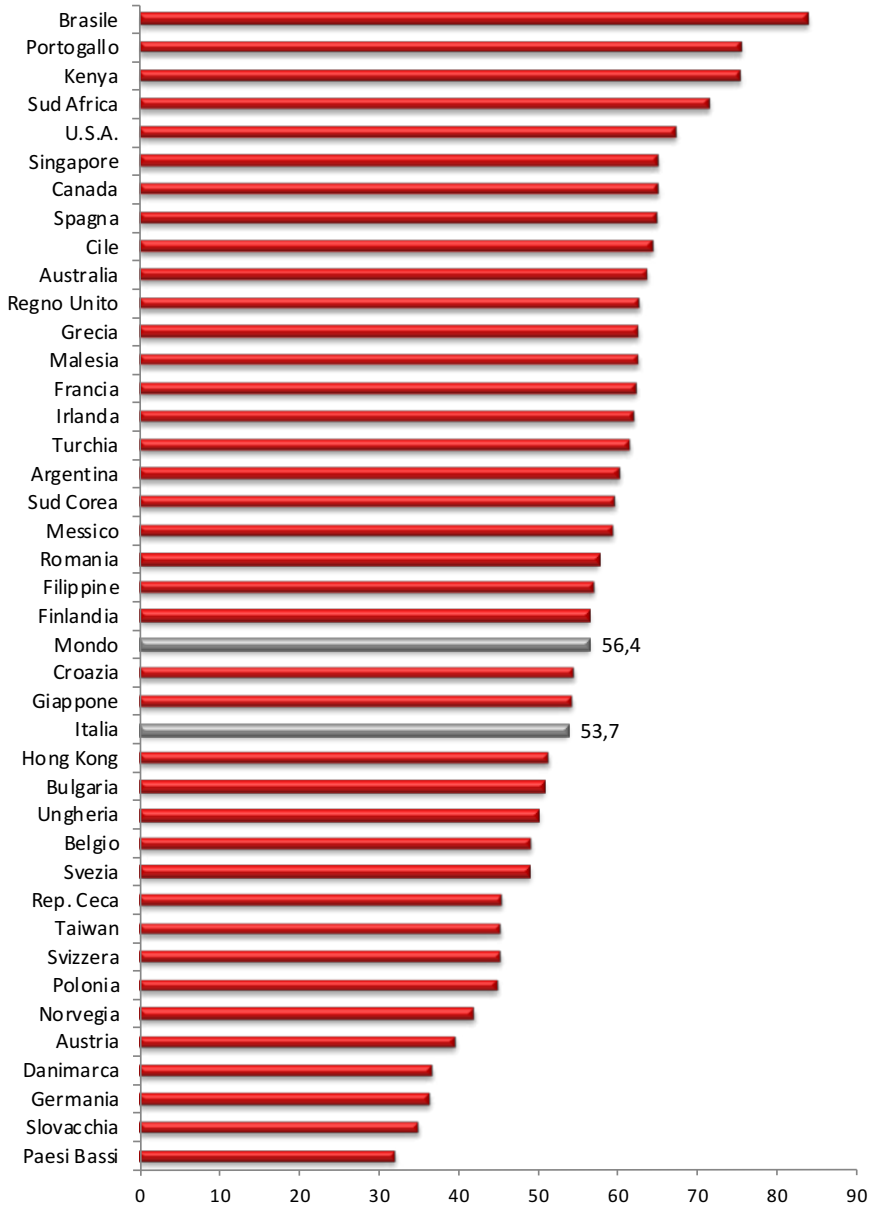


Figura 3.4 Preoccupazioni degli utenti di Internet legate alla veridicità delle notizie online (% rispondenti, 2021)

Fonte: We Are Social



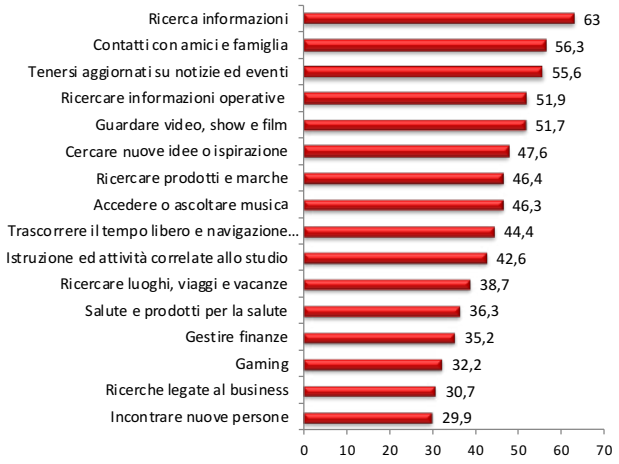
Se la percentuale massima di utenti preoccupati per gli utilizzi dei dati personali compiuti online è del 53,9% in Portogallo, ancora più forte risulta il timore legato alla disinformazione e alle fake news, che in Brasile e in Portogallo è stato espresso rispettivamente da ben l'84 ed il 75,7% degli utenti di Internet (Fig. 3.4). Per quanto concerne l'Italia, i dati appaiono leggermente al di sotto della media.

Si tratta di numeri importanti che vanno letti in combinato con quelli relativi ai motivi che spingono a utilizzare Internet.

Al riguardo, i dati We Are Social collocano in vetta alla classifica dei moventi per l'utilizzo di Internet la **ricerca di informazioni** (per il 63% degli utenti globali di internet), seguita dal **desiderio di stare in contatto con amici e parenti** (56,3%) (Fig. 3.5).

Figura 3.5 Principali motivi per usare Internet (utenti globali 16-64) (%, 2021)

Fonte: We Are Social



Se a livello globale, in termini di penetrazione di Internet, l'Europa guida la classifica, in considerazione degli ambiziosi obiettivi fissati dall'UE in tema di digitalizzazione, dopo aver descritto, nel capitolo precedente, le dinamiche dell'offerta relativamente alle reti fisse e mobili, è interessante ora verificare lo stato di avanzamento del processo di digitalizzazione dei paesi UE rispetto ad alcuni tra i principali servizi digitali, iniziando dall'analisi della variabile principale, ossia l'utilizzo di internet (Fig. 3.6).

Innanzitutto è incoraggiante rilevare come nei Paesi meno avanzati digitalmente dal lato della **domanda** (molti dei quali, invece, come già evidenziato nel capitolo precedente, presentano buoni o addirittura ottimi livelli di sviluppo infrastrutturale), la percentuale di non utilizzo di Internet continui positivamente a ridursi, attestandosi nel 2020 al 21% in Bulgaria e al 20 e 18% in Grecia e Portogallo a fronte del 24 e 22% del 2019. A primeggiare, come d'altronde ormai rileviamo da anni, il **Nord Europa** dove le percentuali sono dell'1-2%.

Alle medesime conclusioni si giunge con riguardo all'utilizzo quotidiano di Internet che vede ancora una volta affermare il primato del Nord Europa con Danimarca, Svezia, Finlandia e Lussemburgo, dove nel 2020 ben il 94 e 92% degli individui ha utilizzato Internet ogni giorno. L'Italia registra un dato leggermente al di sotto della media (76% vs 80%) che, sebbene denoti un timido avanzamento di 3 p.p. rispetto al 2019, la colloca ancora una volta nella parte medio bassa della classifica europea. Le performance peggiori riguardano invece Portogallo, Grecia, Bulgaria e Romania con percentuali che si fermano rispettivamente al 70%, 69% e 62% (Fig. 3.7).

Andando ad analizzare l'utilizzo quotidiano di Internet per fascia d'età (Fig. 3.8), nel 2020, anno

Figura 3.6 Individui che non hanno mai utilizzato Internet (%, 2020)

Fonte: Eurostat
* dato 2019

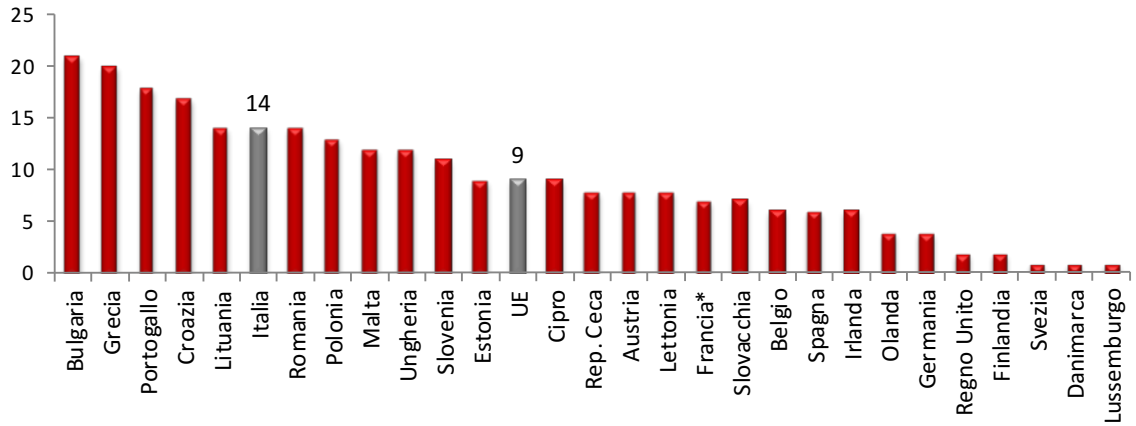


Figura 3.7 Individui che utilizzano Internet ogni giorno (%, 2020)

Fonte: Eurostat

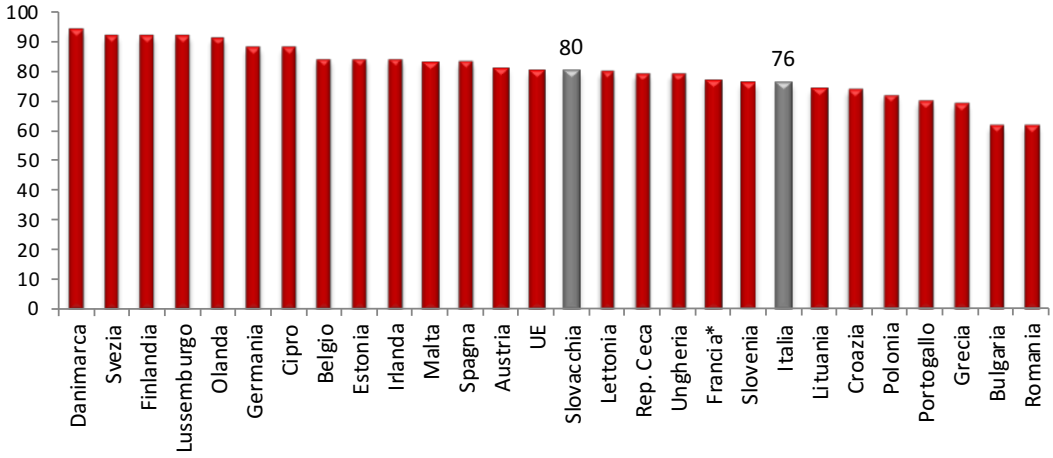
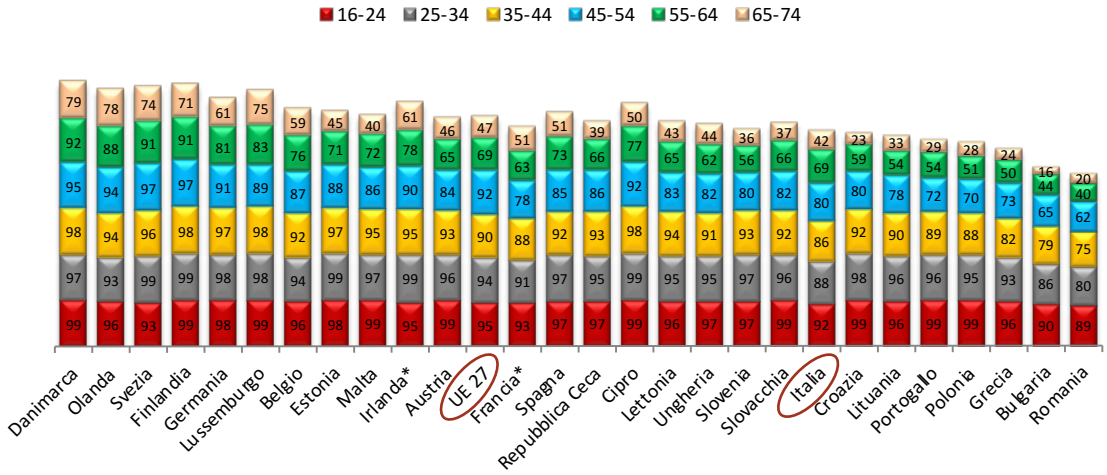


Figura 3.8 Utilizzo quotidiano di Internet per fascia d'età (%, 2020)

Fonte: Eurostat
* dato 2019



in cui i servizi digitali sono diventati una necessità per esercitare i propri diritti e coltivare relazioni e interessi socio-economici, si segnala una maggior convergenza verso un elevato utilizzo.

Se tradizionalmente si sono registrate rilevanti differenze di utilizzo con una conclamata prevalenza delle fasce d'età più giovani (soprattutto 16-24 e 25-34), nel 2020 si rilevano a livello UE percentuali di utilizzo di Internet molto importanti anche nelle fasce d'età più avanzate (69% nella fascia 55-64 e 47% in quella 65-74).

Con riguardo all'Italia, la percentuale è perfettamente in linea con quella europea nella fascia d'età 55-64 (69% come il dato europeo), mentre si rilevano lievi discostamenti nelle fasce d'età 16-24 (92% vs 95%), 25-34 (88% vs 94%), 35-44 (86% vs 90%) e 65-74 (42% vs 47%). Si attesta invece a 12 p.p. la distanza tra il dato italiano e quello europeo nella fascia 45-54 (80% vs 92%).

Se appare tutto sommato contenuto il ritardo rispetto alla media UE, molto ampio risulta invece il gap con i Paesi digitalmente più avanzati in cui

le percentuali di utilizzo di Internet sono superiori al 90% e vicine al 100% in tutte le fasce d'età esclusa quella 65-74 dove comunque il dato non scende al di sotto del 70%.
Non si rilevano, invece, significative differenze di genere nell'utilizzo quotidiano di Internet (Fig. 3.9).

Rispetto alle attività compiute, nel 2020 i dati UE mostrano che il 70% degli individui ha usato Internet per cercare informazioni su beni e servizi, il 62,2% per fare chiamate o videochiamate, il 57,7% per utilizzare l'*online banking*, il 57,3% per partecipare ai social network, il 35,3% per salvare documenti, foto, video ed altri file e il 13,2% per seguire un corso online.

Se queste sono le tendenze degli individui, **per il mondo delle imprese è stato fortissimo l'impatto della pandemia** sia sugli aspetti meramente organizzativi, sia sul modello di business. Le aziende sono state chiamate, in tempi rapidi e nel pieno di un'emergenza sanitaria gravissima, a prevedere lo smart working come l'unica o comunque la prevalente modalità di organizzazione del lavoro e a mettere in atto strategie e investimenti finalizzati a proporre i propri beni e/o servizi in rete, l'unico "*luogo*" di interazione, scambio e acquisto al fine di arginare le perdite, da un lato, e captare nuove occasioni di business, dall'altro.

In un contesto a così elevata complessità, sebbene sia forte l'accelerazione verso la digitalizzazione, le dinamiche delle aziende mostrano trend diversificati. Le Figg. 3.10 e 3.11 in particolare riportano la percentuale di imprese europee (con almeno 10 persone impiegate e non esclusione del settore finanziario) con elevato e basso livello di intensità digitale, facendo riferimento, con tale espressione, alla sussistenza di specifici requisiti tecnologici e di connettività (tra cui connessione fissa superiore a 30 Mbps, adozione di sistemi ERP, CRM etc.).

Ebbene, rispetto alle imprese con elevato livello di intensità digitale, i dati evidenziano una **flessione rispetto al 2019 anche nel Nord Europa**. Si tratta, infatti, di una tendenza generalizzata seppur con intensità variabile di Paese in Paese, che probabilmente si spiega con la crisi economica che è conseguita allo scoppio della pandemia e che ha determinato una contrazione anche degli investimenti nella digitalizzazione e il

Figura 3.9 Uomini e donne che utilizzano Internet ogni giorno (%, 2020)

Fonte: Eurostat
* dato 2019

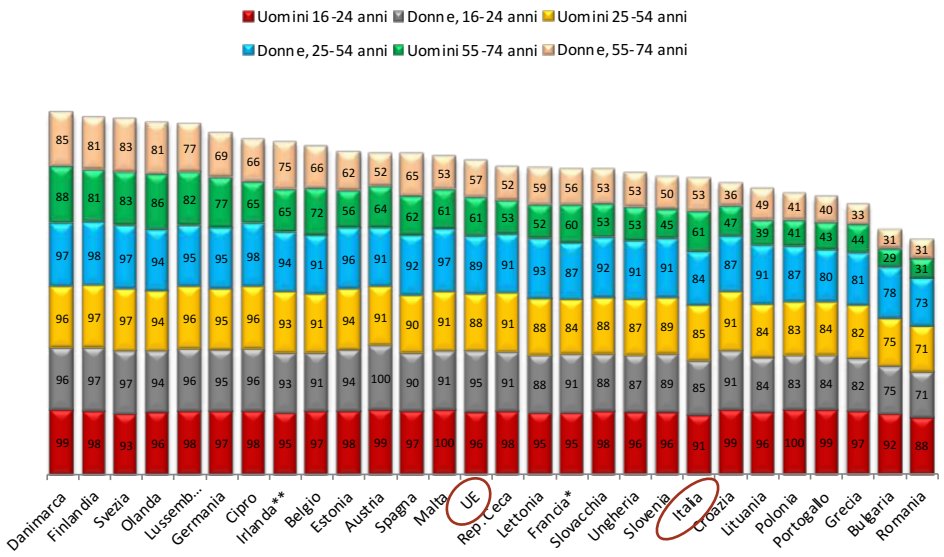


Figura 3.10 Imprese con un elevato grado di intensità digitale (%)

Fonte: Digital Agenda Scoreboard

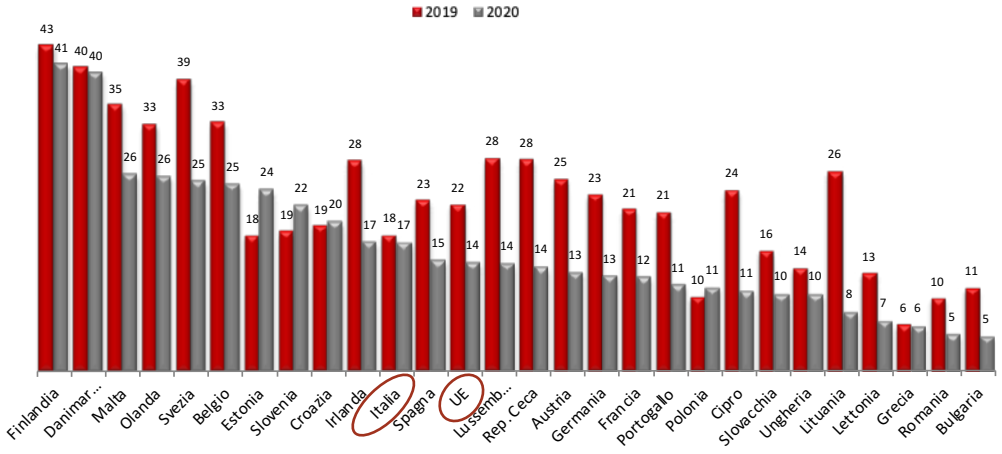
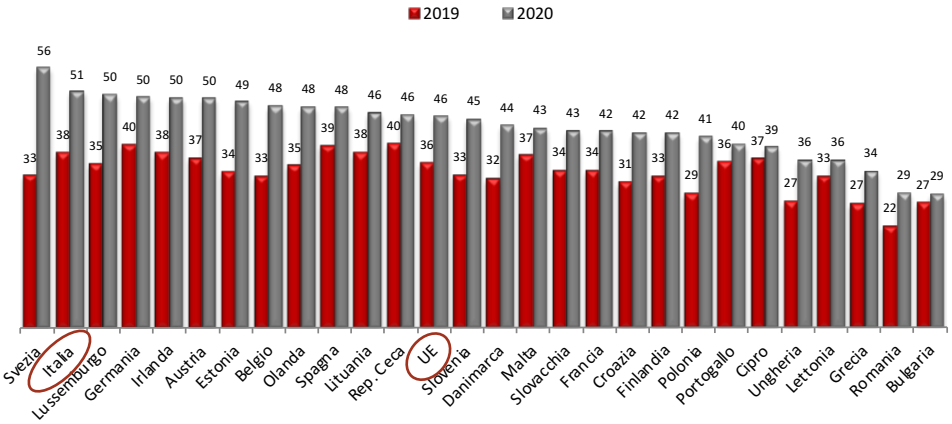


Figura 3.11 Imprese con un basso grado di intensità digitale (%)

Fonte: Digital Agenda Scoreboard



ripiegamento, forse, verso livelli di sofisticazione digitale inferiore. Tale conclusione sembra trovare conferma nelle evidenze relative alla percentuale di imprese con un basso grado di intensità digitale che, al contrario, hanno subito un forte incremento nel 2020. L'**Italia si posiziona al secondo posto in Europa**, dopo la Svezia, con una percentuale di imprese a bassa intensità del 51%, con un incremento di ben 13 p.p. rispetto al 2019.

Nel dettaglio, il 73% delle imprese italiane (con almeno 10 persone impiegate e con esclusione del settore finanziario) possiede un sito web, mentre il 57%, con un mirabile +21 p.p. rispetto al 2019, ne possiede uno con funzionalità avanzate (ad es. per personalizzare il design di un prodotto) (Fig. 3.12). Si tratta di numeri importanti, soprattutto il secondo, che recupera gran parte del gap rispetto alla media europea riducendolo a solo 4 p.p. a fronte dei 21 del 2019.

Molto positiva la performance delle imprese italiane rispetto all'acquisto di **servizi cloud**. Con una percentuale di imprese pari al 57%, infatti, il nostro Paese si posiziona quarto, dopo Finlandia, Svezia e Danimarca e ben 23 p.p. al di sopra della

Figura 3.12 Imprese con sito web (%, 2020)

Fonte: Digital Agenda Scoreboard

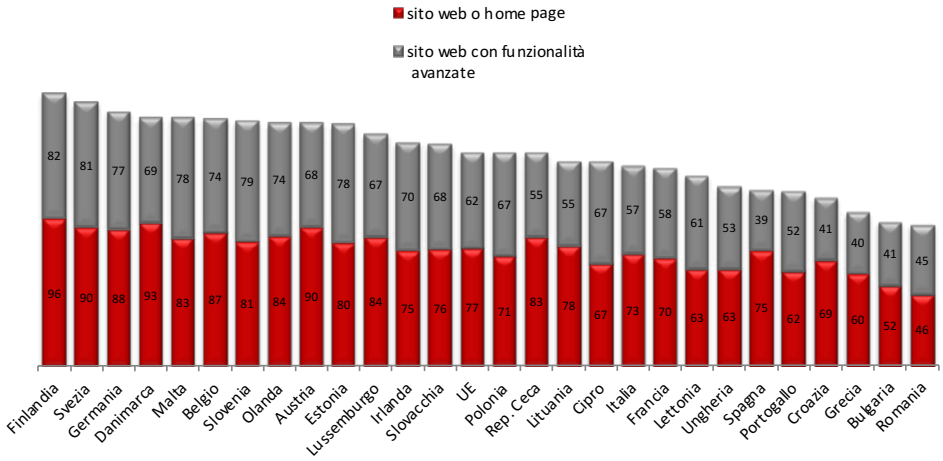
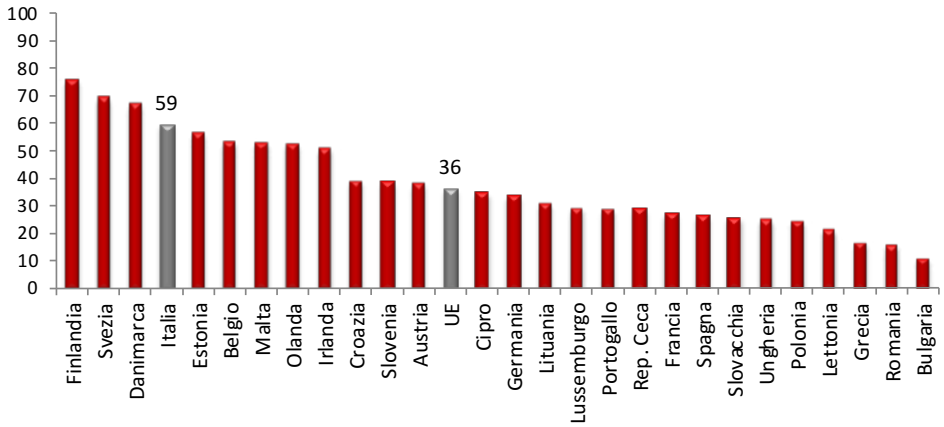


Figura 3.13 Imprese che acquistano servizi cloud (%, 2020)

Fonte: Digital Agenda Scoreboard



media europea (Fig. 3.13).

3.2 LE TENDENZE ED IL RUOLO DEI SOCIAL MEDIA

Uno degli ambiti che certamente ha trovato maggior espansione nel 2020, complice ancora una volta l'accelerazione impressa alla digitalizzazione dal distanziamento sociale imposto dalla pandemia, è quello dei **social media**. Questi ultimi hanno rappresentato uno strumento straordinariamente efficace per condividere pensieri ed esperienze, creare nuovi rapporti, pubblicizzare attività d'impresa, monitorare le strategie commerciali altrui, intercettare preferenze e gusti di potenziali nuovi clienti e offrire un'assistenza efficace ai clienti già acquisiti, praticamente senza alcuna limitazione spazio-temporale.

Anche rispetto al fenomeno social media, il report stilato da We Are Social offre importanti spunti di analisi. La ricerca, in particolare, quantifica in **4,2 miliardi gli utenti social media nel mondo**, con una penetrazione del 53,6% sulla popolazione totale e un incremento annuale del 13,2%.

Considerato che tali numeri guardano alla popolazione e che la maggioranza degli Stati vieta l'utilizzo delle piattaforme agli under 13, è evidente l'assoluta rilevanza del fenomeno.

Quanto al **tempo medio trascorso quotidianamente sui social media** (Fig. 3.14), il report lo quantifica in 2 ore e 25 minuti. Il primato spetta alle Filippine, secondo una tendenza consolidata nel tempo, con 4 ore e 15 minuti. L'Italia, con 1 ora e 52 minuti, si pone al di sotto della media mondiale, ma sostanzialmente in linea con le tendenze in atto negli altri Paesi analizzati dalla ricerca.

Dal punto di vista territoriale, l'Europa occidentale e settentrionale rappresentano le aree a più alta penetrazione, con il 79% di utenti social media sul totale della popolazione. Segue il Nord America con il 74%. L'Africa, al contrario, è il continente decisamente più indietro, con una percentuale di penetrazione che si attesta all'8 e al 10% rispettivamente nelle regioni centrali e dell'Est.

Per quanto attiene le motivazioni che spingono all'utilizzo dei social media (Fig. 3.15), è interessante notare come la ragione primaria non sia più il contatto con amici e parenti, bensì l'**accesso alle notizie**, con tutto quello che ne

Figura 3.14 Tempo trascorso sui social media quotidianamente (numero medio di ore, gennaio 2021)

Fonte: We Are Social

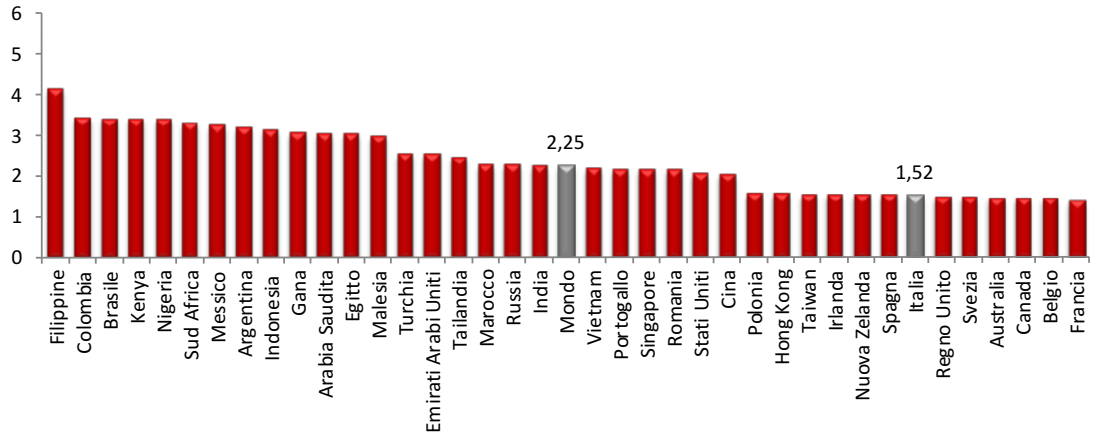


Figura 3.15 Ragioni per l'utilizzo dei social media (%, gennaio 2021)

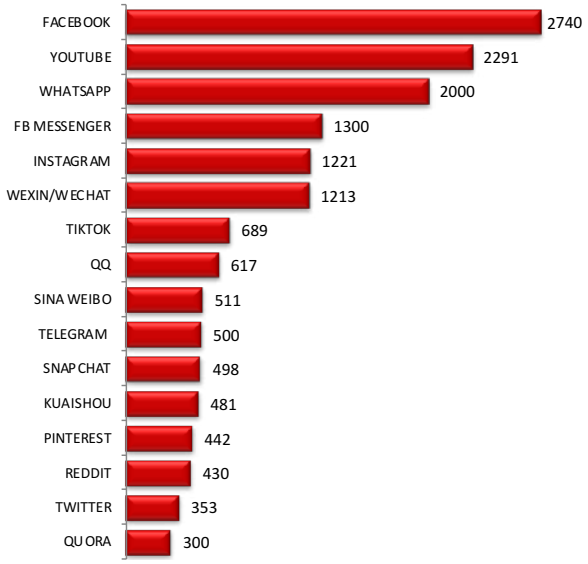
Fonte: We Are Social

consegue in termini di rischi di disinformazione e fake news.

Andando a verificare il peso dei diversi social in termini di utenti attivi mensili, a livello globale continua a primeggiare secondo una tendenza consolidata Facebook, con oltre 2,7 miliardi, seguito da Youtube e Whatsapp con rispettivamente 2,29 e 2 miliardi di utenti (Fig. 3.16).

Figura 3.16 Utenti attivi sulle principali piattaforme social mondiali (milioni, gennaio 2021)

Fonte: We Are Social



Focalizzando ora l'attenzione sul contesto europeo, nel 2020 il 57% degli individui è stato attivo sui social network, una percentuale che sale all'85% in Danimarca, Paese *best performer*. Al contrario, gli individui meno attivi sui social sono stati ancora una volta, in linea con i dati 2019, gli italiani, insieme ai francesi (per i quali il dato 2020 non è disponibile), con una percentuale che si ferma al 48%, a ben 37 p.p. di distanza dal Paese capolista ma anche 9 p.p. dalla media europea (Fig. 3.17).

Quanto alla propensione all'utilizzo dei social da parte degli individui delle diverse fasce d'età, il dato che vale la pena evidenziare è che **cresce, a livello generale, la percentuale di utilizzatori nelle fasce mature**, che raggiunge livelli importanti anche nella fascia 45-54 per poi iniziare a diminuire nelle classi più anziane, tradizionalmente meno attratte dai social (Fig. 3.18).

Quanto alle preferenze degli utenti social italiani, il contesto del nostro Paese esprime una tendenza diversa da quella globale: se a livello mondiale a primeggiare è Facebook, in Italia quest'ultima piattaforma si posizionava al terzo posto a gennaio 2020, dopo YouTube e Whatsapp, con una distanza di 5 p.p. (Fig. 3.19).

Figura 3.17 Individui che utilizzano i social network (%, 2020)

Fonte: Eurostat

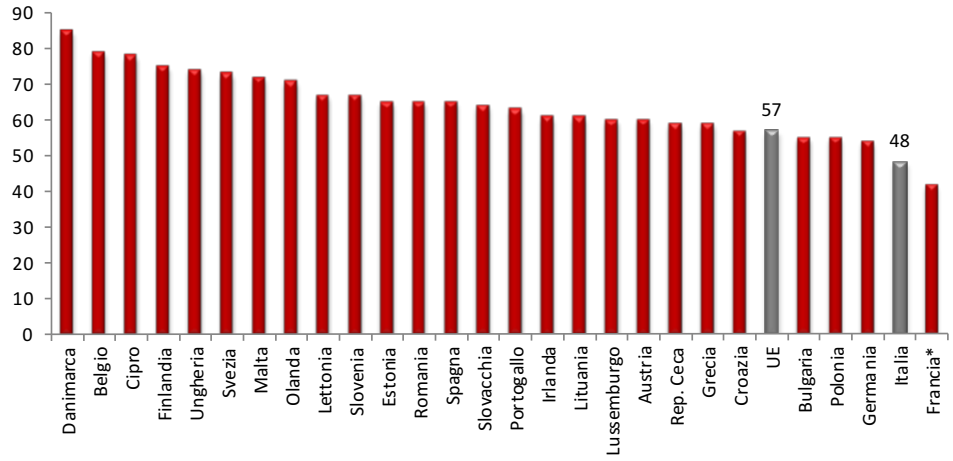


Figura 3.18 Individui che utilizzano i social network per fascia d'età (%, 2020)

Fonte: Eurostat
*dati 2019
**dato 2019 per la fascia d'età 16-24

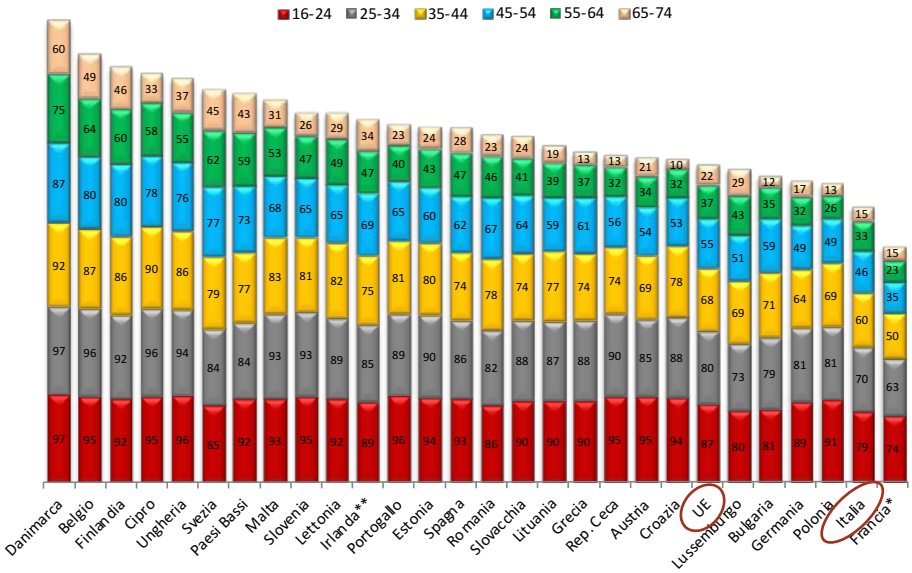
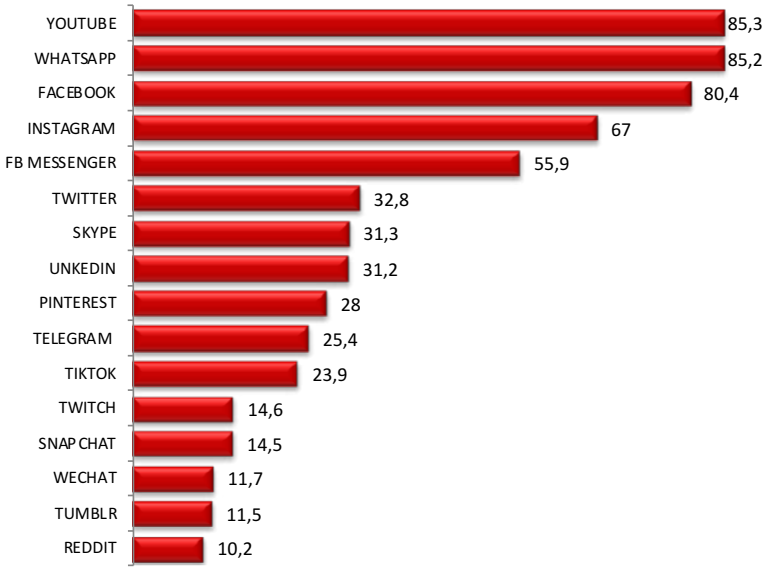


Figura 3.19 Piattaforme social maggiormente attive in Italia (% utenti nel mese precedente l'indagine, gennaio 2021)

Fonte: We Are Social



3.3 LO STATO DELL'E-COMMERCE. LE TENDENZE E LE PROSPETTIVE DI SVILUPPO

Le fortissime limitazioni imposte a cittadini e imprese nel corso del 2020 hanno favorito la massiccia affermazione dell'***e-commerce***.

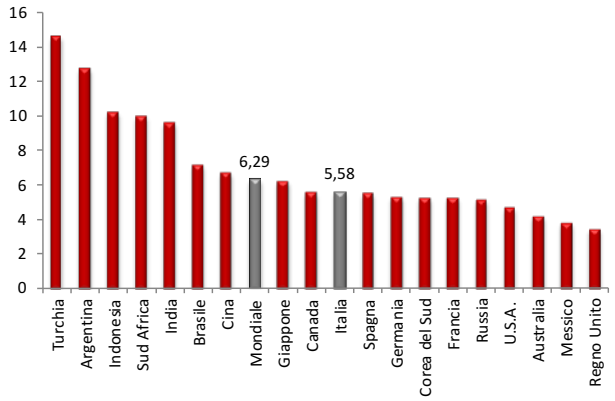
Secondo i dati eMarketer 2021, l'*e-commerce* B2C vale a livello globale 4.280 miliardi di dollari, con una **crescita del 27,6%** rispetto all'anno precedente e una stima che quantifica in 4.891 miliardi la soglia raggiunta dal fatturato nel corso del 2021 (con una percentuale di crescita del

14,3%). In termini di peso percentuale sul totale delle vendite retail, il fatturato *e-commerce* B2C 2020 rappresenta il 18% del totale, in crescita rispetto al 13,6% del 2019.

Dal punto di vista geografico, lo studio Casaleggio Associati "*Lo stato dell'e-commerce*" evidenzia come la regione Asia-Pacifico continui a dominare, rappresentando il 63% del totale, con un fatturato di 2.448 (in aumento rispetto ai 2.271 miliardi di dollari dell'anno precedente), con la Cina che da sola genera 2.090 miliardi di dollari pari al 48% del mercato. È generalizzata, tuttavia, e in media pari al 27%, la crescita delle vendite al dettaglio nell'*e-commerce*. In un contesto di sviluppo generale, spiccano tuttavia alcuni Paesi come l'Argentina e Singapore, dove la crescita delle vendite al dettaglio è cresciuta addirittura del 79 e 71,1%. Si segnalano anche l'America Latina, dove l'aumento è pari al 36,7%, e il Nord America, che ha visto una crescita del 32%. Segue l'Europa centrale e dell'Est con un +29%, Asia-Pacifico e Europa occidentale con un +26%, Medio Oriente e Africa con un +20%.

Figura 3.20 Previsioni di crescita (CAGR, 2021-2025)

Fonte: Statista

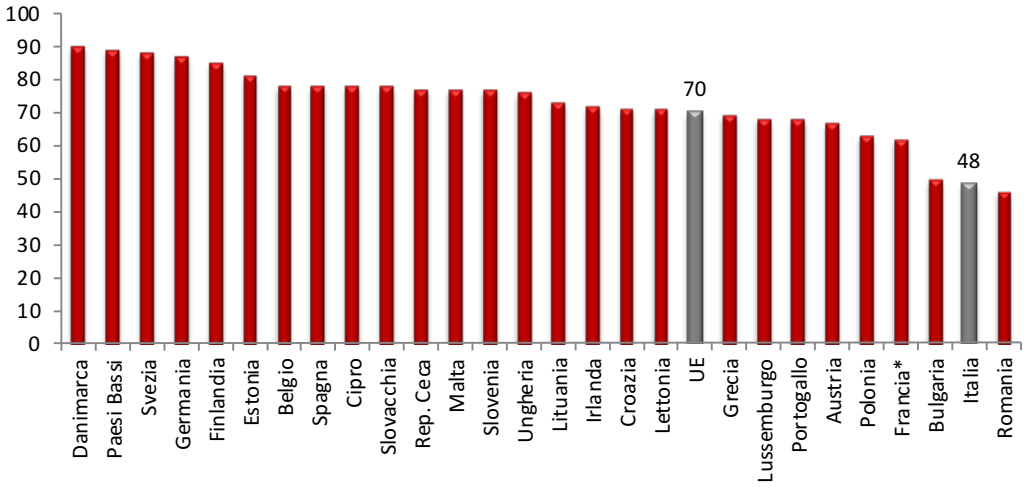


Guardando al futuro, le previsioni di crescita nel periodo 2021-2025 (Fig. 3.20) se stimano un CAGR a livello mondiale del 6,26%, attribuiscono un aumento record alla Turchia, con un 3 previsto del 14,59%, seguita da Argentina ed Indonesia con, rispettivamente, 12,76% e 10,21%. Per quanto attiene all'Italia, invece, il CAGR previsto è del 5,58%.

Passando ora all'analisi del contesto europeo, è interessante innanzitutto commentare i dati relativi all'utilizzo del canale online per la **ricerca di informazioni su beni o servizi**. A primeggiare, anche in questo ambito, sono i Paesi nordici - Danimarca (90%), Paesi Bassi (89%) e Svezia (88%)

Figura 3.21 Individui che ricercano informazioni su beni o servizi su internet (%, 2020)

Fonte: Eurostat
* dato 2019



- mentre l'Italia, nonostante un incremento di 8 p.p. rispetto al 2019, si posiziona penultima, perdendo anche un'ulteriore posizione nella classifica europea con solo il 48% degli individui che nel 2020 hanno cercato informazioni su beni o servizi su Internet, a dimostrazione di quanto sia grave il ritardo e di quanto rapida sia l'evoluzione degli altri Paesi (Fig. 3.21).

Negativa, come le premesse appena descritte lasciavano prevedibilmente pensare, la performance italiana con riguardo alla percentuale di individui che hanno acquistato online nel 2020. A fronte di una media europea del 65%, il dato italiano si attesta su un modesto 44%, che vale al nostro Paese la terzultima posizione in classifica, a una distanza abissale dalla Danimarca, in cima al ranking europeo (89%) (Fig. 3.22).
Si tratta di un divario che, sebbene in riduzione (peraltro molto lenta), permane purtroppo da molti anni (Fig. 3.23).

La crescita in atto rende quantomai interessante verificare l'**impatto dell'*e-commerce* sul fatturato delle imprese europee piccole, medie e grandi**.

La Fig. 3.24, in particolare, scatta una fotografia

Figura 3.22 Individui che acquistano beni o servizi su Internet (%, 2020)

Fonte: Eurostat

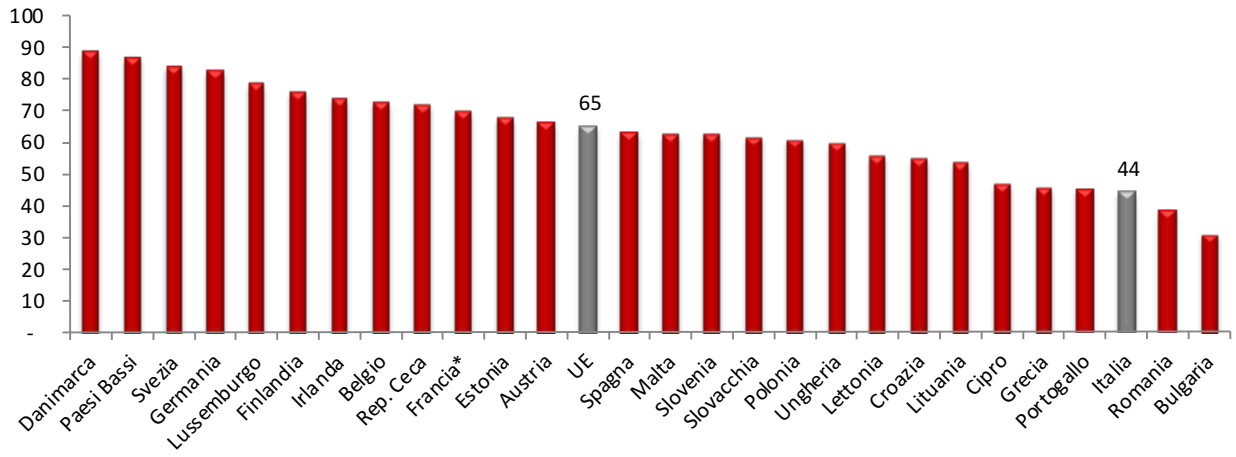


Figura 3.23 L'andamento dell'e-commerce. Italia vs Europa (% individui che acquistano online)

Fonte: Eurostat

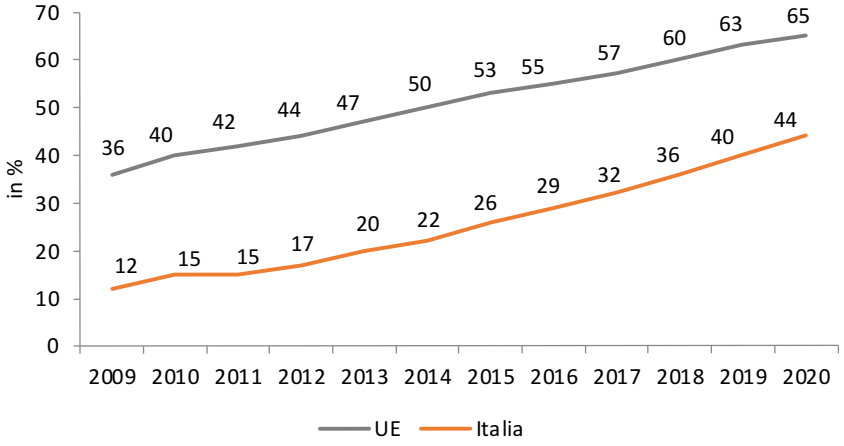
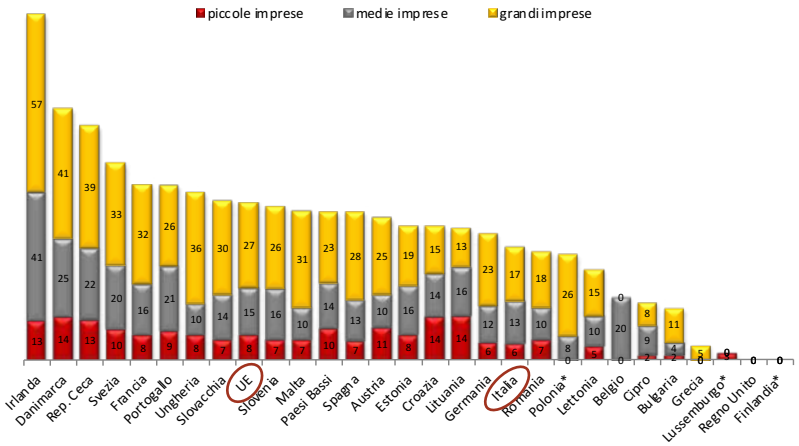


Figura 3.24 Quota di fatturato derivante da e-commerce (%, 2020)

Fonte: Eurostat / *n.d.



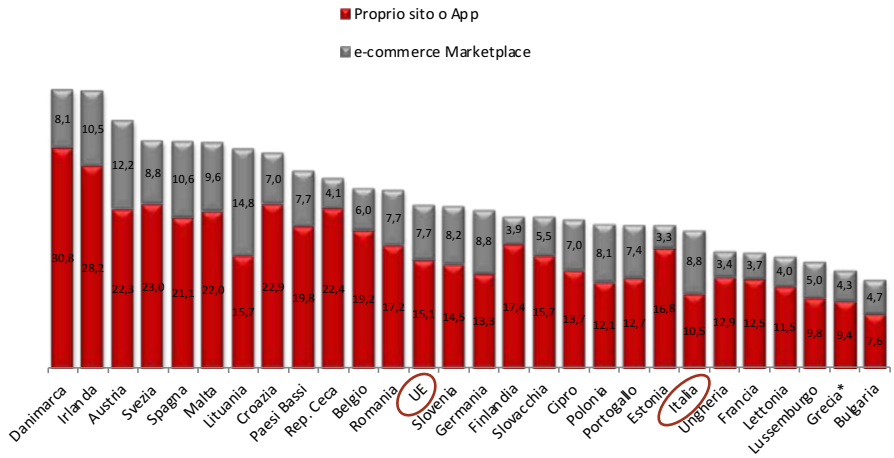
che si ripete ormai da diversi anni e che vede le grandi imprese trarre dall'*e-commerce* le percentuali maggiori di fatturato, essendo esse presumibilmente dotate di maggiori risorse e competenze da impiegare per trarre il massimo beneficio dal canale digitale.

A livello europeo, rispetto alle grandi imprese, a primeggiare è l'Irlanda, con una percentuale di fatturato derivante dall'*e-commerce* pari al 57%. Per le medie imprese, invece, il primato spetta alla Danimarca con il 41% di fatturato derivante dall'*e-commerce*. Quest'ultima, invero, registra il dato migliore – con un ben più modesto 14% - anche con riguardo alle piccole imprese, insieme a Croazia e Lituania. **L'Italia resta ancora distante dai best performer** e vicina alla media europea in relazione alla percentuale di fatturato dall'*e-commerce* prodotta dalle piccole e medie imprese, mentre resta ancora di 10 p.p. la differenza che riguarda le grandi realtà.

Molto interessanti i dati relativi alla percentuale di imprese che hanno utilizzato i propri siti per le vendite e la percentuale di imprese che invece hanno ricevuto ordini mediante *marketplace* (Fig. 3.25). Ebbene, ciò che emerge in tutti i Paesi è - con una buona dose di sorpresa vista la crescente

Figura 3.25 Provenienza degli ordini e-commerce (%, 2020)

Fonte: Eurostat
* dati 2019

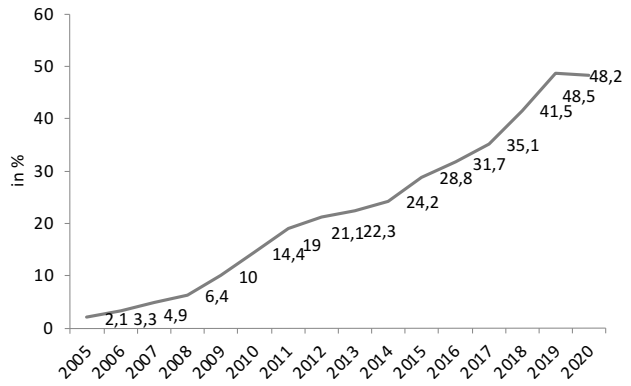


e massiccia affermazione dei *marketplace* - una schiacciante prevalenza della percentuale di imprese che utilizzano il proprio sito o App.

Nonostante sia ancora grave il gap rispetto ai Paesi più avanzati digitalmente, il contesto nazionale non risulta completamente refrattario alle tendenze di crescita in atto. I dati del Registro delle Imprese confermano **una dinamica crescente rispetto all'*e-commerce***, rilevando come nel 2020, le imprese che si sono registrate al Registro imprese con codice ATECO 47.91.1 relativo al commercio online (primario o secondario) siano state 10.467, contro le 6.968 dell'anno precedente, con un incremento del 50% (a fronte del +20% del 2019). Secondo i dati riportati nello studio realizzato da Casaleggio Associati nel 2021, in Italia la diffusione dell'online tra la popolazione (dai 2 anni in su) nel mese di dicembre 2020 ha raggiunto quota 74,7% (+4,7% rispetto all'anno precedente), con 44,7 milioni di utenti unici mensili e un incremento di 3,2 milioni di utenti. **Gli utenti che accedono da smartphone ammontano a 39,3 milioni**, ben il 90% della popolazione maggiorenne.

La dinamica di crescita che sta caratterizzando il nostro Paese è ben rappresentata nella Fig. 3.26

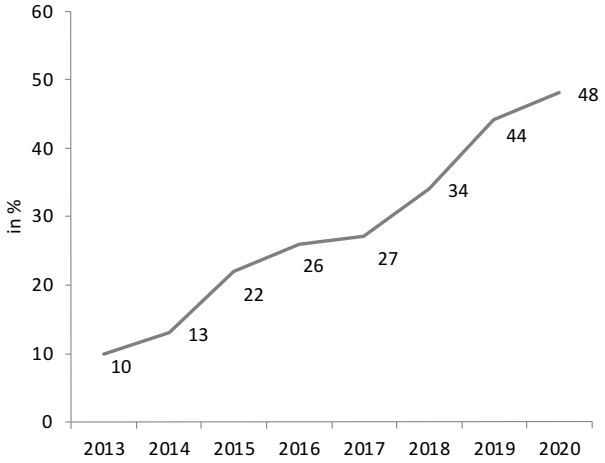
Figura 3.26 Crescita del fatturato e-commerce in Italia (mld)
Fonte: Casaleggio Associati



che stima il valore del fatturato *e-commerce* in Italia nel 2020 in **48,25 miliardi di euro**, con una riduzione dell'1% sul 2019, che interrompe il trend di forte crescita degli ultimi anni.

Il canale mobile nel 2020 continua a guadagnare importanza con un transato, in media, del 48% del fatturato delle aziende *e-commerce italiane*, con un incremento del 4% rispetto al 2019 (Fig. 3.27).

Figura 3.27 Andamento del canale mobile (% utilizzatori)
Fonte: Casaleggio Associati



Dal punto di vista della distribuzione del fatturato *e-commerce* (Fig. 3.28), a primeggiare è anche nel 2020 **il tempo libero** che rappresenta il 48% del fatturato totale, con un incremento del 12% decisamente inferiore al +21% segnato nell'anno precedente, in conseguenza, evidentemente, di una dinamica di crescita che ha riguardato il settore del gioco online e, al contempo di una grave perdita che ha colpito il comparto dello spettacolo. Al secondo posto in termini di fatturato, si posizionano i **centri commerciali online** con il 21%, contro il 16% dell'anno precedente e una crescita in termini di fatturato pari al 36%. Il **turismo** rivela le perdite maggiori (-58%) arrivando a pesare solo per l'11% del fatturato (contro il 26% dell'anno precedente). Il **settore alimentare** è quello che ha beneficiato della crescita maggiore rispetto all'anno

precedente con un +63%. Cresce del 12% invece l'**elettronica di consumo** raggiungendo il 4% del fatturato, così come **moda** ed **editoria** che, con un incremento rispettivamente del 14 e del 13%, riescono a conservare il 2% di *share*. Stabili le **assicurazioni** che mantengono la quota del 5% sul totale con un tasso di crescita del 6%. A chiudere la classifica i comparti **salute e bellezza** / **casa e arredamento**, settori che impattano decisamente poco sul totale (l'1% ciascuno) ma che nel 2020 sono cresciuti, rispettivamente, del 39 e del 24%, nonostante la perdita complessiva dell'8,9% del comparto del mobile in Italia.

Figura 3.28 Distribuzione del fatturato e-commerce (%, 2020)
Fonte: Casaleggio Associati

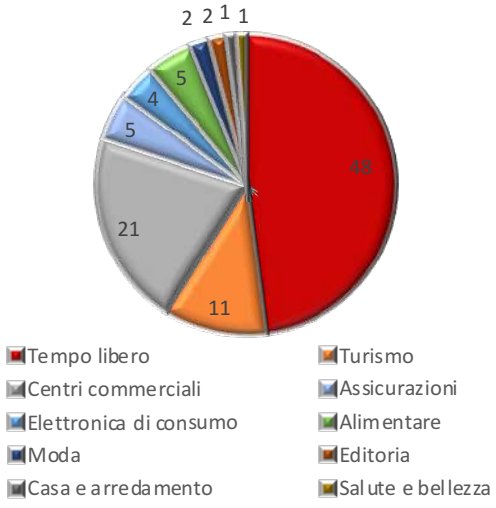
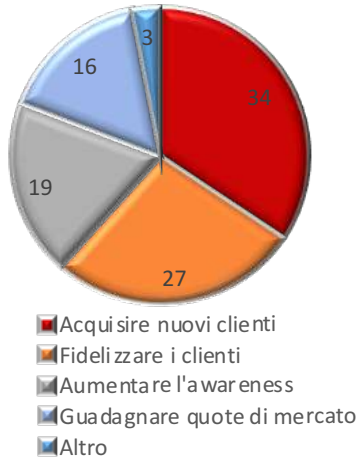


Figura 3.29 Principali obiettivi della strategia digitale (%, 2021*)
Fonte: Casaleggio Associati / * stime



Se questa è la fotografia del 2020, molto interessante è pure andare a verificare **la strategia e gli obiettivi fissati dalle aziende per il 2021** (Fig. 3.29). A primeggiare è nel 34% dei casi l'obiettivo di acquisizione di nuovi clienti, seguito dalla fidelizzazione degli attuali (27%). Per il 19% invece aumentare l'*awareness*, per il 16% guadagnare quote di mercato rispetto ai competitor, mentre per il 3% altri obiettivi.

3.4 LA DIGITALIZZAZIONE DEI SERVIZI FINANZIARI E BANCARI

Anche rispetto alla **digitalizzazione del settore bancario** l'emergenza sanitaria ha agito da fattore catalizzatore. Le forti limitazioni disposte soprattutto durante i periodi di lockdown hanno reso quantomai urgente per gli istituti bancari garantire ai propri clienti la disponibilità di servizi digitali in grado di assicurare la continuità della relazione con la banca e l'esercizio delle proprie attività finanziarie.

Nonostante sia immersa in un contesto generale di grande cambiamento e sostanziale ripensamento del tradizionale rapporto banca-cliente, l'Italia, rispetto all'***Internet banking***, continua ad arrancare. **Nel 2020, in particolare, soltanto il 39% degli individui ha utilizzato l'*Internet banking*** a fronte di una media europea del 58%. Se la distanza rispetto al dato medio è molto ampia e ci colloca quartultimi in Europa, enorme è il gap se si guarda alla vetta della classifica che vede Danimarca, Finlandia e Paesi Bassi con percentuali di utilizzo rispettivamente del 94%, 92% e 89% (Fig. 3.30).

Si tratta di un ritardo tanto grave quanto radicato che peraltro si è andato ad aggravare negli anni, passando da 13 p.p. del 2007 a 19 p.p. nel 2020. L'unico aspetto positivo è che rispetto al 2019 la distanza dal dato europeo si è ridotta di 3 p.p., suggerendo un timido avanzamento dell'Italia (Fig. 3.31).
In questo clima di radicata arretratezza la

Figura 3.30 Internet banking (% utilizzatori, 2020)

Fonte: Eurostat

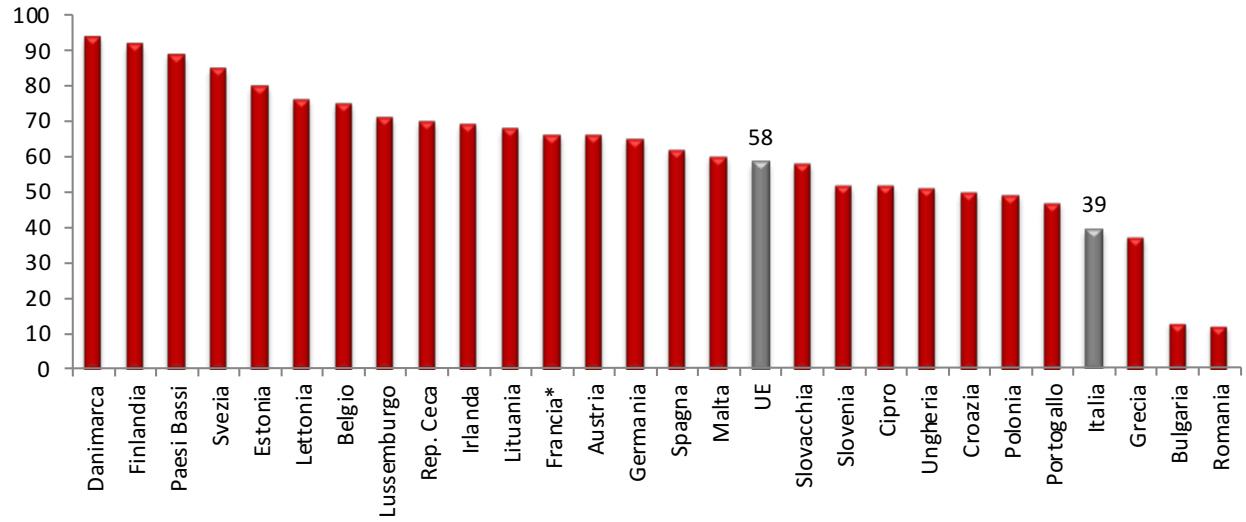
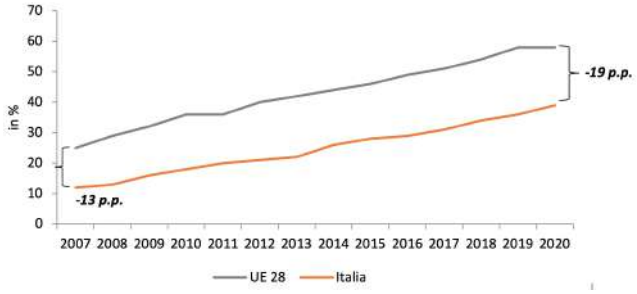


Figura 3.31 Trend di utilizzo dell'Internet banking. Italia vs Europa (%)

Fonte: Eurostat



pandemia ha imposto, anche agli italiani, il ripensamento delle proprie abitudini. La necessità di continuare a compiere operazioni finanziarie si è tradotta, secondo i dati del Politecnico di Milano, in un incremento ad aprile 2020 degli **utenti unici consumer online delle banche** del 17% rispetto allo stesso mese del 2019 e in una crescita delle transazioni online del 32%. Una grandissima accelerazione è stata rilevata anche rispetto al numero dei nuovi clienti acquisiti senza la necessità di una interazione fisica (+75% con punte del 198%).

Per la verifica delle principali tendenze in atto risulta preziosa l'analisi fornita dal Rapporto ABI Lab 2021 che offre una fotografia molto interessante e dettagliata del contesto italiano, sia lato domanda che lato offerta. Per quanto concerne i clienti, l'analisi, pur riconoscendo ancora il primato del pc in termini di volumi (173 milioni di operazioni dispositive nel 2020), quantifica in 171 milioni i volumi da ricondurre al mobile e una crescita del 15% dei clienti attivi su quest'ultimo canale. Le limitazioni imposte dalla pandemia hanno favorito tale dinamica traducendosi in un aumento degli accessi medi mensili per il cliente, rispettivamente +31% per il mobile e +14% per l'*Internet banking*.

Approfondendo l'analisi sul **canale mobile**, mediamente ogni banca offre 2,6 App (a campione costante il 76% ha mantenuto invariato il numero, il 12% lo ha aumentato e il 12% lo ha diminuito) con una forte attenzione per le funzionalità legate ai pagamenti, in particolare i bonifici istantanei, già offerti dal 52% delle banche e gli strumenti di gestione della finanza personale (57% già disponibili da app, 52% da *Internet*

banking).

Se la domanda, nonostante timidi passi avanti, continua ad esprimere una certa ritrosia nei confronti del digitale, **le imprese del settore bancario stanno vivendo a pieno la ventata di digitalizzazione** che le circonda andando a pianificare in maniera sempre più strutturata i propri investimenti nel canale digitale.

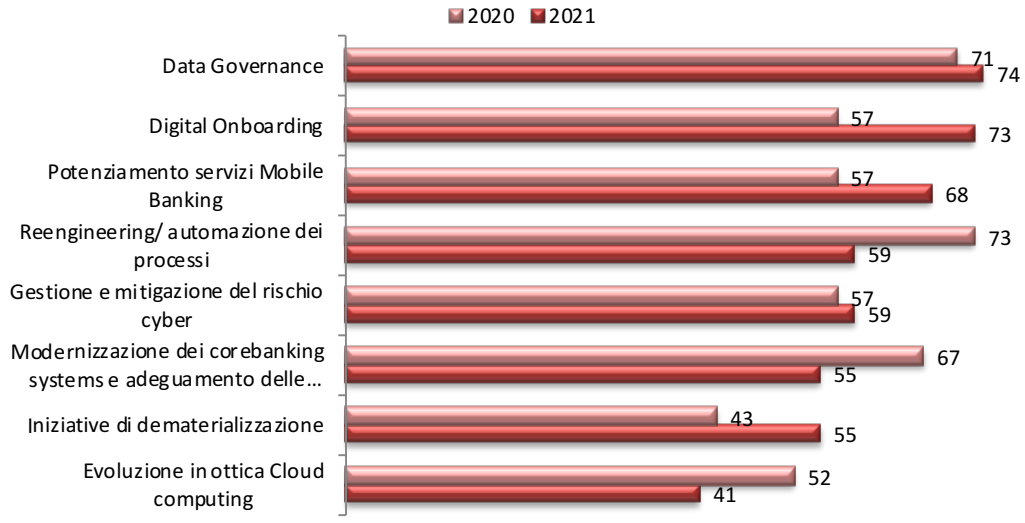
Secondo il Rapporto ABI Lab 2021, il **budget ICT per il 2021 è in aumento o stabile rispetto all'anno precedente**.

Se le risorse messe in campo sono rilevanti, quanto alle priorità ICT di investimento per le banche italiane (Fig. 3.32), a primeggiare risultano le iniziative legate alla data governance (74%), seguite da quelle sul *digital onboarding*[25] (73%), che hanno suscitato un interesse decisamente superiore rispetto a quanto registrato nel 2019 e da quelle tese al potenziamento dei servizi di *mobile banking* (68%), fondamentali per assicurare alle banche la capacità di gestire in maniera efficace la relazione con i clienti.
Quanto invece alle priorità di ricerca e sviluppo, i progetti considerati fondamentali dalle banche sono tesi soprattutto al potenziamento dell'**intelligenza artificiale** e alla **modernizzazione delle infrastrutture tecnologiche**. Seguono, in ordine di importanza, la gestione e mitigazione dei rischi cibernetici, le iniziative sui dati e il potenziamento dei servizi di *mobile banking*. In una logica di implementazione delle disposizioni contenute nella **direttiva europea PSD2 (*Payment Services Directive 2*)**, spiccano le iniziative in materia di *open banking*, rese possibili dalle piattaforme **API (*Application Programming Interface*)**. Centrale rimane anche l'automazione dei processi, il potenziamento della sicurezza dei canali remoti (identità e accessi) e la trasformazione delle architetture tecnologiche.

Non stupisce che le banche siano focalizzate sul rafforzamento degli strumenti di *mobile banking*. La forte accelerazione registrata dall'*e-commerce* si è tradotta nel crescente ricorso ai **pagamenti digitali**. Secondo lo studio Casaleggio Associati già richiamato, in tutto il mondo nel 2020 gli *e-wallet* sono stati il metodo di pagamento più utilizzato dai consumatori *e-commerce*, con il 44,5% delle transazioni totali, una crescita del

Figura 3.32 Principali Priorità ICT di investimento per le banche italiane 2021 (%)

Fonte: ABI Lab



[25] Per "*digital onboarding*" si intende una procedura digitale che permette ad aziende e istituzioni di conoscere e verificare online l'identità di una persona, per poter ottenere una firma legalmente valida di contratti e documenti.

6,5% rispetto al 2019 e stime secondo cui diventerà il principale metodo di pagamento nei prossimi anni per raggiungere, nel 2014, il 51,7% dei volumi di pagamento *e-commerce*. In seconda posizione si collocano, invece, le carte di credito (22,8% delle transazioni) e le carte di debito (12,3%). Residuale il ricorso al pagamento in contante alla consegna (con il 3,3% di quota di mercato) e ai bonifici istantanei le cui quote si fermano al 3,3 e 4%. In fase di affermazione invece la modalità di pagamento dilazionato (*buy now/pay later*), che secondo le stime passerà da una quota del 2,1% del 2020 (in crescita rispetto all' 1,6% nel 2019) al 4,2% entro il 2024.

3.5 LA DIGITALIZZAZIONE DELLA P.A.

La necessità di garantire ai cittadini l'esercizio di diritti fondamentali ha assunto, in un anno contrassegnato da periodi di lockdown, forti restrizioni agli spostamenti e pesantissime limitazioni alla socializzazione, assoluta centralità. A livello generale, nonostante l'emergenza sanitaria abbia favorito un'accelerazione del processo di **digitalizzazione delle PA**, assottigliando le differenze tra i Paesi membri, permane una situazione di disomogeneità sia nell'offerta di servizi digitali messa in campo alle autorità pubbliche, sia (e soprattutto) con riferimento all'effettivo utilizzo di tali servizi da parte di cittadini e imprese.

Quanto all'offerta, a livello generale, i dati dimostrano una buona maturità nella grande maggioranza dei Paesi dell'Unione in relazione all'offerta di servizi pubblici digitali per cittadini (Fig. 3.33) e imprese (Fig. 3.34). Nello specifico, i dati di seguito riportati descrivono in quale misura - completamente, parzialmente o per nulla - un servizio o un'informazione riguardante un servizio per i cittadini e le imprese è fornito online. Per quanto riguarda l'Italia, emerge una diversa tendenza: da un lato, l'offerta di servizi pubblici digitali per i cittadini risulta al di sotto della media (69% vs 75%), dall'altro, rispetto al mondo delle imprese, l'offerta di servizi digitali, con l'89% si colloca al di sopra del dato UE dell'84%.

Positiva, ma meno brillante a livello generale, anche la performance relativa alla percentuale di **dati precompilati nei moduli online dei servizi pubblici** (Fig. 3.35). A tale riguardo, se i dati parlano di realtà molto avanzate come Estonia, Finlandia e Malta, dove tale percentuale si attesta al 97%, **l'Italia con il 51% si pone ancora al di sotto della media europea** a distanza di 12 p.p., con un piccolo avanzamento di 3 p.p. rispetto al 2019. In un contesto che vede l'offerta di servizi digitali

Figura 3.33 Servizi digitali per i cittadini (%, 2020)

Fonte: Digital Agenda Scoreboard

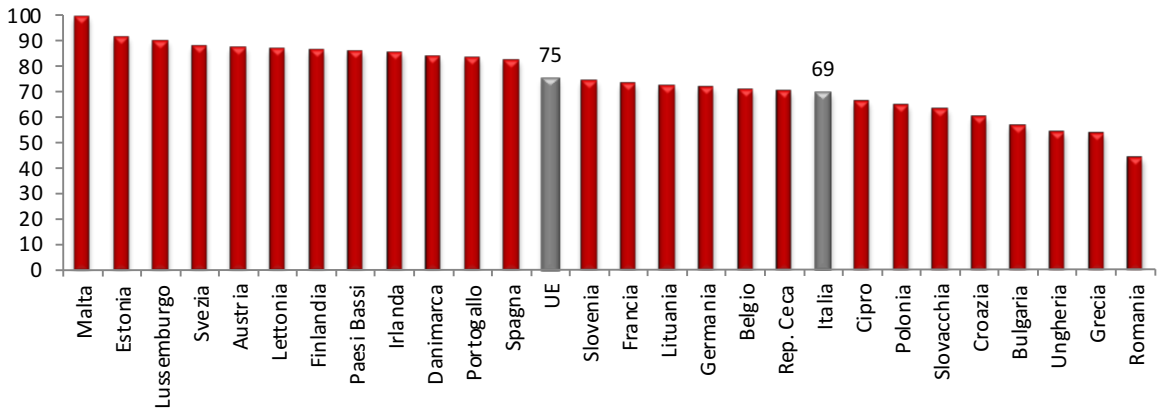


Figura 3.34 Servizi digitali per le imprese (%, 2020)

Fonte: Digital Agenda Scoreboard

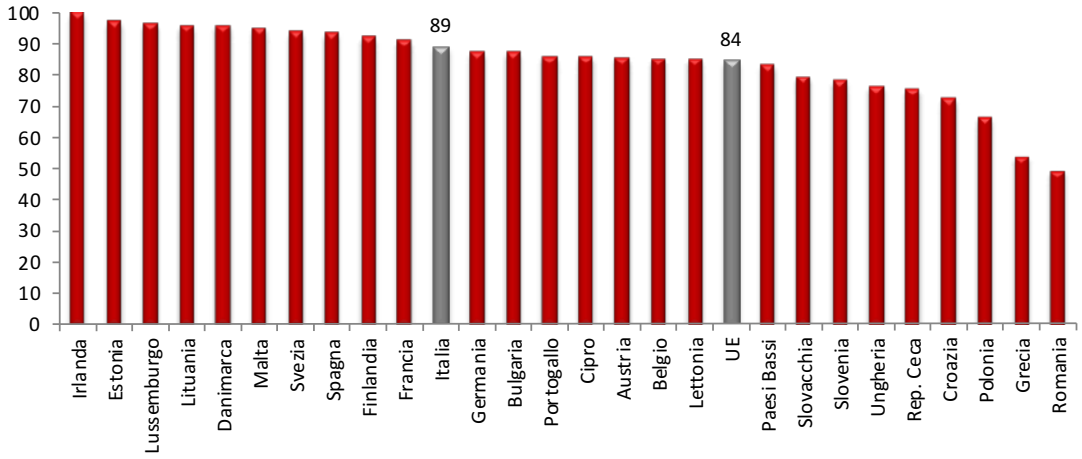
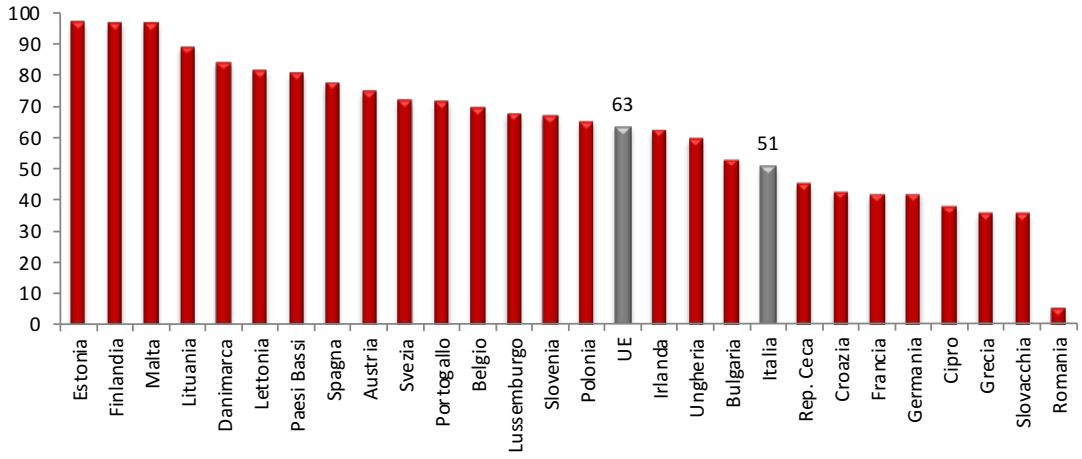


Figura 3.35 Percentuale di dati precompilati nei moduli online dei servizi pubblici (2020)

Fonte: Digital Agenda Scoreboard



da parte delle pubbliche amministrazioni abbastanza matura, la domanda di tali servizi da parte dei cittadini mostra una dinamica parzialmente diversa.

Il Nord Europa, secondo una tendenza consolidata negli anni, dimostra il maggior livello di maturità mentre l'Italia continua a occupare i gradini più bassi, posizionandosi terzultima con percentuali che non vanno oltre il 29%, ben al di sotto della media UE (Fig. 3.36).
Nonostante la grave immaturità mostrata dai cittadini italiani nell'utilizzo dei servizi digitali messi a disposizione dalle pubbliche amministrazioni, le misure di contenimento dei contagi ed i benefici messi in campo dal Governo accessibili, per lo più, mediante il canale online, hanno determinato una forte accelerazione nell'avvicinamento degli italiani ai servizi pubblici digitali.

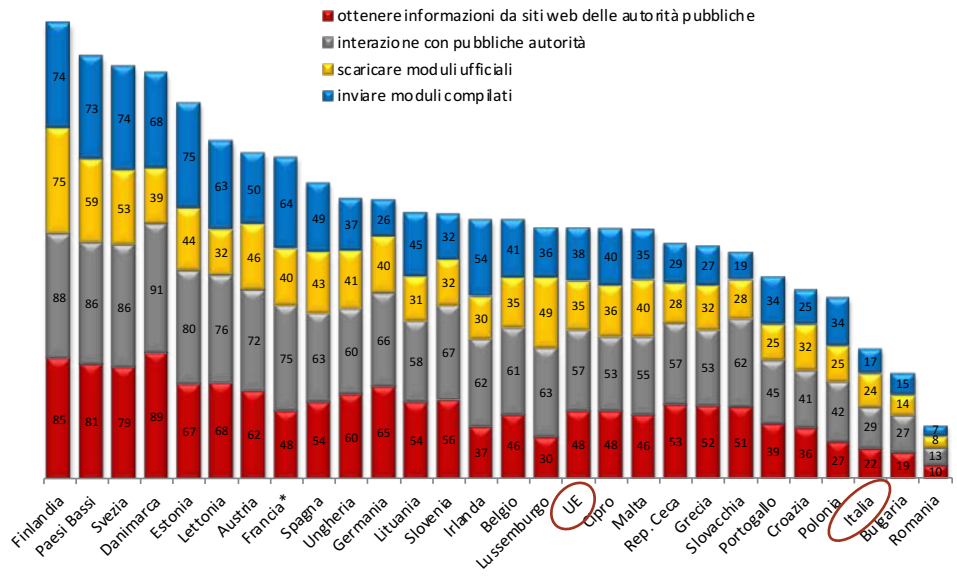
Tale effetto catalizzatore si è tradotto in un **fortissimo incremento nell'utilizzo del Sistema Pubblico di Identità Digitale (SPID)**: da gennaio a settembre 2021, infatti, sono circa 374 milioni gli accessi con SPID ai servizi online pubblici e privati.

I primi nove mesi del 2021 hanno visto un massiccio uso dell'identità digitale tale da superare il totale degli accessi del biennio precedente: 143,9 milioni nel 2020 e oltre 55 milioni nel 2019. L'accelerazione ha riguardato anche il numero di amministrazioni che utilizzano SPID: tale numero è cresciuto, in particolare, del 70%, superando gli 8.308 enti (dato del 3/10/2021), il doppio rispetto a ottobre 2020. Alle amministrazioni si aggiungono poi 53 fornitori privati che consentono l'uso di SPID per usufruire dei propri servizi.

Trend positivo anche rispetto al numero delle identità digitali rilasciate, che ad ottobre 2021 supera la cifra di 25 milioni, segnando un incremento del 61,5% da inizio 2021.

Figura 3.36 eGovernment (% individui, 2020)

Fonte: Eurostat / *dati 2019



CAPITOLO 4

UNA MISURA DELLO SVILUPPO DELLE RETI E SERVIZI DIGITALI: L'ITALIA NELL'I-COM ULTRABROADBAND INDEX (IBI)

4.1 METODOLOGIA

L'**I-Com Ultrabroadband Index (IBI)**, giunto alla 8ª edizione, sintetizza i dati esposti e analizzati all'interno dello studio annuale e ha lo scopo di fotografare **lo sviluppo delle reti e dei servizi digitali nei mercati nazionali europei**, contestualizzando la posizione relativa dell'Italia. Dal punto di vista metodologico, le variabili considerate per l'elaborazione dell'IBI vengono di seguito elencate:

- il grado di penetrazione della banda larga rispetto al numero di famiglie;
- il grado di sviluppo dell'*e-commerce*;
- l'accesso giornaliero a Internet da parte degli individui;
- la percentuale di connessioni fisse con capacità di download maggiore o uguale a 100 Mbps;
- il grado di copertura della banda larga nelle aree rurali, in termini di percentuale di famiglie raggiunte;
- il grado di copertura della banda ultralarga (connessioni pari o superiori a 30Mbps), in percentuale di abitazioni raggiunte;
- il grado di copertura o disponibilità di connessioni in tecnologia *fiber-to-the-premises*, in termini di percentuale di abitazioni raggiunte;
- il grado di copertura 4G (LTE), in percentuale di abitazioni raggiunte dalla rete;
- il grado di copertura 5G.

Con le nove variabili così definite sono state elaborate tre versioni dell'indice: una generale, comprendente i valori relativi a tutti gli indicatori, e due sottoindici, il primo specifico per la domanda, che include i dati relativi alle prime 4 variabili elencate, il secondo focalizzato sull'offerta, basato sugli ultimi 5 indicatori.

Dal punto di vista metodologico, per ciascun Paese è stata calcolata una media di tutti gli indicatori analizzati, attribuendo un peso complessivo equivalente alla domanda e all'offerta[26]. Le medie così calcolate sono poi state normalizzate rispetto al Paese *best performer*, così da elaborare una scala da 0 a 100 punti.

4.2 RISULTATI DELL'ANALISI

L'IBI complessivo è illustrato nella Tabella 4.1 e comprende la graduatoria dei Paesi ordinati secondo le migliori performance complessive relativamente all'edizione 2021.

La Danimarca, con un punteggio pari a 100, prende il posto della Svezia nel guidare la classifica europea. Ciò avviene grazie all'esemplare copertura della rete 5G, già pari all'80% (solo il 14% per la Svezia). La performance è spiegata anche da una buona copertura delle reti fisse f*iber-to-the-premises* (FTTP), nettamente superiore alla media europea (70% contro 42,5%), sulla quale a farsi notare sono anche Lettonia (89%), Spagna (87%), Portogallo (85%) e Svezia (80%), nonché Lussemburgo (72%) ed Estonia (71%). La Danimarca, inoltre, continua a eccellere sul fronte della domanda digitale, con valori elevati in tutti e quattro gli indicatori, in particolare con riguardo alla diffusione dell'*e-commerce*, dove si afferma prima assoluta sul panorama europeo, con l'89% di cittadini che acquista online.

Seguono nella classifica, conquistando il podio, Svezia (94,9) e Paesi Bassi (94,4). La prima si distingue in maniera particolare sulle reti fisse veloci, sia lato domanda che lato offerta: l'80% delle abitazioni è, infatti, connesso in FTTP (+38 p.p. rispetto alla media UE), e altrettanto elevato è il grado di adozione (l'80% degli abbonamenti in banda larga è con una velocità almeno pari a 100

[26] Si precisa che, per quanto riguarda la copertura della rete mobile, si è scelto di dare un peso relativamente maggiore al 5G (7,5) rispetto al 4G (5), essendo quest'ultima una tecnologica oramai tendenzialmente matura. Nel complesso, alla copertura di rete mobile viene attribuito lo stesso peso attribuito a ciascuna delle altre 7 variabili (12,5).

Mbps). Si segnala, invece, una scarsa performance per quanto riguarda la copertura della banda larga nelle aree rurali (81%), al di sotto della media europea. I Paesi Bassi, che guadagnano due posizioni rispetto al 2020, hanno, invece, un profilo molto più simile alla Danimarca, con una performance particolarmente brillante sul 5G (copertura dell'80%, contro solo il 13,8% europeo) e un grado di diffusione molto elevato dell'*e-commerce* (87% degli individui). I Paesi Bassi sono meno forti, invece, sulla copertura della rete FTTP (36%), inferiore rispetto alla media UE di 6,9 p.p.

L'Italia finalmente guadagna due posizioni rispetto alla scorsa edizione, piazzandosi al 20° posto. A dispetto di questo risultato positivo, va detto che il punteggio IBI si riduce, seppure di poco (quasi 3 punti), conseguente a un aumento del divario rispetto al vertice della classifica. **Il nostro Paese rimane sotto la media europea in gran parte degli indicatori**, in particolar modo con riguardo all'*e-commerce*, abitudine di solo il 44%

Tabella 4.1 I-Com Broadband Index (IBI)

Fonte: Elaborazioni I-Com

	IBI			Ranking		
PAESI	2020	2021	Variazione 2021 su 2020	2020	2021	Variazione 2021 su 2020
Danimarca	97,3	100,0	2,7	2	1	1
Svezia	100,0	94,9	-5,1	1	2	-1
Paesi Bassi	93,8	94,4	0,5	5	3	2
Spagna	95,8	94,0	-1,8	4	4	0
Lussemburgo	97,3	93,6	-3,7	2	5	-3
Lettonia	91,6	88,6	-3,0	6	6	0
Irlanda	85,1	86,5	1,4	13	7	6
Portogallo	88,7	85,2	-3,4	7	8	-1
Ungheria	87,1	84,3	-2,8	9	9	0
Malta	88,1	83,4	-4,8	8	10	-2
Belgio	87,1	82,4	-4,7	9	11	-2
Slovenia	86,2	81,7	-4,5	12	12	0
Romania	82,2	81,5	-0,7	19	13	6
Germania	83,8	81,0	-2,8	16	14	2
Finlandia	86,4	80,4	-6,0	11	15	-4
Estonia	83,8	79,6	-4,2	16	16	0
Rep. Ceca	84,6	79,1	-5,4	15	17	-2
Francia	81,5	79,0	-2,6	20	18	2
Austria	78,3	77,6	-0,7	18	19	-1
Italia	**79,8**	**77,0**	**-2,9**	**22**	**20**	**2**
Slovacchia	84,8	76,7	-8,1	14	21	-7
Polonia	76,5	74,8	-1,7	23	22	1
Lituania	81,0	74,0	-7,0	21	23	-2
Cipro	75,6	73,1	-2,5	25	24	1
Croazia	75,9	71,7	-4,2	24	25	-1
Bulgaria	69,8	65,4	-4,4	26	26	0
Grecia	68,1	63,5	-4,6	27	27	0

degli italiani e aumentato soltanto di 6 p.p. rispetto all'anno precedente. Nonostante il 2020 sia stato un anno del tutto particolare, caratterizzato da frequenti e prolungati lockdown che hanno dato una spinta senza precedenti ai servizi digitali, la diffusione dell'*e-commerce* rimane ben inferiore alla media UE (65%).

Sotto la media europea anche la copertura della rete FTTP (circa 34%), con un ritardo rispetto al resto d'Europa che si amplia, passando dai 3,7 p.p. di distacco agli 8,8 p.p. (la media dell'Unione, per il 2020, è infatti pari al 42,5%) e della rete 5G, sebbene su questo piano la copertura dell'8% - inferiore alla media europea (13,8%), per via della presenza di pochi Paesi con una copertura altissima (in particolare, Danimarca e Paesi Bassi con l'80% circa e Austria col 50% circa) - non è da interpretarsi troppo negativamente, se si considera che la maggior parte degli Stati membri non presenta ancora alcuna copertura della tecnologia mobile di quinta generazione.

Degno di nota è il segnale positivo che, finalmente, arriva sul **fronte della domanda**, che pone l'Italia per la prima volta al di sopra della media UE nel grado di penetrazione della banda larga ultra veloce, con quasi il 47% degli abbonamenti in banda larga che prevedono una velocità almeno pari a 100 Mbps: un dato cresciuto di oltre 11 p.p. (+7,2 p.p. per l'UE), cosa che le ha consentito di superare la media UE di 2,2 p.p. Un risultato senza dubbio legato all'effetto Covid-19, che ha tenuto a casa una larga fascia della popolazione per gran parte del 2020 e costretto a svolgere presso le proprie abitazioni tutte le attività prima eseguite prevalentemente fuori, da quelle lavorative a quelle scolastiche, passando per le relazioni sociali. Ciò ha portato un certo numero di famiglie, prima "*disinteressate*", a equipaggiarsi con un servizio di connettività a elevate prestazioni. Si precisa, inoltre, che l'effetto registrato è, con ogni probabilità, solo parziale, trattandosi di dati aggiornati a giugno 2020.

Da sottolineare, per rimanere a Paesi del Sud Europa, che **la Spagna mantiene il suo quarto posto**, raggiunto lo scorso anno grazie agli importanti progressi nella connettività ultra veloce (≥ 100 Mbps). Progressi che sono proseguiti nel corso dell'ultimo anno, soprattutto sul piano della domanda, aumentata di 12 p.p. nel giro di un anno e attestatasi a quasi l'80% degli abbonamenti, con un divario positivo di ben 35,3 p.p. rispetto alla media europea. La copertura in FTTP raggiunge l'85% delle famiglie spagnole (+5 p.p. rispetto all'anno prima e ben 42,4 p.p. in più rispetto alla media UE). Inoltre, anche la Spagna ha investito sul 5G, che raggiunge una copertura appena al di sotto della media europea (12,5%).
Altro Paese che non passa inosservato è l'Irlanda, che si piazza in settima posizione, guadagnando ben 6 posti: merito, in particolare, degli sforzi compiuti sul 5G (che raggiunge il 30% della popolazione) e dei progressi dell'*e-commerce* (74%), che vede impegnato il 7% della popolazione in più rispetto all'anno prima e il 9% in più rispetto ai cittadini europei.

Altrettante posizioni guadagna la Romania che, come la Spagna, eccelle sul piano della connettività ultraveloce, registrando oltre 30 p.p. di scarto rispetto al resto d'Europa, sia sul fronte della domanda che dell'offerta, sebbene resti, invece, fortemente indietro in quanto a uso di Internet e *e-commerce*. Anche in questo caso, si tratta di uno dei Paesi che ha investito sul 5G, che raggiunge l'11,7% della popolazione.

Di contro la Finlandia, non registrando miglioramenti sostanziali e non avendo ancora investito sul mobile di ultima generazione, continua a scendere di posizione e a perdere terreno (-6 punti rispetto all'IBI 2020 e 4 posizioni nella classifica europea). A perdere molto è anche la Slovacchia (-8 punti e 7 posizioni), che si classifica 21°, appena sotto l'Italia: a eccezione della copertura di rete FTTP e della copertura della banda larga nelle zone rurali, infatti, il Paese registra risultati peggiori della media UE in tutti gli

indicatori, in particolar modo rispetto a copertura NGA e sottoscrizione di abbonamenti con velocità ≥100 Mbps, nonché la copertura del 5G in cui il Paese non ha investito per il momento.

Le tabelle che seguono mostrano, come anticipato in precedenza, **il grado di sviluppo della domanda e dell'offerta separatamente**, al fine di evidenziare eventuali scostamenti tra le due (Tab.4.2 e Tab.4.3).

Si può così notare come cambia il posizionamento dell'Italia che, da un 20° posto nella classifica generale, **si posiziona 22°** sul piano della domanda, guadagnando una posizione rispetto alla scorsa edizione, merito – come abbiamo già avuto modo di sottolineare – soprattutto della spinta impressa dall'emergenza sanitaria alla sottoscrizione di abbonamenti Internet ultraveloci. Il divario rispetto all'apice, dopo la stasi dello scorso anno, torna a ridursi di 6 punti.

La posizione guadagnata sul piano della domanda

Tabella 4.2 -Com Broadband Index (Lato domanda)

Fonte: Elaborazioni I-Com

	IBI			Ranking		
PAESI	2020	2021	Variazione 2021 su 2020	2020	2021	Variazione 2021 su 2020
Svezia	100,0	100,0	0,0	1	1	0
Danimarca	89,9	94,0	4,1	3	2	1
Lussemburgo	88,1	93,5	5,3	4	3	1
Spagna	85,7	92,4	6,7	7	4	3
Paesi Bassi	91,1	92,2	1,2	2	5	-3
Belgio	85,9	90,0	4,1	6	6	0
Finlandia	86,2	88,9	2,7	5	7	-2
Germania	81,7	85,2	3,5	8	8	0
Ungheria	79,1	84,9	5,8	10	9	1
Irlanda	79,4	83,4	3,9	9	10	-1
Lettonia	77,0	82,5	5,5	12	11	1
Malta	77,3	82,2	4,8	11	12	-1
Polonia	72,4	79,8	7,4	17	13	4
Portogallo	74,6	79,6	5,0	14	14	0
Francia	74,0	79,2	5,2	16	15	1
Rep. Ceca	74,0	77,2	3,3	15	16	-1
Slovenia	70,8	76,5	5,7	19	17	2
Estonia	75,0	76,0	1,1	13	18	-5
Romania	68,6	75,1	6,5	22	19	3
Slovacchia	68,6	74,8	6,1	21	20	1
Lituania	72,4	74,3	2,0	18	21	-3
Italia	**67,0**	**73,0**	**6,0**	**23**	**22**	**1**
Austria	70,4	72,6	2,2	20	23	-3
Cipro	60,9	66,4	5,5	24	24	0
Croazia	59,8	65,1	5,3	25	25	0
Grecia	53,2	57,2	4,0	26	26	0
Bulgaria	51,1	56,9	5,8	27	27	0

Tabella 4.3 I-Com Broadband Index (Lato offerta)

Fonte: Elaborazioni I-Com

	IBI			Ranking		
PAESI	2020	2021	Variazione 2021 su 2020	2020	2021	Variazione 2021 su 2020
Danimarca	98,3	100,0	1,7	4	1	3
Paesi Bassi	90,6	90,9	0,2	9	2	7
Spagna	99,5	90,0	-9,5	3	3	0
Lettonia	99,7	89,3	-10,4	1	4	-3
Lussemburgo	100,0	88,2	-11,8	2	5	-3
Portogallo	96,5	85,7	-10,8	6	6	0
Irlanda	85,3	84,5	-0,8	17	7	10
Svezia	93,8	84,3	-9,6	8	8	0
Romania	90,0	82,9	-7,0	12	9	3
Slovenia	95,5	81,9	-13,6	7	10	-3
Malta	92,9	79,6	-13,3	10	11	-1
Ungheria	89,3	78,7	-10,6	13	12	1
Estonia	87,0	78,5	-8,5	14	13	1
Austria	80,9	78,0	-2,9	19	14	5
Rep. Ceca	89,3	76,3	-13,0	11	15	-4
Italia	**87,0**	**76,3**	**-10,7**	**15**	**16**	**-1**
Cipro	84,8	75,4	-9,5	24	17	7
Francia	83,6	74,1	-9,5	22	18	4
Croazia	86,4	74,0	-12,4	16	19	-3
Slovacchia	94,8	74,0	-20,9	5	20	-15
Germania	80,6	72,0	-8,6	25	21	4
Belgio	82,9	70,1	-12,8	17	22	-5
Bulgaria	83,2	69,9	-13,3	21	23	-2
Lituania	84,2	69,3	-14,9	23	24	-1
Finlandia	81,3	67,2	-14,1	20	25	-5
Grecia	78,0	66,1	-12,0	26	26	0
Polonia	75,7	65,4	-10,3	27	27	0

viene, invece, persa sull'offerta, dove il nostro Paese si colloca al **16° posto**, a vantaggio dell'Ungheria, che è cresciuta più velocemente nell'ultimo biennio anche lato offerta (oltre che negli indicatori della domanda dove purtroppo ci guarda dall'alto del suo nono posto).

L'Italia, invece, ha registrato un incremento nella copertura dell'FTTP di soli 4 p.p. nell'ultimo anno, a fronte di un incremento medio, a livello europeo, di 9 p.p.

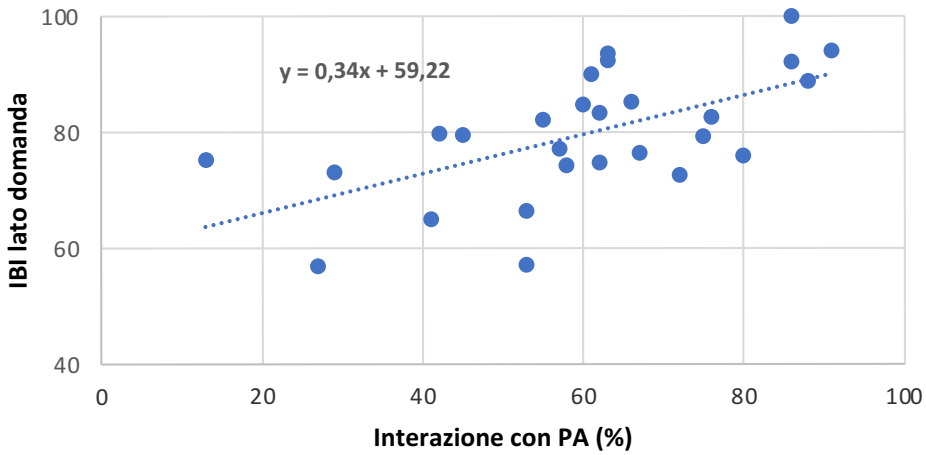
Si registra, in generale, un'inversione di tendenza nel processo di convergenza tra Paesi: migliora per quanto riguarda la domanda di digitale, risultando ridotto il divario tra il primo e l'ultimo Paese nella graduatoria generale, e peggiora quello relativo all'offerta, aumentando la distanza tra migliore e peggior Paese di 10 p.p.
Sebbene in diminuzione, va precisato che **il**

divario, a livello europeo, nella domanda di digitale resta comunque più ampio rispetto all'offerta. Anche nel nostro Paese, il miglioramento è tangibile ma è anche spiegato da un evento, la pandemia, di natura (per fortuna) del tutto eccezionale. Occorre dunque rafforzare gli sforzi per far sì che il processo di convergenza rispetto ai Paesi più performanti non si arresti. In questo senso, riteniamo che **un sostegno alla domanda digitale possa venire dal settore pubblico**. Esiste, in effetti, una correlazione positiva (e pari al 60%) tra il grado di interazione con la PA – intesa come percentuale di individui che interagiscono con la PA attraverso Internet – e l'indice IBI lato domanda: i Paesi con un maggior grado di interazione online tra cittadini e PA mostrano anche un miglior indice di domanda digitale[27] (Fig. 4.1). In particolare, a un 10% in più di cittadini che utilizzano i servizi pubblici digitali è associato, in media, un punteggio IBI lato domanda superiore di circa 3,4 punti. Appare, dunque, sempre più importante puntare sulla digitalizzazione della PA e dei servizi pubblici, che possono fornire un importante incentivo alla domanda di digitale da parte dei cittadini particolarmente restii e reticenti al cambiamento che, per ragioni di necessità, potrebbero invece apprezzare i benefici della digitalizzazione e replicare l'esperienza in altri ambiti. L'Italia, in questo senso, non brilla affatto: è, infatti, il terzultimo Paese nel quadro europeo, con un grado di interazione con la PA **pari a solo il 29%**, enormemente distante dai Paesi nordici, che registrano percentuali comprese tra l'86% e il 91%.

Dall'altro lato, un miglioramento appare necessario, in quanto la domanda digitale rappresenta un importante input dei processi di avanzamento tecnologico che caratterizzeranno il futuro della nostra società. Ad esempio, come mostra la figura 4.2, esiste una **relazione positiva tra domanda digitale e investimenti in Intelligenza Artificiale (IA)**: nei Paesi caratterizzati da un maggior grado di sviluppo della domanda digitale si riscontrano anche maggiori investimenti in IA. In particolare, a un punteggio IBI lato domanda superiore di 10 punti è associato, in media, un investimento pro-capite di 6,5 euro in più. Ciò potrebbe tradursi, per l'Italia, in un investimento addizionale di circa **390 milioni di euro** rispetto agli attuali 60 milioni: un incremento

Figura 4.1 Relazione tra domanda digitale e servizi pubblici digitali

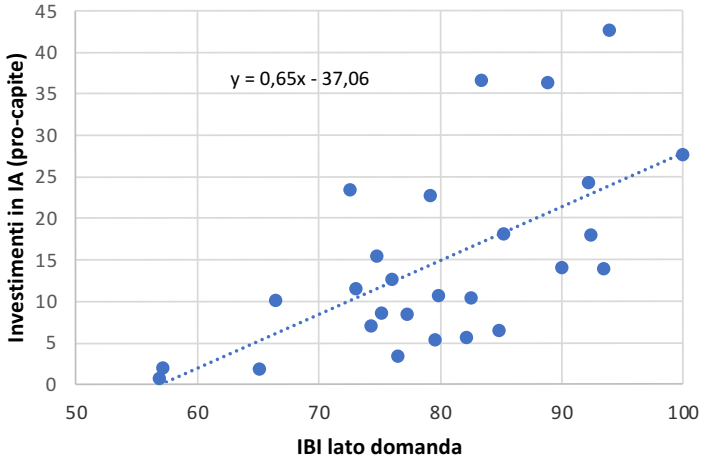
Fonte: Elaborazioni I-Com su dati Eurostat



[27] È bene precisare che anche una relazione inversa tra le due variabili potrebbe essere altrettanto valida. Per verificare questo, occorrerebbe svolgere un'analisi più sofistica e rigorosa che verifichi anche il contributo di altre variabili, ma che esula dagli scopi del presente lavoro.

Figura 4.2 Relazione tra Intelligenza Artificiale e domanda digitale

Fonte: Elaborazioni I-Com su dati Eurostat e Commissione europea

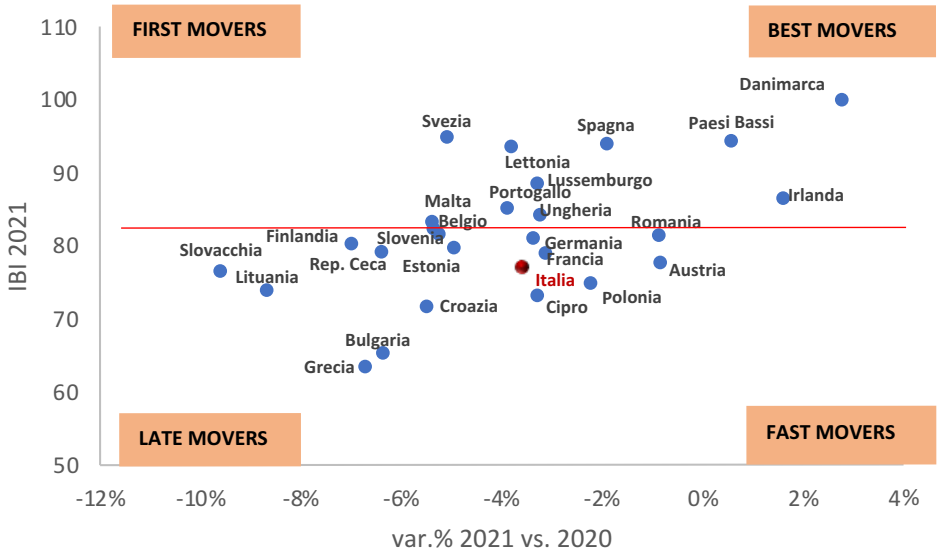


stimato di oltre il 50%, a fronte di un significativo (ma non impossibile) miglioramento della domanda digitale, tenendo naturalmente presente che gli investimenti in IA dipendono da molti altri fattori, più o meno collegati con lo sviluppo digitale di un Paese.

Infine, le figure che seguono (Figg. 4.3, 4.4 e 4.5) mostrano congiuntamente il grado di sviluppo digitale dei vari Paesi – misurato dall'IBI 2021 (asse verticale) – e la variazione percentuale dell'indice tra il 2020 e il 2021 (asse orizzontale). **L'Italia continua a posizionarsi nel cluster dei Paesi *fast mover***, ossia quelli che, pur denotando livelli di sviluppo digitale inferiore, presentano una buona dinamica di crescita nel tempo. E questo è, per la prima volta, merito soprattutto della domanda, che presenta una tendenza nel tempo più dinamica, con una variazione percentuale più marcata rispetto alla media UE[28]. L'offerta digitale,

Figura 4.3 Livello e dinamica della digitalizzazione complessiva

Fonte: Elaborazioni I-Com



invece, nell'ultimo anno mostra minore dinamicità, registrando una variazione di punteggio inferiore alla media europea e uno *score*, per il 2021, sostanzialmente in linea con la media europea. Ciò è spiegato in parte dal fatto che, per quanto riguarda le reti fisse, l'Italia, nell'ultimo anno, ha nuovamente visto aumentare lo svantaggio, parzialmente recuperato negli anni precedenti, rispetto al resto d'Europa, in parte dal fatto che, sul fronte 5G, la nuova frontiera della connettività mobile, seppur attiva, registra una performance inferiore alla media europea.

Figura 4.4 Livello e dinamica della domanda digitale

Fonte: Elaborazioni I-Com

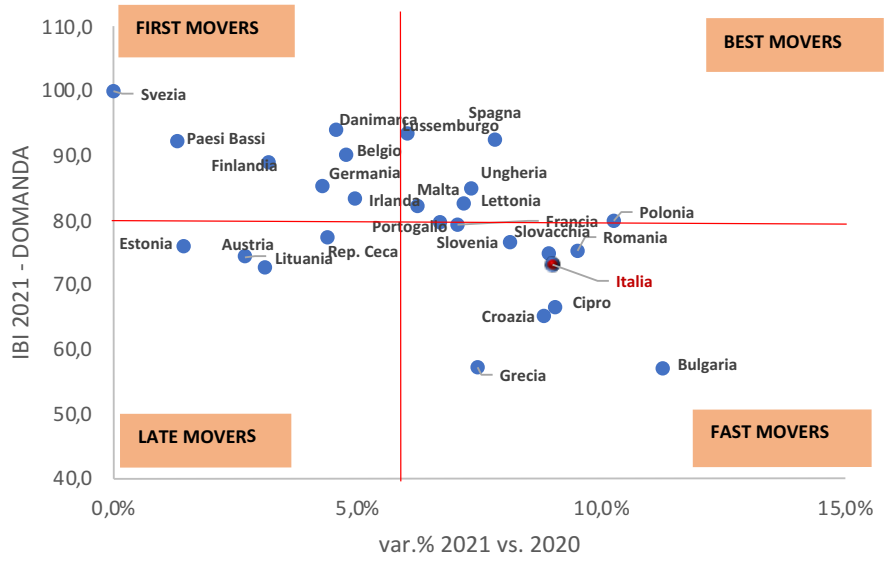
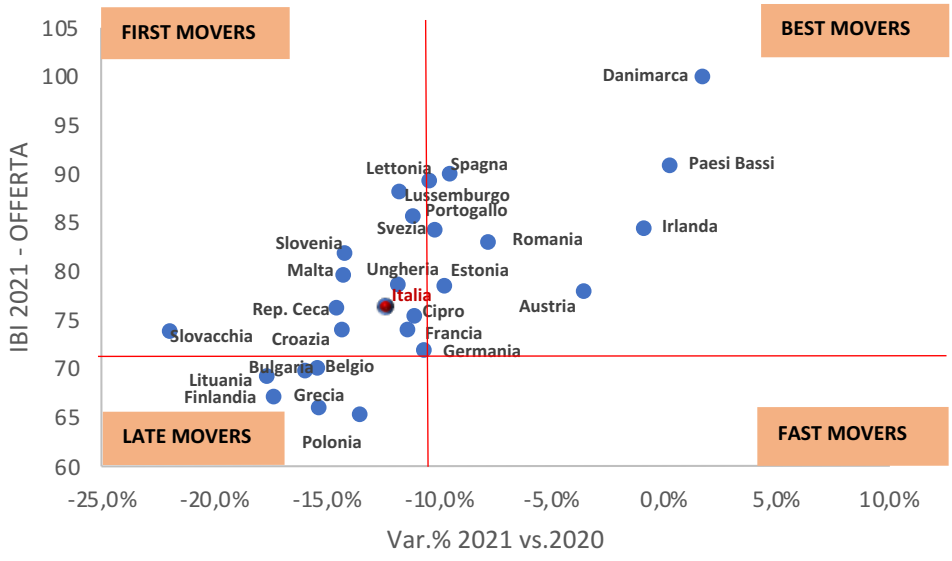


Figura 4.5 Livello e dinamica dell'offerta digitale

Fonte: Elaborazioni I-Com



[28] L'IBI UE è calcolato, così come per i singoli Paesi, basandosi sulla media UE: quest'ultima è calcolata come media delle medie relative ai singoli Paesi, ponderate per il numero di famiglie presenti in ciascun Paese.

CAPITOLO 5

LE POLICY NAZIONALI A SOSTEGNO DELLA DIGITALIZZAZIONE

5.1 IL PIANO NAZIONALE DI RIPRESA E RESILIENZA. GLI OBIETTIVI E LE RISORSE ASSEGNATE AL DIGITALE

La pandemia scoppiata nel 2020 ha travolto in maniera inaspettata e con una forza inaudita l'intera UE, che ha cercato di rispondere alla crisi economica e sociale con interventi senza precedenti. La principale iniziativa, e quella che certamente avrà maggiori ripercussioni nel medio-lungo termine, è il **Next Generation EU (NGEU)**, un programma poderoso, articolato in due strumenti principali, il **Dispositivo per la Ripresa e Resilienza (RRF)** e il **Pacchetto di Assistenza alla Ripresa per la Coesione e i Territori d'Europa (REACT-EU)**, incentrato su investimenti e riforme per accelerare la transizione ecologica e digitale, rafforzare la formazione dei lavoratori e conseguire una maggiore equità di genere, territoriale e generazionale. L'Italia è la prima beneficiaria, in valore assoluto, dei fondi previsti dal programma: l'RRF, in particolare, garantisce risorse per 191,5 miliardi di euro, da impiegare nel periodo 2021-2026, di cui 68,9 miliardi sono sovvenzioni a fondo perduto. A ciò si aggiunge la possibilità per l'Italia di utilizzare appieno la propria capacità di finanziamento tramite i prestiti della RRF, stimata in 122,6 miliardi di euro.

In attuazione del dispositivo RRF che richiede agli Stati membri di presentare un pacchetto di investimenti e riforme, il **Piano Nazionale di Ripresa e Resilienza (PNRR)**, il 25 aprile scorso il Governo ha presentato il Piano italiano - definitivamente approvato il 13 luglio scorso con decisione di esecuzione del Consiglio - che si articola in **sei Missioni** e **16 Componenti**.

Le sei Missioni del Piano, in particolare, sono: digitalizzazione, innovazione, competitività, cultura e turismo; rivoluzione verde e transizione ecologica; infrastrutture per una mobilità sostenibile; istruzione e ricerca; inclusione e coesione; salute.

Dal punto di vista metodologico, accanto a riforme orizzontali o di contesto d'interesse trasversale traversale a tutte le Missioni, il Piano prevede **riforme abilitanti** e **riforme settoriali** cui si aggiungono le misure che, sebbene non ricomprese nel perimetro del Piano, vanno considerate concorrenti alla realizzazione degli obiettivi generali del PNRR. Il Piano, in particolare, annuncia quattro importanti riforme di contesto: pubblica amministrazione, giustizia, semplificazione della legislazione e promozione della concorrenza. La riforma finalizzata alla razionalizzazione e semplificazione della legislazione, nello specifico, persegue il fine di abrogare o modificare leggi e regolamenti che rendono particolarmente gravosa la vita quotidiana dei cittadini, delle imprese e della P.A. andando a intervenire sulle leggi in materia di pubbliche amministrazioni e di contratti pubblici, sulle disposizioni ostative della concorrenza e sulle regole e procedure che hanno favorito il verificarsi di frodi o episodi corruttivi. Rispetto invece al tema concorrenza, nel PNRR il Governo si è impegnato a presentare in Parlamento il **disegno di legge annuale per il mercato e la concorrenza** e ad approvare norme che possano agevolare l'attività d'impresa in settori strategici, come le reti digitali, l'energia e i porti.

Rispetto al **digitale**, il Piano, partendo dalla considerazione degli enormi benefici in termini di incremento della produttività, innovazione e occupazione, accesso più ampio all'istruzione e alla cultura e riduzione dei divari territoriali che la rivoluzione digitale garantisce e dalla constatazione del ritardo in termini di adozione digitale ed innovazione tecnologica che continua a caratterizzare il nostro paese, ha fissato innanzitutto **obiettivi di connettività**. Nello specifico, il Piano persegue il fine di garantire una connettività omogenea ad alta velocità in tutto il Paese per residenti, aziende, scuole e ospedali, mediante l'utilizzo di tutte le tecnologie più avanzate (Fibra, FWA7, 5G) e attraverso semplificazioni normative in grado di facilitarne

l'implementazione.

Cruciale la **digitalizzazione della PA** focalizzata su una strategia "*cloud first*" che prevede la possibilità di migrare verso una nuova infrastruttura cloud nazionale all'avanguardia (**"*Polo Strategico Nazionale*", PSN**) o verso un cloud "*pubblico*" sicuro, a seconda della sensibilità dei dati e dei servizi coinvolti e la garanzia di piena interoperabilità tra enti pubblici e le loro basi informative al fine di snellire le procedure pubbliche grazie alla piena realizzazione del principio del "*once only*" (molto rilevante, in tale logica, il progetto di rafforzamento dell'identità digitale).

Alla luce poi delle carenze messe in luce dalla pandemia, il Piano ha declinato importanti iniziative tese alla **digitalizzazione della sanità** attraverso il miglioramento, l'armonizzazione e la diffusione del **Fascicolo Sanitario Elettronico (FSE)** e lo sviluppo di ecosistemi avanzati di **telemedicina**.

Particolare attenzione è riservata ai temi della **sicurezza informatica** - che viene articolato rispetto all'intera gamma di domini, dalle forze dell'ordine alle attività operative, dall'ispezione del software all'audit delle tecnologie installate - e della "*cittadinanza digitale*", attraverso iniziative dedicate volte a migliorare le competenze digitali di base.

Per quanto concerne le risorse assegnate a missioni e componenti del PNRR, alla missione n.1, digitalizzazione, innovazione, competitività, cultura e turismo, sono state assegnati 40,32 miliardi di euro di cui 9,75 per digitalizzazione, innovazione e sicurezza nella PA, 6,68 per turismo e cultura 4.0 e 23,89 per digitalizzazione, innovazione e competitività nel sistema produttivo. In tale segmento, in particolare, si collocano le iniziative relative alle **infrastrutture** (investimento 3: Reti ultraveloci) che meritano uno specifico approfondimento in considerazione delle tematiche analizzate nella presente ricerca.

Il Piano, in particolare, partendo dagli obiettivi fissati dalla nuova strategia europea **Digital Compass** che, come già rilevato nel capitolo 1, si prefigge di garantire entro il 2030 una connettività a 1 Gbps per tutti e la piena copertura 5G delle aree popolate, fissa obiettivi ancora più ambiziosi in termini di tempistiche, prevedendo connessioni a 1 Gbps su tutto il territorio nazionale entro il 2026. Quanto all'impiego delle risorse, il Piano ha stanziato fondi per portare la connettività a 1 Gbps (**Piano "*Italia a 1 Giga*"** di cui si parlerà nei paragrafi successivi) a circa 8,5 milioni di famiglie, imprese ed enti nelle aree grigie e nere NGA a fallimento di mercato, nel rispetto del principio della neutralità tecnologica, per completare il **Piano "*Scuola connessa*"**, teso a garantire la connessione in fibra a 1 Gbps ai 9.000 edifici scolastici rimanenti (pari a circa il 20 per cento del totale), assicurare connettività da 1 Gbps fino a 10 Gbps simmetrici agli oltre 12.000 punti di erogazione del Servizio sanitario nazionale (**Piano "*Sanità connessa*"**), munire 18 isole minori di un *backhauling* sottomarino in fibra ottica (**Piano "*Collegamento isole minori*"**) e incentivare lo sviluppo e la diffusione dell'infrastruttura 5G nelle aree mobili a fallimento di mercato (**Piano "*Italia 5G*"** di cui si parlerà più approfonditamente infra).

Rispetto al modello di governance, il Governo ha istituito una struttura di coordinamento centrale presso il Ministero dell'Economia e delle Finanze, che ha il compito di supervisionare l'attuazione del Piano ed è responsabile dell'invio delle richieste di pagamento alla Commissione europea al raggiungimento degli obiettivi previsti. Accanto a questa struttura di coordinamento, agiscono strutture di valutazione e di controllo mentre alle amministrazioni è attribuita la responsabilità dei singoli investimenti e delle singole riforme e dell'invio dei rendiconti alla struttura di coordinamento centrale. In una logica di efficacia ed efficienza, è prevista la possibilità per il Governo di costituire delle *task force* locali di

sostegno alle amministrazioni territoriali per migliorare la loro capacità di investimento e a semplificare le procedure.

5.2 LE PRINCIPALI INIZIATIVE NAZIONALI PER FAVORIRE LO SVILUPPO DELLE RETI

5.2.1 Dal Decreto Semplificazioni Bis al Ddl Concorrenza

La **semplificazione normativa** rappresenta senza dubbio una delle riforme più impattanti sullo sviluppo delle infrastrutture fisse e mobili, fattori abilitanti i servizi digitali. Al fine di accelerare il *deployment* delle reti in Italia, negli ultimi due anni sono stati consistenti gli interventi tesi a snellire le procedure e ridurre gli oneri a capo degli operatori impegnati nello sviluppo delle infrastrutture fisse e mobili.

In particolare, con il **decreto Semplificazioni** (D.L. n. 76/2020, convertito in legge 11 settembre 2020, n. 120) sono state varate una serie di misure dedicate al comparto delle reti e dei servizi di comunicazioni elettroniche che hanno come obiettivo quello di appianare gli ostacoli al completo dispiegamento del **Piano strategico nazionale della banda ultra-larga** e alla piena diffusione della tecnologia 5G. A tal scopo, le misure del decreto Semplificazioni sono andate a integrare quanto già previsto del Decreto Cura Italia del 17 marzo 2020, proponendo un iter standardizzato e semplificato per ottenere l'autorizzazione a effettuare interventi di installazione e manutenzione delle reti in fibra ottica, nonché il permesso di installare infrastrutture per impianti radioelettrici (di qualunque tecnologia e potenza) sul territorio. In particolare, rispetto al *rollout* delle reti fisse, è introdotta la possibilità di effettuare la posa di infrastrutture a banda ultra larga mediante la tecnica con **micro trincea** attraverso l'esecuzione di uno scavo e contestuale riempimento di ridotte dimensioni (larghezza da 2,00 a 4,00 cm, con profondità regolabile da 10 cm fino a massimo 35 cm) in ambito urbano ed extraurbano, anche in prossimità del bordo stradale o sul marciapiede, è stata prevista per gli operatori la possibilità di presentare opportuna documentazione cartografica invece dell'autorizzazione archeologica nel caso si intervenga con scavi a basso impatto ambientale in zone del territorio in cui siano già presenti infrastrutture fisiche e sotto-servizi (es. tubature, cavidotti, ecc.), è stato ridotto a 8 giorni il termine per l'accoglimento delle istanze di occupazione del suolo pubblico nel caso di sedime ferroviario, strade ferrate, aerodromi, porti, interporti e altri beni immobili appartenenti alla PA, è consentito effettuare gli interventi di scavo, installazione e manutenzione di reti di comunicazione in fibra ottica mediante la presentazione di una SCIA all'amministrazione locale competente e agli organismi competenti ad effettuare i controlli anche in deroga a quanto disposto dal Codice delle comunicazioni elettroniche e dai regolamenti adottati dagli enti locali.

Rispetto alle **reti mobili**, invece, è introdotto un regime autorizzatorio semplificato per la posa di impianti temporanei di telefonia mobile che possono essere installati previa comunicazione di avvio lavori all'amministrazione comunale mentre in caso di realizzazione di impianti e reti 5G, il decreto ha riconosciuto ai comuni la possibilità di prevedere limitazioni soltanto su siti specifici e non su aree generalizzate del territorio senza discriminazioni in base alla specifica tecnologia di rete.

In questo contesto è intervenuto il D.L. 77/2021 (c.d. **Decreto Semplificazioni bis**), convertito con modificazioni dalla Legge 29 luglio 2021, n. 108, recante "*Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure*". Tale decreto, in particolare, al Titolo II, si occupa della "*Transizione digitale*". Si tratta di una serie di disposizioni con ambiti applicativi diversi ma che

tendono tutte a un unico obiettivo: **favorire la digitalizzazione**. Ed infatti, se l'articolo 38 contiene misure per la diffusione delle comunicazioni digitali delle pubbliche amministrazioni e divario digitale che vanno a incidere su alcuni aspetti della notifica digitale degli atti della pubblica amministrazione attraverso la Piattaforma per la notificazione digitale degli atti della pubblica amministrazione ed interventi in materia di domicilio digitale e identità digitale nella logica del superamento del divario digitale, l'articolo 39 introduce misure di semplificazione relative all'**Anagrafe nazionale della popolazione residente (ANPR)** e interventi per semplificare i meccanismi di condivisione dei dati e di interoperabilità tra le amministrazioni.

L'articolo 40, invece, rappresenta una delle previsioni certamente più rilevanti in quanto va a incidere sui procedimenti di autorizzazione per l'installazione di infrastrutture di comunicazione elettronica e, dunque, sulle reti, che costituiscono la precondizione per il positivo esito del processo di digitalizzazione. Tale disposizione, in particolare, introduce **forme di semplificazione e agevolazione per l'infrastrutturazione digitale degli edifici e delle unità immobiliari**, prevedendo:

1) la convocazione, ad opera del responsabile del procedimento, entro cinque giorni lavorativi dalla presentazione dell'istanza, di una conferenza di servizi, alla quale prendono parte tutte le amministrazioni, enti e gestori di beni o servizi pubblici interessati dall'installazione. La determinazione positiva della conferenza sostituisce ad ogni effetto tutti i provvedimenti, determinazioni, pareri, intese, concerti, nulla osta o altri atti di concessione, autorizzazione o assenso, comunque denominati, necessari per l'installazione delle infrastrutture, di competenza di tutte le amministrazioni, enti e gestori di beni o servizi pubblici interessati;
2) il silenzio-assenso una volta decorsi, senza riscontro, 90 gg. dalla presentazione del progetto e della relativa domanda;
3) in caso di dissenso espresso da parte di un'Amministrazione preposta alla tutela ambientale, paesaggistico-territoriale o dei beni culturali la possibilità, per l'interessato, di rivolgersi al responsabile del procedimento perché, entro un termine pari alla metà di quello originariamente previsto (quindi 45 giorni), concluda il procedimento attraverso le strutture competenti o con la nomina di un commissario (non è dunque più necessaria una delibera del Consiglio dei Ministri ai fini del superamento del dissenso);
4) la possibilità, fino al 31 dicembre 2026, in deroga agli artt. 5 e 7 del D. Lgs. n. 33/2016, nonché ai regolamenti adottati dagli enti locali, qualora sia tecnicamente fattibile per l'operatore, di procedere alla posa in opera di infrastrutture a banda ultra larga con la metodologia della micro trincea, attraverso l'esecuzione di uno scavo e contestuale riempimento di ridotte dimensioni, in ambito urbano ed extraurbano, anche in prossimità del bordo stradale o sul marciapiede (l'operatore di rete si limita a comunicare, con un preavviso di almeno quindici giorni, l'inizio dei lavori alla soprintendenza competente, allegando la documentazione cartografica prodotta dall'operatore medesimo relativamente al proprio tracciato e, nel caso la posa in opera interessi spazi aperti nei centri storici, un elaborato tecnico che dia conto delle modalità di risistemazione degli spazi oggetto degli interventi);
5) ulteriori semplificazioni fino al 2026 per l'installazione di apparati con tecnologia UMTS, sue evoluzioni o altre tecnologie su infrastrutture per impianti radioelettrici preesistenti o di modifica delle caratteristiche trasmissive, e nel caso di modifiche delle caratteristiche degli impianti

già provvisti di titolo abilitativo, ivi incluse le modifiche relative al profilo radioelettrico, disciplinati rispettivamente dagli articoli 87-bis e 87-ter del Codice delle comunicazioni elettroniche.

Il successivo articolo 41, invece, al fine di assicurare l'attuazione dell'**Agenda digitale italiana ed europea**, la digitalizzazione dei cittadini, delle pubbliche amministrazioni e delle imprese disciplina le ipotesi di violazione degli obblighi di transizione digitale attribuendo ad AGID poteri di vigilanza, verifica, controllo e monitoraggio sul rispetto di ogni norma in materia di innovazione tecnologica e digitalizzazione della pubblica amministrazione. A tali poteri si accompagna quello di irrogare **sanzioni amministrative pecuniarie** nel minimo di 10.000 e nel massimo di 100.000 euro nel caso di accertamento di violazioni (da cui la disposizione fa discendere una responsabilità dirigenziale e disciplinare) e di definire, con proprio regolamento, la disciplina delle procedure di contestazione, accertamento, segnalazione e irrogazione delle sanzioni. La stessa disposizione prevede la segnalazione delle violazioni accertate da parte di AGID alla struttura della Presidenza del Consiglio dei Ministri competente per l'innovazione tecnologica e la transizione digitale e la possibilità per la Presidenza stessa, in caso perdurante inottemperanza rispetto agli obblighi normativi vigenti, di esercitare i poteri sostitutivi del Presidente del Consiglio dei Ministri o del Ministro delegato con nomina di commissari *ad acta* (senza alcuna corresponsione di compensi, indennità o rimborsi).

Se sono importanti le misure di semplificazione introdotte, non sfugge l'importanza di assicurare una **concorrenza infrastrutturale adeguata**. L'Autorità Garante della Concorrenza e del Mercato, nella segnalazione inviata al Governo a marzo 2021 al fine della predisposizione del DDL annuale per il mercato e la concorrenza, ha posto l'accento proprio sulla concorrenza infrastrutturale come principale motore di sviluppo delle reti e sui benefici, in termini di qualità e velocità del servizio e prezzi, conseguenti alla pressione concorrenziale. L'azione tesa ad accelerare l'infrastrutturazione del Paese potrebbe basarsi, secondo le indicazioni fornite dall'AGCM, su alcune leve che si sostanziano nella garanzia della concorrenza infrastrutturale, nella riduzione degli oneri amministrativi ed autorizzatori, nell'allineamento agli standard europei e nello stimolo della domanda e della mobilità dei consumatori.

In particolare, rispetto all'esigenza di promuovere la concorrenza infrastrutturale, l'AGCM ha esortato, da un lato, il ricorso a politiche pubbliche di sostegno alle reti ad altissima capacità nelle aree grigie, ossia quelle a parziale fallimento di mercato, mediante ricorso alla leva fiscale o all'erogazione di incentivi economici con procedure competitive trasparenti e non discriminatorie; dall'altro, rispetto alla aree nere, ha richiesto al Governo di indirizzare la propria attività a preservare e tutelare la concorrenza infrastrutturale e la pluralità delle reti e delle tecnologi disponibili.

Rispetto invece al **tema frequenze**, l'Autorità ha posto in luce la necessità di definire un quadro di regole certe e di lungo periodo nella gestione di tali risorse scarse che sia in grado di superare le criticità connesse all'assenza di regole *ex ante* circa il rinnovo delle frequenze e la tardiva definizione dei canoni di rinnovo delle stesse. Con riguardo, invece, ai **limiti elettromagnetici**, la stessa AGCM ha invitato il Governo a verificare la validità dei limiti vigenti e degli standard di misurazione in considerazione del fatto che l'estremo rigore potrebbe costituire una barriera all'entrata e all'espansione di nuovi operatori e nuovi servizi e determinare il proliferare delle torri di trasmissione.

Lato domanda, l'AGCM invitava il Governo a ridurre (da 24 a 12 mesi) il termine entro il quale

è consentito al consumatore recedere, a rivedere i principi che governano la portabilità delle numerazioni sulle reti fisse e a modificare il **Piano Voucher**, di cui si parlerà infra, prevedendo un sistema di semplice applicazione e limitando i benefici all'utilizzo di reti in grado di raggiungere una velocità di almeno 100 Mbps con privilegio per le connessioni con tecnologia Gigabit.

5.2.2 La nuova "Strategia italiana per la banda ultralarga"

Nell'ottica di favorire la diffusione della connettività e beneficiare di tutte le opportunità di crescita a essa connesse, sin dal 2009 son state messe in campo iniziative di complessità e ambiziosità crescente. In particolare, se con il **Piano Banda Larga del 2009**, l'obiettivo fissato consisteva nel portare a tutti i cittadini una connettività di almeno 2 Mbps, allora ritenuta la soglia minima indispensabile, anche in sede europea[28], nel 2015 è stata lanciata la **Strategia per la Banda Ultralarga** che, partendo dagli obiettivi dell'Agenda digitale UE 2020 (pubblicata nel 2010) - ossia connettività ad almeno 30 Mbps[29] a tutta la popolazione ed oltre il 50% della popolazione abbonata con connessioni ad almeno 100 Mbps[30] -, ha fissato come obiettivo nazionale la **copertura di almeno l'85% della popolazione con connettività ≥100 Mbps**[31].

Si tratta di obiettivi in linea con la **Comunicazione Gigabit Society del 2016**, che ha aggiornato gli obiettivi per il 2025, prevedendo connettività in fibra con capacità fino a 1 Gbps verso i principali motori socioeconomici[32] e per le imprese ad alta intensità digitale, copertura 5G ininterrotta in tutte le aree urbane e su tutti i principali assi di trasporto terrestre[33] e accesso ad almeno 100 Mbps, potenziabile fino a 1 Gbps, per tutte le famiglie europee, anche quelle delle aree rurali.

All'interno della Strategia per la Banda Ultralarga del 2015 si colloca il **Piano Aree Bianche**, che riguarda specificamente le aree a fallimento di mercato rispetto alle quali si è puntato su un modello a concessione tramite fondi nazionali (FSC), fondi comunitari (FESR e FEASR, assegnati dalle Regioni al Ministero dello Sviluppo economico in base ad accordi Stato-Regioni) e fondi regionali per la realizzazione di una rete di proprietà pubblica aperta a tutti gli operatori tlc in modalità *wholesale*[34], affidata in concessione per 20 anni all'aggiudicatario, individuato tramite procedura di gara pubblica, chiamato a realizzare e gestire l'infrastruttura passiva.

L'attuazione del Piano Banda Ultralarga del 2015 è stata affidata a Infratel, con l'obiettivo di fornire 7.700 comuni con la connessione in fibra ottica, in aggiunta ai comuni da coprire con connessione **mista fibra-wireless (FWA)** con prestazioni fino a 100 Mbps. I comuni oggetto di intervento sono stati suddivisi in tre diverse gare, parcellizzati in lotti regionali (o relativi alle Provincie Autonome) e messi a gara con tre diversi bandi tutti aggiudicati, come noto, ad Open Fiber. Se questi sono gli obiettivi perseguiti, secondo i dati al 31

[28] Nell'Agenda Digitale Europea 2010 si affermava la necessità di "*garantire a tutti i cittadini una copertura del servizio di connettività a banda larga (almeno 2 Mbps)*".
[29] Definita "*fast broadband*" nell'Agenda Digitale Europea.
[30] Definita "*ultra fast broadband*" nell'Agenda Digitale Europea.
[31] Sebbene si sia parlato di un innalzamento rispetto alla soglia del 50% della popolazione a 100 Mbps prevista in sede europea, la strategia italiana ha stabilito questo obiettivo in base correlazione tra utenti coperti e utenti abbonati e stimando quindi che, per raggiungere l'obiettivo di almeno il 50% delle famiglie abbonate a 100 Mbps, sarebbe stato necessario coprirne almeno l'85%. Cfr Strategia BUL 2015.
[32] Scuole, università, stazioni ferroviarie, porti, aeroporti, ospedali ambulatori, centri di ricerca e edifici di enti pubblici locali.
[33] Strade nazionali, autostrade e ferrovie.
[34] Gli altri operatori tlc acquistano connettività in modalità *wholesale* dal concessionario, a prezzi definiti da Agcom, e rivendono il servizio al dettaglio ai clienti finali, ovvero cittadini, imprese e pubblica amministrazione.

agosto 2021 pubblicati da Infratel, punto di vista progettuale risultavano più di 8300 progetti approvati su oltre 9500 previsti in FTTH e oltre 7.760 approvati su 7121 previsti in FWA. A livello realizzativo, per le infrastrutturazioni in fibra sono stati emessi quasi 5.000 ordini di esecuzione, di cui oltre 3.000 risultano chiusi, ovvero con **CUIR (Comunicazione Ultimazione Impianto di Rete)**, a fronte di oltre 2000 interventi "*completati*". Per cantieri FWA risultano quasi 2.200 ordini emessi, di cui oltre 1.900 con CUIR. L'avanzamento economico del progetto a livello nazionale ha raggiunto attualmente circa il 70% in termini di avanzamento dei lavori con 1.090 milioni di euro impiegati su oltre 1,5 miliardi di euro di lavori ordinati a Open Fiber.

Se il Piano Aree Bianche si occupa dell'offerta, il **Piano Voucher**, divenuto operativo a novembre 2020, consiste in una misura finalizzata ad incentivare la fruizione di servizi a banda ultralarga su tutto il territorio nazionale. Al 9 settembre 2021, gli operatori accreditati erano 169 (su 225 che avevano presentato domanda)[35].

Gli operatori accreditati devono presentare le offerte commerciali relative ai servizi di connettività nell'ambito del Piano Voucher Fase I, corredate dalla propria carta dei servizi. Alla data sopraindicata sono state approvate 804 offerte di 107 diversi operatori (su un totale di 1.364 offerte provenienti da 113 diversi operatori)[36]. Quanto alle risorse impegnate, al 24 settembre 2021, esse ammontavano a oltre 96,8 milioni di euro, pari al 48,43% dei fondi disponibili. Complessivamente, dal 9 novembre 2020, giorno a partire dal quale i cittadini interessati potevano richiedere il Voucher agli operatori che hanno presentato offerte valide, sono stati attivati oltre 173.500 Voucher in tutta Italia, per un totale di oltre 86,7 milioni di euro erogati. Risultavano inoltre prenotati voucher per un importo pari a oltre **7,8 milioni di euro**.

Da ultimo, in seguito all'approvazione del Piano di Ripresa e Resilienza, lo scorso 27 maggio è stata pubblicata la **nuova strategia italiana per la banda ultralarga** che, partendo da quanto già previsto con le precedenti, arricchisce il set di iniziative aventi a oggetto le infrastrutture digitali. La nuova strategia, in particolare, si compone di 7 azioni, di cui due già in atto, ovvero il **Piano Aree Bianche** (infrastrutturazione aree a fallimento di mercato) e il **Piano Voucher** (incentivi alla domanda), cui si aggiungono: 1) il Piano "*Italia a 1 Giga*", 2) il Piano "*Italia 5G*", 3) il Piano "*Scuole connesse*", 4) il Piano "*Sanità connessa*" e 5) il Piano "*Isole Minori*".

Per quanto attiene le risorse destinate alla nuova strategia, i fondi ammontano a 6,7 miliardi di euro di cui 3,8 circa destinati alla copertura in banda ad altissima capacità delle aree nere e grigie[37].

Il Piano "Italia a 1 Giga"

Nell'ambito della nuova strategia, il **Piano "*Italia a 1 Giga*"**, sottoposto a consultazione pubblica dal 6 agosto al 15 settembre 2021 unitamente alla "*Relazione della mappatura reti fisse 2021*" redatta da Infratel, si prefigge l'ambizioso obiettivo di fornire connettività ad almeno 1 Gbit/s in download e 200 Mbit/s in upload alle unità immobiliari (8,5 milioni) che, a seguito della

[35] La procedura di accreditamento degli operatori verifica che ciascuno di essi sia in possesso dei titoli necessari e non versi in nessuna delle situazioni di cui all'art. 80 del d.lgs. n. 50/2016.

[36] Le altre 560 offerte sono state rifiutate per via di clausole contrattuali difformi da quanto indicato in convenzione (es. rinnovo tacito alla scadenza del contratto), livelli di servizio non sufficienti (es. banda upload), dispositivi Tablet/PC non in linea con le specifiche tecniche minime richieste, difformità tra i documenti presentati e i dati caricati sul Portale Voucher.

[37] Il Piano Italia a 1 Giga indica inoltre che una quota dell'ammontare complessivo stanziato per il Piano è destinata a fornire connettività a circa 450.000 unità immobiliari presenti nelle aree già interessate dal precedente Piano "*Aree bianche*", ma rimaste fuori dall'intervento pubblico affidato alla società concessionaria Open Fiber S.p.A. Tali interventi saranno attuati nell'ambito di una fase distinta dello stesso Piano.

mappatura delle infrastrutture presenti o pianificate al 2026 dagli operatori di mercato, sono risultate non coperte da almeno una rete in grado di fornire in maniera affidabile velocità di connessione in download ≥ 300 Mbps.

La soglia minima di intervento, dunque, è stata fissata a 300 Mbps (in download) - con un innalzamento rispetto ai 100 Mbps previsti inizialmente dalla Strategia formulata a maggio - ed è stata ritenuta necessaria e sufficiente per raggiungere, entro il 2026, l'obiettivo di connettività ad almeno 1 Gbps definito nel Digital Compass.

Se questi sono gli obiettivi e le soglie, secondo i dati Infratel, i civici – rispetto al totale di civici neri e grigi oggetto della consultazione – che non verrebbero coperti a 300 Mbps con le normali dinamiche di mercato, di qui al 2026, sono oltre 6 milioni, quasi il 30% di quelli monitorati. A livello regionale, quelle con il maggior *digital divide* senza intervento pubblico risulterebbero, in termini percentuali, la Sardegna (62% dei civici), l'Abruzzo (53%), la Calabria (49%) e la Valle d'Aosta (46%). In valori assoluti, invece, i maggiori interventi dovrebbero riguardare la stessa Calabria (oltre 800.000 civici), la Puglia (620.000), la Sardegna (619.000) e la Toscana (517.000).

Stante il principio della neutralità tecnologica, è interessante quanto previsto dal Piano di rispetto al ***Fixed Wireless Access***, la tecnologia che, utilizzando un sistema ibrido di collegamenti via cavo e senza fili per offrire servizi di connettività in banda larga e ultralarga, rappresenta un'alternativa di qualità, più economica e flessibile rispetto a quella tradizionale in particolare per le zone montane, rurali e a bassa densità abitativa, dove sarebbe anti-economico costruire una rete cablata in grado di arrivare fino in casa dell'utente. Ebbene, rispetto all'FWA, partendo dall'assunto che i civici "*coperti*" in FWA non siano direttamente equiparabili a quelli raggiunti in modalità via cavo (in particolare tramite fibra ottica), a causa di fattori quali la dispersione (dovuta anche a fenomeni atmosferici) e la ripartizione della capacità della cella tra gli utenti effettivamente connessi, il Piano distingue utenti raggiunti, ovvero "*passed*" e utenti effettivamente serviti o "*served*" e ritiene ragionevole, in attesa di compiere comunque ulteriori approfondimenti, applicare il **criterio del 10%**, che consiste nel considerare effettivamente serviti con tutta la banda richiesta circa il 10% degli utenti coperti dalle celle elettromagnetiche (o "*passed*").

Dalla consultazione condotta da Infratel è emerso che, **nel 2026, i civici coperti in modalità FWA con capacità ≥300 Mbps arriverebbero a quota 560.000**.

Rispetto al modello di intervento, la proposta contenuta nel Piano punta a un modello "*ad incentivo*" (o *gap funding*) in cui le risorse previste dal PNRR per il medesimo Piano Italia 1 Giga vengono assegnate a seguito di bandi per le aree risultate a fallimento di mercato (ai quali gli operatori possono presentarsi sia in forma individuale che associata), in forma di contributo pubblico determinato come percentuale massima sul costo complessivo delle opere che - in discontinuità rispetto a quanto previsto per le aree bianche – sono e restano di proprietà dell'operatore privato.

Tali risorse vengono sbloccate solo a seguito del raggiungimento da parte dell'operatore di una **soglia base di copertura**. Il Piano specifica infine che i soggetti aggiudicatari dovranno offrire accesso *wholesale* – a condizioni e ai criteri definiti dall'Agcom – garantendo l'accesso a tutti i soggetti interessati anche mediante una completa ed effettiva disaggregazione.

Quanto alle tempistiche, la pubblicazione dei bandi è prevista tra la fine del 2021 e l'inizio del 2022 con aggiudicazione delle gare entro la metà del 2022.

Il Piano "Italia 5G"

Se il Piano Italia a 1 Giga raccoglie l'eredità delle precedenti strategie fissando obiettivi più ambiziosi e promuovendo iniziative tese a completare il processo di infrastrutturazione con riguardo alle reti fisse (con l'ausilio dell'FWA), il **Piano "*Italia 5G*"** dà avvio a un'iniziativa che non ha precedenti nel nostro Paese: realizzare una mappatura particolareggiata della copertura del territorio nazionale con reti mobili in tecnologia 4G e 5G propedeutica alla pianificazione di interventi pubblici.

Le risorse assegnate, 2 miliardi di euro, sono relative a tre voci principali: 1) la copertura di 10.000 chilometri di strade extraurbane per la realizzazione del *backhauling* in fibra (600 milioni di euro); 2) i corridoi di trasporto europei (420 milioni di euro), con l'obiettivo di incentivare lo sviluppo di servizi e applicazioni 5G dedicate a sicurezza stradale, mobilità, logistica e turismo; 3) il potenziamento della rete mobile nelle aree a fallimento di mercato, ovvero quelle zone del Paese in cui gli operatori non hanno interesse a investire (1 miliardo).

La realizzazione della mappatura, alla data del 31 maggio 2021, i cui esiti sono in attesa di pubblicazione, è stata affidata a Infratel, che ha indetto una consultazione pubblica a partire dal 10 giugno 2021 (con scadenza 26 luglio), nell'ambito della quale gli operatori sono stati chiamati a presentare i propri piani per i prossimi 5 anni. Nello specifico, gli operatori sono stati invitati a fornire la seguente documentazione:

> a) "*piano dettagliato degli investimenti, che includa per ogni fase di attuazione le date di inizio e completamento e gli elementi che ne evidenzino la concreta attuabilità, suddiviso negli anni per macrocategorie e relativi finanziamenti, approvati dagli organi competenti*";
> b) "*architettura e struttura della rete sul territorio (numero siti, dislocazione territoriale, tipologia link di backhaul, apparati di trasporto, POP e relativo posizionamento), apparati e tecnologie previste*";
> c) "*dimensionamento dei siti radio (con evidenza dei metodi e parametri utilizzati per le simulazioni radioelettriche) in termini di numero medio di utenti per sito e per antenna, coerente con quanto fornito nei questionari compilati e dimensionamento della banda, della rete dati e di trasporto*".

I piani dichiarati dagli operatori dovranno essere chiaramente riferibili a decisioni strategiche ed esecutive, adottate dai competenti organi di indirizzo e gestione degli operatori ed indicare anche le coperture di rete attuali.

Una volta ricevuti gli esiti della consultazione, sarà dunque possibile individuare le "*aree bianche*" di intervento sulle quali designare e pubblicare i bandi, operazioni che dovrebbero realizzarsi tra la fine di quest'anno e l'inizio del prossimo. **Entro il 2022**, secondo il cronoprogramma, tutte le gare del Piano Italia 5G dovrebbero essere state assegnate, potendo così dare avvio alla fase realizzativa che dovrebbe tradursi nel completamento del 20% dei lavori entro il terzo trimestre 2023 (con completamento delle opere entro la prima metà del 2026).

5.3 DAL PERIMETRO DI SICUREZZA CIBERNETICA ALLA NASCITA DELL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE. L'ECOSISTEMA ITALIANO DELLA CYBERSECURITY

Con il decreto legge n. 105/2019, convertito con la legge n. 133/2019, è stato istituito il **perimetro di sicurezza nazionale cibernetica** al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori (pubblici e privati aventi una sede nel

territorio nazionale), da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Paese e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

Per raggiungere tale obiettivo, la disciplina istitutiva del perimetro ha tracciato un percorso attuativo frazionato con **scadenze temporali diversificate**, che si snoda attraverso cinque decreti del Presidente del Consiglio dei Ministri e un regolamento governativo di esecuzione. In particolare, la norma primaria sul perimetro di sicurezza nazionale cibernetica prevede l'adozione di:

1) un DPCM che definisca le modalità e i criteri procedurali di individuazione dei soggetti (amministrazioni pubbliche, enti e operatori pubblici e privati) inclusi nel perimetro di sicurezza nazionale cibernetica e che, pertanto, saranno tenuti al rispetto delle misure e degli obblighi previsti dal decreto legge e declini i criteri con i quali i soggetti inclusi nel perimetro predispongono e aggiornano l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica;
2) un DPCM di natura provvedimentale di definizione dell'elenco dei soggetti individuati;
3) un DPCM che disciplini i termini e le modalità attuative delle procedure secondo cui i soggetti rientranti nel perimetro notificano al Gruppo di intervento per la sicurezza informatica (CSIRT) gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici e stabilisca le misure di sicurezza da adottare;
4) un regolamento governativo per la disciplina delle procedure, delle modalità e dei termini con cui i soggetti danno comunicazione al CVCN delle procedure per l'affidamento di forniture di beni, sistemi e servizi ICT e i soggetti individuati quali fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici assicurano la propria collaborazione per l'effettuazione delle attività di test di sicurezza;
5) un DPCM per l'individuazione, sulla base di criteri di natura tecnica, delle categorie di forniture di beni, sistemi e servizi ICT destinati ad essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici assoggettati all'obbligo di comunicazione;
6) un DPCM per la definizione dei criteri per l'accreditamento, da parte del CVCN, dei laboratori di cui lo stesso CVCN può avvalersi per lo svolgimento dei suoi compiti di verifica, in attesa di pubblicazione sulla G.U.

Nonostante il ritardo rispetto alla tabella di marcia che ne prevedeva l'adozione entro 4 mesi dall'entrata in vigore della legge di conversione del decreto istitutivo del perimetro, complice, certamente, anche l'emergenza sanitaria ancora in atto, il 20 ottobre 2020 è stato pubblicato sulla G.U. il **DPCM 30 luglio 2020, n. 131** che ha formalmente dato avvio all'articolata e complessa procedura di attuazione della disciplina del perimetro di sicurezza cibernetica. Tale decreto, in particolare, ha definito le modalità e i criteri procedurali di individuazione dei soggetti (amministrazioni pubbliche, enti e operatori pubblici e privati) inclusi nel perimetro di sicurezza nazionale cibernetica e che, pertanto, saranno tenuti al rispetto delle misure e degli obblighi previsti dal decreto legge e, dall'altro, ha declinato i criteri con i quali i soggetti inclusi nel perimetro predispongono e aggiornano l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica. Nello specifico, tale decreto ha fornito una

definizione di funzione e servizio essenziale, ha individuato i **settori di attività interessati** (interno, difesa, spazio e aerospazio, energia, telecomunicazioni, economia e finanza, trasporti, servizi digitali, tecnologie critiche, enti previdenziali/lavoro), ha fissato le modalità e i criteri di individuazione dei **soggetti inclusi nel perimetro di sicurezza cibernetica**, ha prescritto alle amministrazioni l'individuazione delle funzioni o servizi essenziali per i quali "*il pregiudizio per la sicurezza nazionale è ritenuto massimo e le possibilità di mitigazione minime*" e la predisposizione di un elenco di tali soggetti, ha istituito un Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica con funzioni di supporto del CISR, ha dettato i criteri per la predisposizione e l'aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici ed ha fissato in sei mesi dal ricevimento della comunicazione di avvenuta iscrizione nell'elenco il termine per procedere alla trasmissione degli elenchi appena descritti alla Presidenza del Consiglio o al Ministero dello sviluppo economico.

In attuazione di quanto previsto dal DPCM appena descritto, il 25 novembre scorso è stato adottato il DPCM provvedimentale con il quale è stata definita la lista segreta degli oltre 100 soggetti pubblici e privati inclusi nel perimetro.

È giunto invece a pubblicazione sulla G.U. del 23 aprile 2021, il **DPR n. 54 del 5 febbraio 2021** contenente il regolamento disciplinante le procedure e i termini per le valutazioni da parte del CVCN e dei CV su prodotti in acquisizione da parte dei soggetti inclusi nel perimetro. Tale decreto, infatti, in attuazione dell'art. 1 c. 6 del decreto istitutivo del perimetro, definisce le procedure, le modalità e i termini da seguire ai fini delle valutazioni da parte dello stesso CVCN e dei centri di valutazione del Ministero dell'Interno e del Ministero della Difesa (CV), ciascuno nell'ambito delle rispettive competenze, in ordine all'acquisizione, da parte dei soggetti inclusi nel perimetro, di oggetti di fornitura rientranti nelle categorie individuate sulla base dei criteri dallo stesso indicati, i criteri di natura tecnica per l'individuazione delle categorie a cui si applica la procedura di valutazione delineata, le procedure, le modalità ed i termini con cui le Autorità competenti effettuano le attività di verifica e ispezione ai fini dell'accertamento del rispetto degli obblighi stabiliti nel decreto legge e nei decreti attuativi. Il decreto si compone di 4 Capi che definiscono con puntualità le tipologie di beni, sistemi e servizi ICT oggetto della valutazione da parte del CVCN, le modalità e i contenuti delle comunicazioni da effettuare in favore di CVCN o CV da parte dei soggetti inclusi nel perimetro, le tipologie di valutazioni, test e verifiche realizzabili, nonché le attività di verifica e ispezione cui possono essere sottoposti i soggetti inclusi nel perimetro. Lo stesso decreto descrive con minuziosità il procedimento di verifica e valutazione dell'analisi documentale contenuta nella comunicazione, detta i criteri da seguire per l'individuazione di condizioni e test (e gli obblighi gravanti sul fornitore in tali ipotesi), individua le singole fasi ed i relativi termini ricollegando all'inutile decorso dei termini fissati il silenzio-assenso, con conseguente possibilità per i soggetti di proseguire nella procedura di affidamento e nell'esecuzione del contratto.

L'11 giugno 2021 è stato poi pubblicato sulla G.U. il **DPCM 14 aprile 2021, n. 81**, recante regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici adottato ai sensi dell'art. 1 comma 2, lett. b) del D.L. n. 105/2019. Si tratta di un decreto che si compone di 11 articoli suddivisi in quattro Capi che classificano gli incidenti aventi impatto sui beni ICT a seconda della gravità degli incidenti anche tenuto conto della tempistica necessaria per una risposta efficace, ricollega al verificarsi di uno degli incidenti avente impatto su un bene ICT l'obbligo di notifica al CSIRT italiano, prescrive tempistiche specifiche - un'ora o sei ore - per la relativa denuncia in funzione della gravità

dell'incidente, disciplina la notifica volontaria degli incidenti non rientranti tra quelli indicati nell'Allegato A, individua le misure minime di sicurezza di natura tecnica e organizzativa che sono volte a tutelare le informazioni relative all'elenco dei soggetti inclusi nel perimetro, all'elenco dei beni ICT e agli elementi delle notifiche di incidente e ne definisce le modalità ed i termini di adozione.

Sulla G.U del 19 agosto 2021 è stato infine pubblicato il **DPCM del 15 giugno 2021** con il quale sono state individuate le categorie in relazione alle quali i soggetti inclusi nel perimetro che intendano procedere, anche per il tramite delle centrali di committenza alle quali sono tenuti a fare ricorso, all'affidamento di forniture di beni, sistemi e servizi ICT (*information and communication technology*), destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui all'art. 1, comma 2, lettera b), del decreto-legge, effettuano la comunicazione al CVCN o ai CV. In particolare, l'Allegato 1 individua quattro categorie (e all'interno di ciascuna categoria singoli beni, sistemi e servizi) ed in particolare:

a) componenti hardware e software che svolgono funzionalità e servizi di rete di telecomunicazione (accesso, trasporto, commutazione);
b) componenti hardware e software che svolgono funzionalità per la sicurezza di reti di telecomunicazione e dei dati da esse trattati;
c) componenti hardware e software per acquisizione dati, monitoraggio, supervisione controllo, attuazione e automazione di reti di telecomunicazione e sistemi industriali e infrastrutturali;
d) applicativi software per l'implementazione di meccanismi di sicurezza.

Manca ancora all'appello, ma è atteso a breve in Gazzetta, l'ultimo DPCM che fisserà le regole di accreditamento per la costituzione della rete nazionale di laboratori pubblico-privati a supporto del CVCN per la conduzione di attività di *testing* e scrutinio tecnologico su beni, servizi e sistemi ICT ricompresi al perimetro.

5.3.1 Il ruolo dell'Agenzia per la cybersicurezza ed il nuovo assetto delle competenze in materia

Mentre prende forma il quadro normativo sul perimetro di sicurezza nazionale cibernetica, con la legge n. 109 del 4 agosto 2021 è stato convertito il D.L. n. 82/2021 recante "*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'**Agenzia per la cybersicurezza nazionale***". Si tratta di un intervento straordinariamente rilevante che, partendo dalla constatazione della centralità assunta dal canale digitale, della crescente e sempre più sofisticata minaccia di attacchi informatici e della estrema complessità del quadro normativo e regolamentare, frutto di una serie di interventi che si sono andati a susseguire - in maniera a volte anche poco organica - negli anni disseminando tra diverse autorità competenze in materia di cybersecurity, persegue una chiara e condivisibile finalità di riordino della materia, attraverso la concentrazione presso un unico soggetto, la neoistituita Agenzia, di tutte le competenze in materia.

Ferma restando l'attribuzione in via esclusiva al Presidente del Consiglio dell'alta direzione e della responsabilità generale delle politiche di cybersicurezza, l'adozione della strategia nazionale di cybersicurezza e la nomina e la revoca, previa deliberazione del Consiglio dei Ministri e con successiva comunicazione al COPASIR (secondo le modifiche introdotte in sede di conversione) del direttore generale e del vice direttore generale dell'Agenzia, il decreto, ormai legge, pone **l'Agenzia al centro del nuovo assetto in materia di cybersicurezza**. Ed infatti, la nuova

Agenzia per la cybersicurezza nazionale, che opererà sotto la responsabilità del Presidente del Consiglio dei ministri e dell'Autorità delegata per la sicurezza della Repubblica e in stretto raccordo con il Sistema di informazione per la sicurezza della Repubblica, sarà l'Autorità nazionale in materia di cybersecurity, predisporrà la strategia nazionale di cybersicurezza, assicurerà, nel rispetto delle competenze attribuite dalla normativa vigente ad altre amministrazioni, il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale, promuoverà la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, opererà come Autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi per le finalità di cui al decreto legislativo NIS e come Autorità nazionale di certificazione della cybersicurezza, accrediterà le strutture specializzate del Ministero della Difesa e di quello dell'Interno quali organismi di valutazione della conformità per i sistemi di rispettiva competenza, assumerà tutte le funzioni in materia di cybersicurezza già attribuite dalle disposizioni vigenti al Ministero dello Sviluppo economico, ivi comprese quelle relative al perimetro di sicurezza nazionale cibernetica, di cui al decreto legge perimetro e ai relativi provvedimenti attuativi, incluse le funzioni attribuite al Centro di valutazione e certificazione nazionale (comprese le attività di ispezione e verifica e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative), acquisirà le competenze attribuite al DIS dal decreto legge perimetro e dai relativi provvedimenti attuativi, quelle relative alla sicurezza e all'integrità delle comunicazioni elettroniche di cui al D.Lgs. n. 259/03 e svolgerà tutte le funzioni attribuite alla Presidenza del Consiglio dei Ministri in materia di perimetro di sicurezza nazionale cibernetica, nonché tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale dalle disposizioni vigenti. A tali funzioni e competenze, in sede di conversione del decreto ne sono state aggiunte ulteriori e, in particolare, l'assunzione di iniziative idonee a valorizzare la **crittografia** come strumento di cybersicurezza (anche attraverso un'apposita sezione dedicata nell'ambito della strategia di cui sopra), l'adozione di ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica dell'Italia, valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali, la qualificazione dei servizi cloud per la pubblica amministrazione, la promozione, nell'ambito delle funzioni di raccordo con le altre amministrazioni competenti in materia di cybersicurezza, di aree dedicate allo sviluppo dell'innovazione finalizzate a favorire la formazione e il reclutamento di personale nei settori avanzati dello sviluppo della cybersicurezza, nonché di studi di fattibilità e analisi valutative finalizzati a tale scopo. Rispetto al tema **formazione** e al compito dell'Agenzia di promuovere la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della cybersicurezza, invece, la legge ha riconosciuto la possibilità per l'Agenzia stessa di avvalersi anche delle strutture formative e delle capacità della Presidenza del Consiglio dei Ministri, del Ministero della Difesa e del Ministero dell'Interno, secondo termini e modalità da definire con apposito decreto del Presidente del Consiglio dei Ministri, di concerto con i Ministri interessati nonché di predisporre attività di formazione specifica riservate ai giovani che aderiscono al servizio civile regolate sulla base di apposite convenzioni.

Si segnala, inoltre, l'istituzione, disposta sempre in sede di conversione, di un **Comitato tecnico-scientifico**, presieduto dal direttore generale della medesima Agenzia, o da un dirigente da lui delegato, e composto da personale della stessa Agenzia e da qualificati rappresentanti dell'industria, degli enti di ricerca,

dell'accademia e delle associazioni del settore della sicurezza, designati con decreto del Presidente del Consiglio dei Ministri (per la cui partecipazione è espressamente esclusa la corresponsione di gettoni di presenza, compensi o rimborsi di spese), la cui composizione e organizzazione è rimessa al regolamento di cui si dirà infra.

La legge attribuisce all'Agenzia personalità giuridica di diritto pubblico e le riconosce autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria. La stessa legge fissa poi alcuni elementi organizzativi dell'Agenzia, disponendo che l'organizzazione e il funzionamento della medesima siano definiti da un apposito regolamento (da adottare, con DPCM, entro 120 gg. dall'entrata in vigore della legge di conversione del decreto stesso previo parere delle Commissioni parlamentari competenti) che ne preveda, in particolare, l'articolazione fino a un numero massimo di otto uffici di livello dirigenziale generale, nonché fino a un numero massimo di trenta articolazioni di livello dirigenziale non generale nell'ambito delle risorse disponibili e fissando in 4 anni (rinnovabili per altri 4 anni una sola volta) la durata degli incarichi del direttore generale e del vice direttore generale. La disciplina in esame dispone, inoltre, che con DPCM (su proposta del direttore generale) da adottarsi entro 120 giorni dall'entrata in vigore della legge di conversione dello stesso, sia previsto il regolamento sulle procedure per la stipula di contratti di appalti di lavori e forniture di beni e servizi per le attività dell'Agenzia mentre con ulteriore regolamento, da adottare sempre nello stesso termine, previo parere delle Commissioni parlamentari competenti, sia dettata la disciplina del contingente di personale addetto all'Agenzia che in sede di prima applicazione viene individuato in 300 unità (fatta salva la possibilità con decreti del Presidente del Consiglio dei Ministri di concerto con il Ministro dell'Economia e delle Finanze, di rideterminare la dotazione organica nei limiti delle risorse finanziarie destinate alle spese per il personale).

Se l'Acn sarà dunque la principale autorità preposta a livello nazionale e internazionale alla salvaguardia della cybersicurezza, la nuova disciplina, nel ripensare il quadro delle competenze in materia, all'articolo 4 istituisce il **Comitato interministeriale per la cybersicurezza (CIC)**, attivo presso la Presidenza del Consiglio con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico.

Presso l'Agenzia è poi costituito il **Nucleo per la cybersicurezza**, a supporto del Presidente del Consiglio, per gli aspetti relativi alla prevenzione e preparazione a eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento, presieduto dal direttore della stessa Acn e composto dal consigliere militare del premier, da un rappresentante, rispettivamente del Dis, dell'Aise, dell'Aisi e di ciascuno dei ministeri rappresentati nel comitato interministeriale per la sicurezza della repubblica (Cisr), oltre che da un rappresentante del Ministero dell'Università, il Ministro delegato per l'Innovazione tecnologica e la Transizione digitale e un rappresentante del dipartimento della protezione civile di Palazzo Chigi - che, nelle situazioni di crisi, assicura supporto al premier e al CISR. Il Nucleo, in particolare, può formulare proposte di iniziative in materia di cybersicurezza del Paese, anche nel quadro del contesto internazionale in materia, promuove la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte delle amministrazioni e degli operatori privati interessati e l'elaborazione delle necessarie procedure di coordinamento interministeriale, in raccordo con le pianificazioni di difesa civile e di protezione civile, promuove e coordina lo svolgimento di esercitazioni interministeriali, ovvero la partecipazione nazionale in esercitazioni internazionali che

riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese, valuta e promuove, in raccordo con le amministrazioni competenti per specifici profili della cybersicurezza, procedure di condivisione delle informazioni, anche con gli operatori privati interessati, ai fini della diffusione di allarmi relativi a eventi cibernetici e per la gestione delle crisi, riceve, per il tramite del CSIRT Italia, le comunicazioni circa i casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità significativi ai fini del corretto funzionamento delle reti e dei servizi e valuta se gli eventi assumono dimensioni, intensità o natura tali da non poter essere fronteggiati dalle singole amministrazioni competenti in via ordinaria, ma richiedono l'assunzione di decisioni coordinate in sede interministeriale.

CAPITOLO 6

LE INFRASTRUTTURE DIGITALI ITALIANE

6.1 LO STATO E LE PROSPETTIVE DELLE RETI FISSE

6.1.1 Il roll-out della banda ultralarga in Italia al 2026

Il Piano Nazionale di Ripresa e Resilienza, oltre a rappresentare un volano fondamentale per la ripresa dell'economia italiana, ha formalizzato il percorso che il Paese intende seguire sulla strada verso la **sostenibilità ambientale e la digitalizzazione**. A maggio 2021 è stato seguito dalla nuova **Strategia italiana per la banda ultralarga** che, sulla scia della nuova strategia europea Digital Compass, pone tra i principali obiettivi l'ambizioso raggiungimento, entro il 2026, della copertura dell'intero territorio nazionale con connettività fino a 1Gbit/s. In particolare, tra le risorse stanziate nell'ambito del PNRR, 6,7 miliardi di euro sono riservati a 7 progetti che costituiscono la presente Strategia per la banda ultralarga, in continuità con la Strategia varata nel 2015 e con le iniziative precedenti volte ad incentivare domanda e offerta di servizi di connettività.

Il precedente **Piano Banda Ultra Larga**, approvato nel 2015, conteneva le politiche di intervento previste a livello nazionale in termini di copertura delle regioni e delle province italiane. L'attuazione di queste misure è in capo ad Infratel Italia S.p.A., società in-house del Ministero dello Sviluppo economico, il cui compito principale consiste nella riduzione del ***digital divide*** nelle aree a fallimento di mercato, cosiddette "*aree bianche*", attraverso procedure finalizzate a promuovere la realizzazione e l'integrazione di infrastrutture in grado di fornire servizi di connettività Internet a banda larga ai cittadini non ancora raggiunti da tali servizi (cfr. paragrafo 6.1.2).

Al fine di impiegare al meglio le risorse stanziate, il Governo ha assegnato a Infratel il compito di effettuare una nuova consultazione sullo stato delle reti fisse e sulle intenzioni di investimento degli operatori da qui al 2026, ovvero il lasso di tempo su cui insiste il PNRR. I risultati di tale consultazione sono già stati pubblicati per quanto concerne la copertura che si verificherebbe al 2026 senza i nuovi stanziamenti, mentre il livello attuale di copertura non è ancora stato reso noto. In assenza di tali dati, un'indicazione di massima può essere estrapolata da quelli contenuti nella *broadband map* dell'AGCOM, che mostra lo stato di copertura delle famiglie italiane[29] distinti per tecnologia: **FTTP (*Fiber to the Premises*)**, equivalente del FTTH (*Fiber to the Home*); **FTTC (*Fiber to the Cabinet*)** e **DSL**.

Sulla base dei dati AGCOM, **la copertura in fibra con reti FTTP raggiunge il 34% delle famiglie** (Fig. 6.1): la copertura maggiore si ha nel **Lazio** (50%), la più bassa in Calabria (10%), dove però è presente una estesa copertura della rete FTTC, che copre un ulteriore 89% delle famiglie della regione. Dove ancora si fa molto affidamento sulla tecnologia ADSL è in Valle d'Aosta – poco più della metà delle famiglie possono contare sulla fibra (FTTC o FTTP) – e in Trentino Alto Adige e Molise, dove circa un quarto delle famiglie gode solo di una copertura in ADSL.

I dati su base provinciale restituiscono una fotografia in cui ancora diverse province – specie di Calabria, Campania, Sardegna, ma anche del Lazio e del Nord Italia – presentano una copertura di rete ad almeno 100 Mbps inferiore al 40% (Fig. 6.2), con minimi nelle province di Ogliastra (3%) e Isernia (13%). Superiore al 60% la copertura in diverse province di Emilia-Romagna, Lombardia, Piemonte e Liguria, per il Nord, Puglia, Campania e, soprattutto, Sicilia, per il Sud. Sopra l'80% solo Siracusa, Taranto, Trieste, BAT, Roma e Palermo. La copertura in FTTP, come la mappa mostra

[29] L'indicatore utilizzato dalla mappatura ufficiale condotta da Infratel è costituito dai n. civici. Il dato relativo al numero di famiglie non tiene conto delle seconde case, delle aziende, delle sedi della PA, etc.

Figura 6.1 Copertura regionale per tecnologia (% famiglie coperte, dicembre 2020)

Fonte: AGCOM

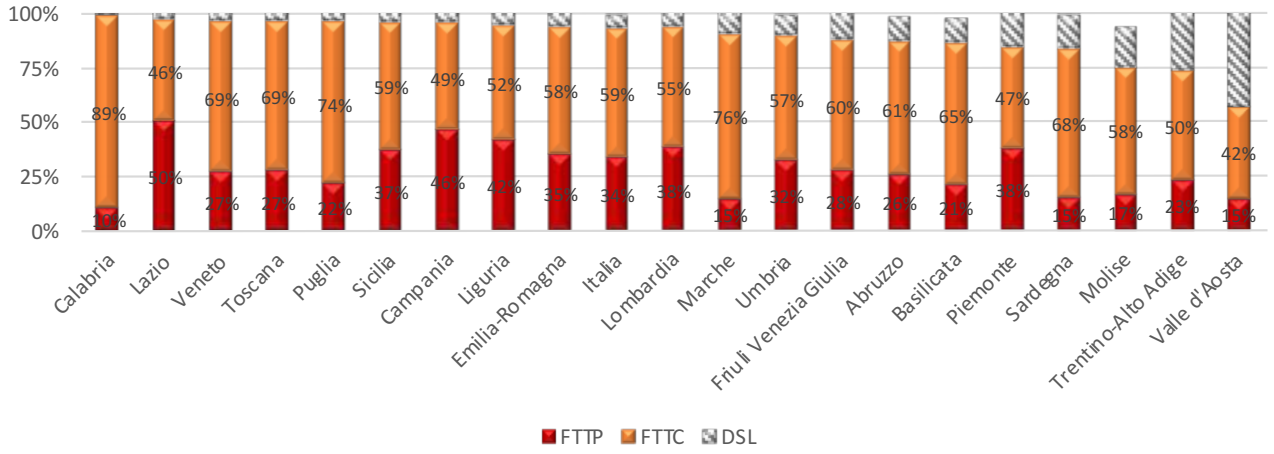
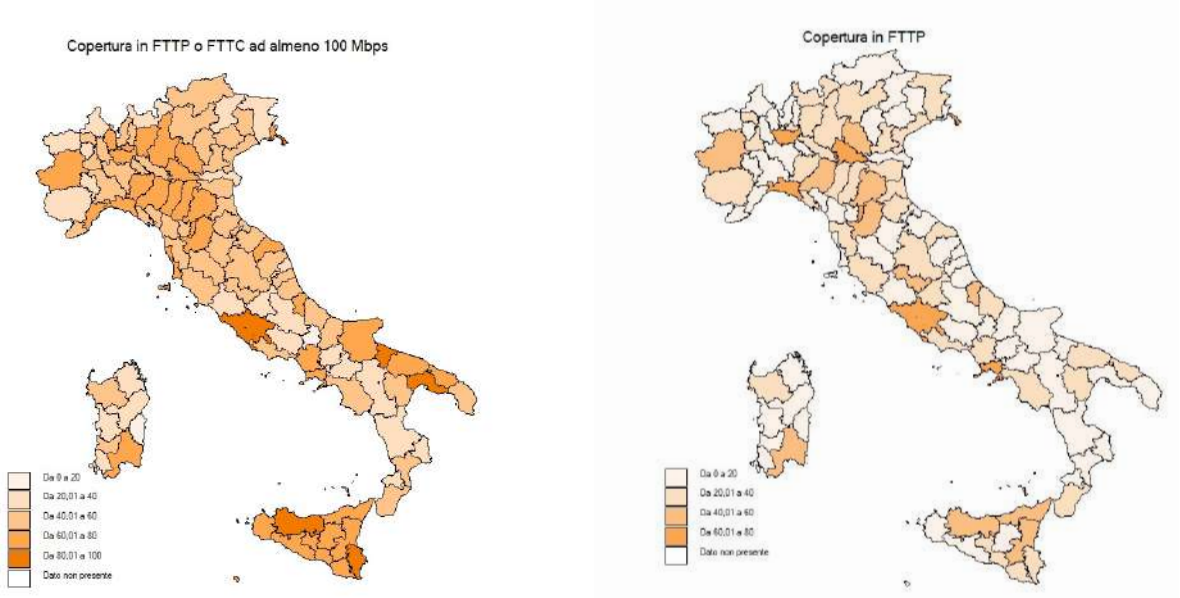


Figura 6.2 Copertura provinciale (% famiglie coperte, dicembre 2020)

Fonte: AGCOM



chiaramente, è ancora appannaggio di pochi, in particolare delle famiglie di Mantova – o, almeno, il 77% di esse – di Trieste (76%), Prato (71%), Genova (69%), Milano (65%), Roma (63%) e Napoli (61%).

Per aumentare decisamente il tasso di copertura in banda ultralarga sul territorio, la Strategia italiana per la Banda Ultralarga ha definito le azioni necessarie al raggiungimento degli obiettivi di trasformazione digitale indicati dalla Commissione europea nel 2016 e nel 2021, tra cui la **realizzazione di infrastrutture digitali sicure e sostenibili**, per far sì che, entro il 2030, tutte le famiglie dell'Unione possano beneficiare di una connettività Gigabit.

Tra le 7 azioni previste, il **Piano "*Italia a 1 Giga*"** è quella dedicata a fornire connettività a 1 Gbps in download e 200 Mbps in upload nelle aree grigie

e nere NGA, in particolare alle unità immobiliari che, a seguito della mappatura delle infrastrutture presenti o pianificate al 2026 dagli operatori di mercato, sono risultate non coperte da almeno una rete in grado di fornire in maniera affidabile velocità di connessione in download ≥300 Mbps. La soglia minima di intervento viene dunque aumentata a 300 Mbps (in download), rispetto ai 100 Mbps previsti inizialmente dalla Strategia di maggio. Tale soglia prestazionale è ritenuta necessaria per raggiungere l'obiettivo di connettività ad almeno 1 Gbps definito nel **Digital Compass**, sviluppando reti "*a prova di futuro*" che permetteranno a cittadini, imprese e PA di fruire di servizi avanzati quali, tra gli altri, video streaming ad alta definizione, realtà virtuale e aumentata, smart working e formazione a distanza, *cloud computing*, *online gaming*, telemedicina, ecc.

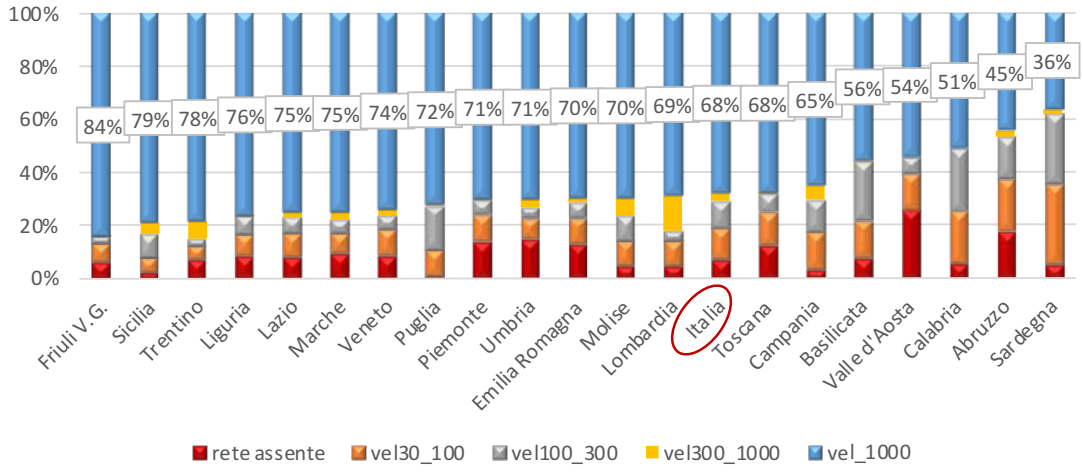
Il primo adempimento procedurale svolto dal Governo italiano, ai fini dell'attuazione del piano di intervento nelle aree "*a fallimento di mercato*", nelle quali non è attualmente presente né lo sarà entro i prossimi 5 anni (entro il 2026) almeno una rete in grado di offrire una velocità di connessione stabile pari o superiore a 300 Mbps, è stata la predisposizione di una mappatura particolareggiata del territorio nazionale, effettuata tramite consultazione pubblica.

La consultazione è stata condotta tra il 30 aprile 2021 e si è conclusa il 15 giugno 2021, mentre i risultati relativi alle coperture previste per il 2026 sono stati pubblicati ad agosto. Le tecnologie monitorate sono: 1) rame con tecniche trasmissive VDSL/VDSL 2+/E-VDSL; 2) rame con tecniche trasmissive vectoring/G.fast/bonding; 3) fibra ottica (secondo le architetture FTTH/FTTB) fino al civico che indentifica l'edificio o al massimo ad una distanza minore o uguale a 50 metri; 4) FWA su frequenza licenziata con fibra fino alla BTS (Base Transceiver Station); 5) FWA su frequenza licenziata senza fibra fino alla BTS. In questo caso, le coperture sono riportate per classi di velocità: 1) tra 30 Mbps e 100 Mbps; 2) tra 100 Mbps e 200 Mbps; 3) tra 200 Mbps e 300Mbps[30]; 4) tra 300 Mbps e 1 Gbps; 5) oltre 1 Gbps[31].

Dalla consultazione, cui hanno risposto 47 operatori, risulta una copertura con velocità superiore a 300 Mbps, al 2026, del 71% del territorio nazionale, prevalentemente costituita da rete a velocità superiore a 1 Gbps (68%) (Fig. 6.3).

Figura 6.3 Copertura di rete, per fascia di velocità (% civici, 2026)

Fonte: Elaborazioni I-Com su dati Infratel



[30] Nell'analisi che segue, le classi 2) e 3) sono state accorpate, dati i numeri esigui relativi alle classe 3).

[31] I valori previsti per la velocità massima raggiungibile in upload sono: 1) tra 15Mbps e 50Mbps; 2) tra 50 Mbps e 100Mbps; 3) tra 100Mbit/s e 200Mbps; 4) oltre 200Mbps.

Mentre il 29% del territorio resterebbe oggetto di intervento: in particolare, un civico su dieci sarebbe raggiunto da una rete a velocità superiore a 100 Mbps ma inferiore a 300 Mbps; poco di più (12%) godrebbe di una velocità inferiore ai 100 Mbps; e resterebbe un 7% di civici non coperti (le cosiddette aree bianche).

Prima regione per copertura ad almeno 1 Gbps sarebbe il Friuli Venezia Giulia (84%), seguita da Sicilia (79%), Trentino Alto Adige (78%) e Liguria (76%). Bene anche Lazio e Marche (75%) e Veneto (74%), mentre tra le regioni del Sud solo Puglia e Molise figurerebbero al di sopra della media nazionale: secondo le previsioni, infatti, il 70% dei civici sarà coperto da rete con velocità oltre 1 Gbps sia in Puglia che in Molise. In quest'ultima si aggiunge, però, un ulteriore 6% di civici coperti con una velocità inferiore a 1 Gbps ma superiore a 300 Mbps. Le rimanenti regioni meridionali compaiono, invece, insieme a Toscana e Valle d'Aosta, nella parte bassa della classifica, con coperture a più di 1 Gbps nettamente inferiori alla media nazionale: nello specifico, in Sardegna e Abruzzo non sarebbe coperto, al 2026, nemmeno la metà del territorio, con una copertura tra i 300 Mbps e 1 Gbps del tutto marginale (e pari a solo il 2%). Ne consegue che, in queste regioni, la maggior parte dei civici rientrerebbe in quelli oggetto di intervento, ai sensi di quanto stabilito dal Piano "*Italia a 1 Giga*".

Nel complesso, emerge una situazione, su base regionale, abbastanza **uniforme**, con criticità maggiori nelle regioni Sardegna, Calabria, Basilicata e Abruzzo, dove oltre il 40% dei civici sarebbe da ritenersi oggetto di intervento, e regioni virtuose – Lombardia, Trentino Alto Adige e Friuli Venezia Giulia – in cui gli interventi riguarderebbero meno di un civico su dieci (Fig. 6.4). Se si guarda, poi, alla **massima velocità raggiungibile**, la situazione cambia parzialmente, lasciando tra le regioni particolarmente virtuose solo il Friuli-Venezia Giulia, in cui si punterà esclusivamente sulla velocità massima (presenterebbe, infatti, una copertura nulla per le velocità comprese tra i 300 Mbps e 1 Gbps).

La fotografia provinciale (Fig. 6.5) segnala un'**elevata diffusione (maggiore dell'80%) della rete ultra-veloce (≥300 Mbps)** in alcune province lombarde e quelle del Nord Est, queste ultime

Figura 6.4 Copertura regionale (% civici, 2026)

Fonte: Elaborazioni I-Com su dati Infratel

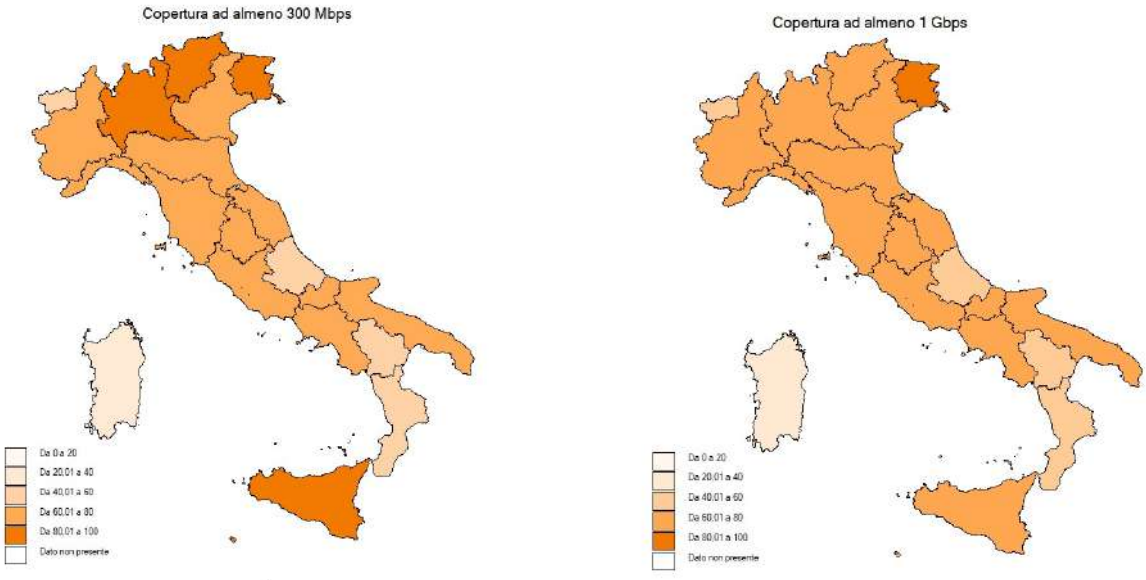


Figura 6.5 Copertura provinciale (% civici, 2026)

Fonte: Elaborazioni I-Com su dati Infratel

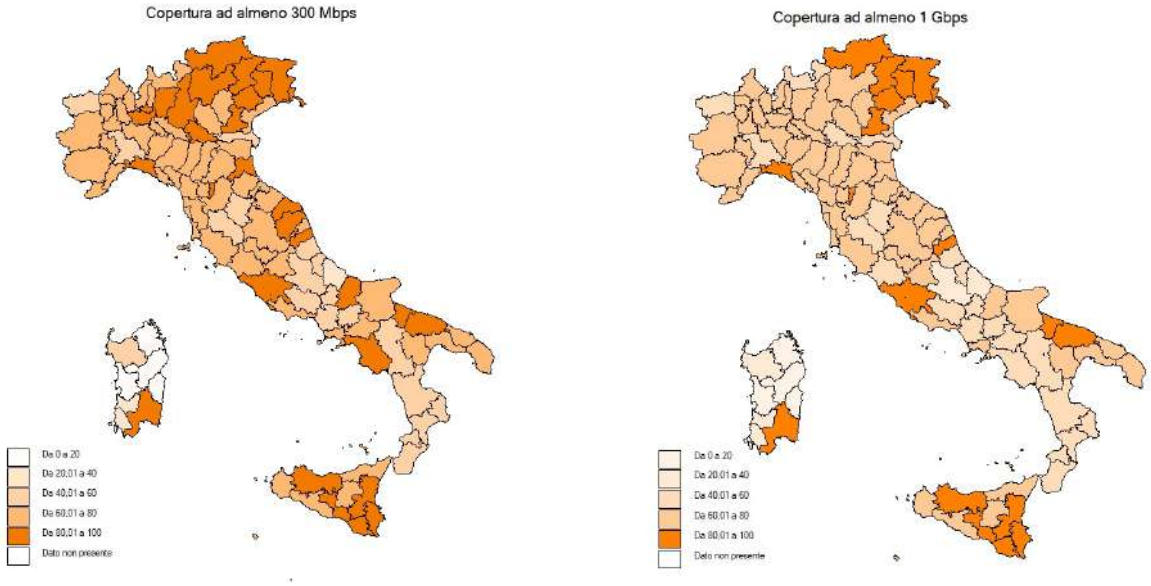
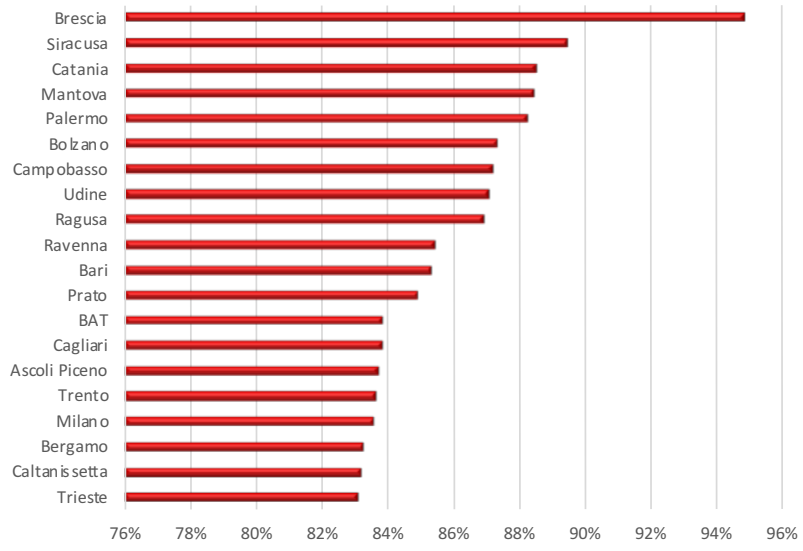


Figura 6.6 Top 20 province per copertura ad almeno 300 Mbps (2026)

Fonte: Elaborazioni I-Com su dati Infratel



particolarmente performanti anche con riguardo alle reti con velocità superiore a 1 Gbps. Nel resto d'Italia, a farsi notare sono cinque province siciliane – Siracusa (89%), Catania (88%), Palermo (88%), Ragusa (87%) e Caltanissetta (83%) – che figurano infatti tra le prime 20 province per copertura ad almeno 300 Mbps (Fig. 6.6). Nella Top 20 anche Cagliari (84%) per la Sardegna, Bari (85%) e BAT (84%) per la Puglia, Campobasso (87%) per il Molise, Ascoli Piceno (84%) per le Marche e Prato (85%) per la Toscana. Pur non rientrando nella Top 20, degne di nota sono anche le province di Genova, Roma, Salerno, Macerata e Ancona, tutte con una copertura ad almeno 300 Mbps, al 2026, superiore all'80%. Per quanto riguarda la copertura alla velocità massima (≥1

Gbps), le prime venti province presentano tutte un dato superiore all'80% (Fig. 6.7). Rientrano tra queste gran parte delle province già menzionate, in particolare quelle del Nord Est, le province di Genova, Roma, Prato, Ascoli Piceno, Bari, BAT, Cagliari e le cinque province siciliane summenzionate.

Dall'altro lato, vi sono, invece, province in cui si renderà necessario un massiccio intervento statale per poter raggiungere la soglia prestazionale dei 300 Mbps necessaria a garantire l'obiettivo di connettività ad almeno 1 Gbps definito nel Digital Compass. Si tratta di Oristano, Nuoro, Sud Sardegna – dove l'intervento riguarderà all'incirca 3 civici su 4 – Chieti, Vibo Valentia, Sassari, L'Aquila, Catanzaro, Teramo e Potenza, dove i civici sotto la soglia variano dal 51% di Potenza al 61% di Chieti (Fig. 6.8).

Figura 6.7 Top 20 province per copertura ad almeno 1 Gbps (2026)
Fonte: Elaborazioni I-Com su dati Infratel

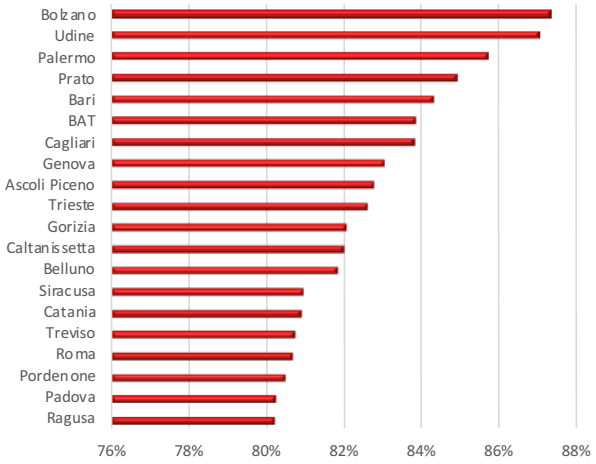
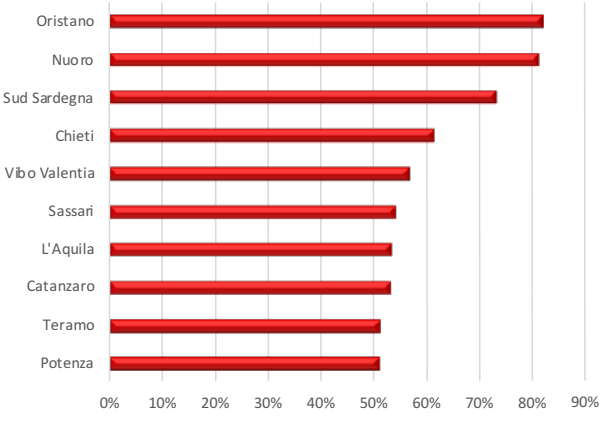


Figura 6.8 Province con più del 50% dei civici oggetto di intervento
Fonte: Elaborazioni I-Com su dati Infratel



6.1.2 Lo stato di avanzamento dei lavori nelle Aree Bianche

All'interno della Strategia per la Banda Ultralarga del 2015, uno dei principali tasselli è costituito dal **Piano Aree Bianche**, che riguarda specificamente le aree a fallimento di mercato (che risultano sguarnite e in cui le normali dinamiche di mercato non garantirebbero un'adeguata realizzazione delle infrastrutture). Per queste aree si è puntato su un modello a concessione tramite fondi nazionali (FSC), fondi comunitari (FESR e FEASR, assegnati dalle Regioni al Ministero dello Sviluppo Economico in base ad accordi Stato-Regioni) e fondi regionali per la realizzazione di una rete di proprietà pubblica aperta a tutti gli operatori TLC in modalità *wholesale*[32], che rimane per 20 anni in concessione all'aggiudicatario, individuato tramite procedura di gara pubblica, il quale si occupa di realizzarla e di gestire l'infrastruttura passiva.

L'attuazione del Piano Banda Ultralarga del 2015 è stata affidata a Infratel, con l'obiettivo di dotare 7.700 comuni di connessione in fibra ottica, in aggiunta ai comuni da coprire con connessione mista fibra-wireless (FWA) con prestazioni fino a 100 Mbps.

I comuni oggetto di intervento sono stati suddivisi in tre diverse gare e parcellizzati in lotti regionali. La prima gara prevedeva 5 lotti in 3.043 comuni di Abruzzo, Molise, Emilia-Romagna, Lombardia, Toscana e Veneto. Il secondo bando copriva 6 lotti

[32] Gli altri operatori tlc acquistano connettività in modalità *wholesale* dal concessionario, a prezzi definiti da Agcom, e rivendono il servizio al dettaglio ai clienti finali, ovvero cittadini, imprese e Pubblica Amministrazione.

comprendenti 3.710 comuni, distribuiti in 10 regioni (Basilicata, Campania, Friuli Venezia Giulia, Lazio, Liguria, Marche, Piemonte, Sicilia, Umbria e Valle d'Aosta) e nella Provincia Autonoma di Trento. Il terzo bando, indirizzato a Sardegna, Puglia e Calabria, è stato assegnato il 18 dicembre 2018 e prevede il collegamento di oltre 317 mila unità immobiliari in 959 comuni.

Come noto, i bandi sono stati tutti aggiudicati a Open Fiber. La sottoscrizione del contratto di concessione tra Infratel e Open Fiber per i lotti del primo bando è avvenuta a giugno 2017, per il secondo a novembre 2017 e per il terzo ad aprile 2019.

Al 31 agosto 2021[33], dal punto di vista progettuale, degli oltre 9.500 progetti previsti in FTTH, ne risultavano approvati più di 8.300, da realizzarsi in circa 5.900 comuni (il 95% dei comuni previsti). Sono, invece, oltre 6.760 (su 7.121 previsti) i progetti approvati in FWA. A livello realizzativo, per le infrastrutturazioni in fibra sono stati emessi quasi 5.000 ordini di esecuzione, di cui oltre 3.000 risultano chiusi, ovvero con CUIR (Comunicazione Ultimazione Impianto di Rete), a fronte di oltre 2.000 interventi "*completati*" (Tab. 6.1). Per i

Tabella 6.1 Progettazione ed esecuzione cantieri in fibra (FTTH; 31 agosto 2021)

Fonte: Infratel

REGIONE	COMUNI PREVISTI	COMUNI PROGETTI APPROVATI	COMUNI CON ORDINE	COMUNI COMPLETATI	COMUNI COLLAUDATI	COMUNI CON COLLAUDI POSITIVI
Abruzzo	174	173	141	98	87	78
Basilicata	103	103	92	60	39	36
Campania	238	184	215	149	40	37
Calabria	449	394	63	46	102	85
Emilia-Romagna	242	232	205	83	58	53
Friuli-Venezia Giulia	182	180	135	100	86	81
Lazio	329	325	186	121	97	95
Liguria	201	200	102	32	11	9
Lombardia	1.147	1.071	534	293	217	183
Marche	221	218	203	86	62	60
Molise	132	132	86	53	45	44
Piemonte	1.115	1.082	515	297	189	171
Puglia	223	196	60	45	29	24
Sardegna	135	130	45	29	26	23
Sicilia	318	277	218	183	165	163
Toscana	210	194	131	66	49	40
Trentino-Alto Adige	214	206	129	51	26	18
Umbria	78	77	74	46	40	38
Valle D'Aosta	68	68	39	23	14	12
Veneto	453	452	331	155	128	121
TOTALE	6.232	5.894	3.504	2.016	1.510	1.371

[33] Fonte: Relazione sullo "*Stato di avanzamento del piano strategico per la banda ultralarga*" pubblicata da Infratel.

Tabella 6.2 Progettazione ed esecuzione cantieri wireless (FWA; 31 agosto 2021)

Fonte: Infratel

REGIONE	COMUNI PREVISTI	COMUNI PROGETTI APPROVATI	COMUNI CON ORDINE	COMUNI COMPLETATI	COMUNI CON COLLAUDI POSITIVI
Abruzzo	147	140	52	51	14
Basilicata	103	103	62	59	11
Campania	373	365	60	48	3
Calabria	525	522	139	115	9
Emilia-Romagna	330	316	218	200	35
Friuli-Venezia Giulia	197	194	86	75	34
Lazio	358	349	120	112	19
Liguria	228	218	82	65	1
Lombardia	1.312	1.112	258	249	37
Marche	233	229	91	80	14
Molise	105	105	31	30	10
Piemonte	1.183	1.164	250	209	47
Puglia	253	252	38	25	4
Sardegna	298	252	85	65	0
Sicilia	314	314	153	146	47
Toscana	252	248	138	91	4
Trentino-Alto Adige	212	210	47	42	0
Umbria	87	85	63	59	16
Valle D'Aosta	71	71	23	21	6
Veneto	540	513	184	166	41
TOTALE	7.121	6.762	2.180	1.908	352

cantieri FWA si osservano quasi 2.200 ordini emessi, di cui oltre 1.900 con CUIR (Tab.6.2).

L'avanzamento economico del progetto a livello nazionale ha raggiunto attualmente circa il 70% in termini di avanzamento dei lavori, con 1,09 miliardi impiegati su oltre 1,5 miliardi di euro di lavori ordinati a Open Fiber.

Tuttavia, per poter fornire i servizi alla cittadinanza è necessario eseguire il **collaudo degli impianti**.

Il collaudo richiede che il comune sia stato completato in tutte le sue componenti e pertanto sia in possesso dei CUIR del PCN (Punto di consegna neutro), della rete primaria e della rete secondaria, ove siano previsti tutti. A questo punto, Open Fiber può presentare la documentazione di *as built* a Infratel Italia che avvia le attività di collaudo.

I collaudi dei siti FWA, invece, vengono eseguiti man mano che sono completati, anche se coprono solo parzialmente il comune.

Per poter collaudare un sito FWA è necessario che siano stati completati con CUIR l'ordine del sito, il PCN a cui il sito è collegato e sia stato realizzato il collegamento ottico tra il sito ed il PCN.

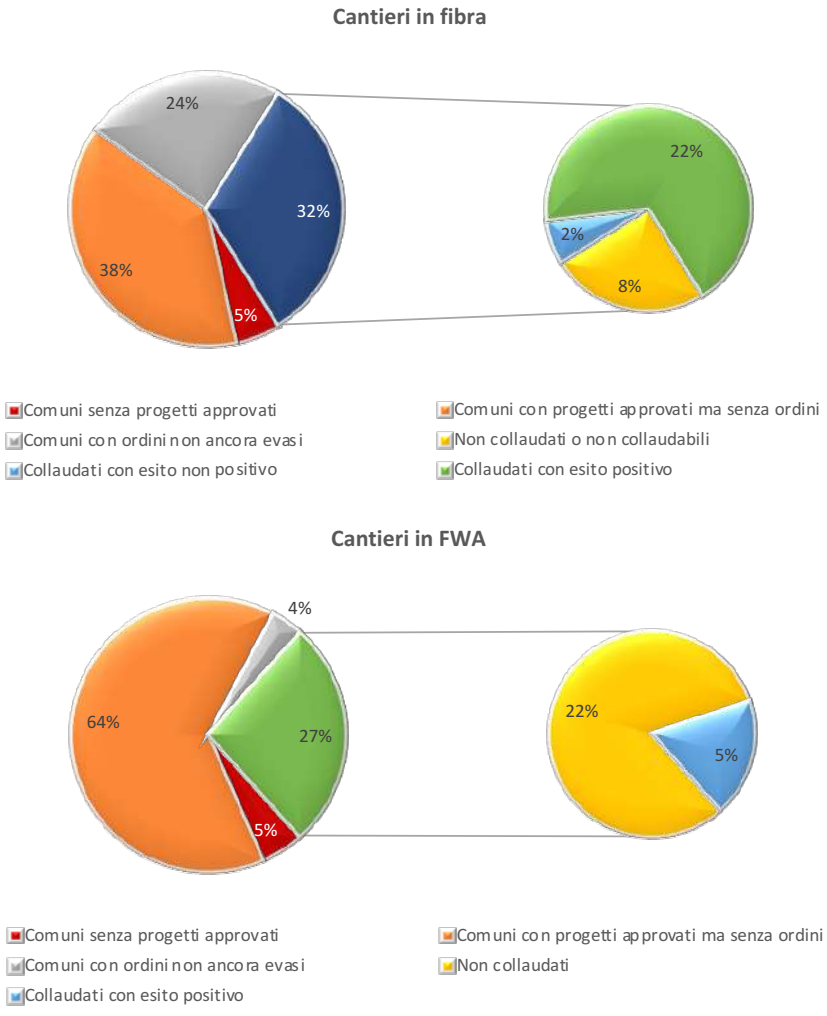
Dei 6.232 comuni coinvolti, **il 32% sono comuni completati**, e di questi 1.371 (pari al 22%) collaudati positivamente e, dunque, pronti a offrire il servizio al cittadino (Fig. 6.9).

Molto inferiore il grado di avanzamento dei siti FWA, pari a solo il 5% dei 7.121 comuni previsti. In questo caso, per il 64% si tratta di progetti approvati per i quali non è ancora stato emesso l'ordine; dei comuni completati (27% dei previsti), invece, meno di uno su cinque risulta essere stato collaudato con successo.

A livello regionale, particolarmente bene vanno

Figura 6.9 Progettazione ed esecuzione cantieri in fibra e FWA (31 agosto 2021)

Fonte: Infratel



gli interventi in Sicilia, Umbria, dove circa un impianto in fibra su due risulta pronto per servire i cittadini (Fig. 6.10), ma anche in Abruzzo e Friuli V.G., dove la percentuale è pari al 45%.

Percentuali invece bassissime si registrano in Liguria (4%) e Trentino A.A. (8%), ma anche in Puglia, dove si supera appena il 10%.

Per quanto riguarda i siti FWA (Fig. 6.11), a discostarsi in maniera relativamente significativa dal dato nazionale (5%) sono Umbria (18%), Friuli V.G. (17%) e Sicilia (15%), mentre dall'altro lato

Figura 6.10 Comuni con cantieri fibra collaudati positivamente (% su totale comuni previsti; 31 agosto 2021)

Fonte: Infratel

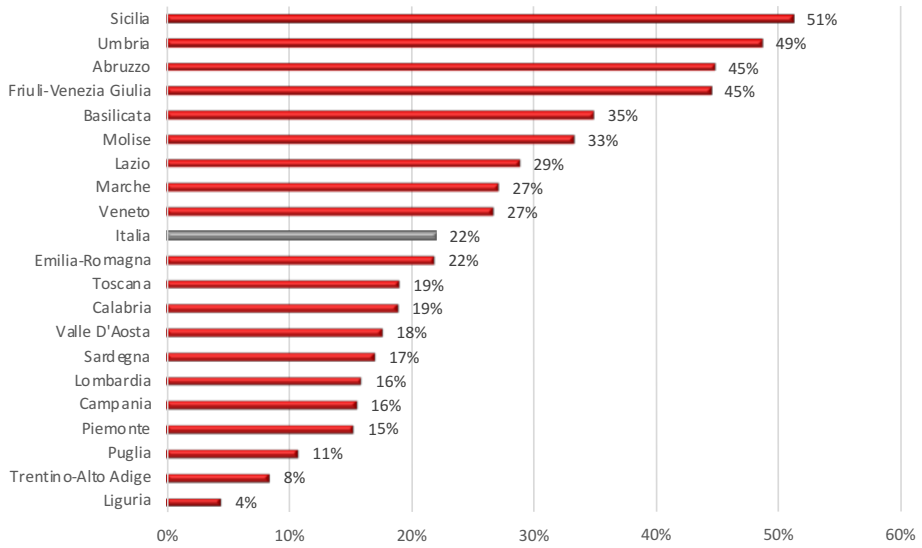
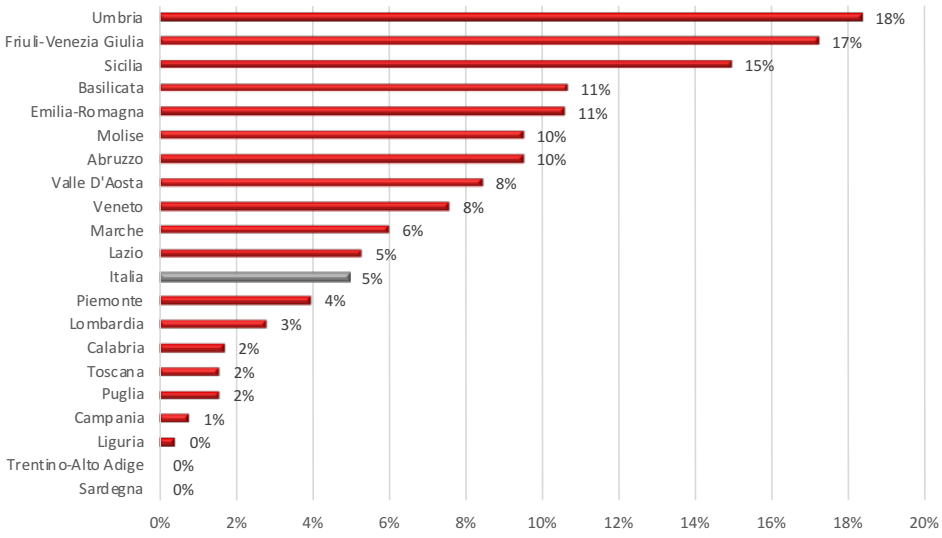


Figura 6.11 Comuni con siti FWA collaudati positivamente (% su totale comuni previsti; 31 agosto 2021)

Fonte: Infratel



non risultano ancora collaudi conclusi con successo in Trentino A.A. e Sardegna.

6.1.3 Il contributo del FWA alla connettività in banda ultralarga

A livello tecnico, una connessione FWA prevede che un cavo, generalmente in fibra ottica, arrivi fino a una stazione radio base (detta BTS) la quale emette un segnale senza fili per raggiungere il terminale ricevente (un'antenna posta in prossimità del domicilio dell'utente) che a sua volta lo distribuisce all'interno dell'abitazione.

Questa architettura costituisce un'alternativa **più economica e flessibile** rispetto a quella

Tabella 6.3 La copertura dell'FWA per regione (per migliaia di famiglie raggiunte e in%)

Fonte: Elaborazioni I-Com su dati AGCOM, 2021
*I dati regionali ed il conteggio complessivo non includono la Sardegna per via di alcune discrepanze tra vecchia e nuove segmentazione provinciale

Regione*	Famiglie coperte in FWA a dicembre 2020	Famiglie al 31.12.2019	Famiglie coperte in FWA (%)	Incidenza famiglie coperte in FWA per regione su tot fam. coperte FWA (%)
Abruzzo	458	557	82%	2%
Basilicata	26	235	11%	0%
Calabria	120	799	15%	1%
Campania	1.396	2.179	64%	7%
Emilia-Romagna	1.730	2.021	86%	9%
Friuli-Venezia Giulia	480	562	85%	3%
Lazio	2.257	2.611	86%	12%
Liguria	715	759	94%	4%
Lombardia	4.119	4.491	92%	22%
Marche	535	645	83%	3%
Molise	44	131	34%	0%
Piemonte	1.902	1.992	95%	10%
Puglia	219	1.597	14%	1%
Sicilia	700	1.986	35%	4%
Toscana	1.387	1.647	84%	7%
Trentino-Alto Adige	363	466	78%	2%
Umbria	308	384	80%	2%
Valle D'Aosta	55	61	91%	0%
Veneto	1.810	2.086	87%	10%
Totale complessivo*	18.625	25.207	74%	100%

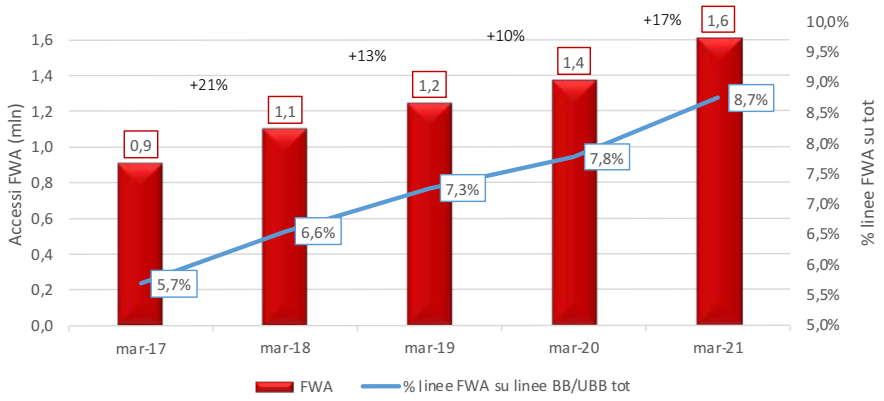
tradizionale, in particolare per le zone dove non è presente una rete cablata fino a casa dell'utente o in cui sarebbe anti-economico costruirla.
A livello di copertura, i dati riportati nell'AGCOM *BroadbandMap* e rielaborati a livello provinciale **indicano che gli operatori FWA coprono circa il 74% delle famiglie italiane**[34]. A tal proposito, è interessante notare come le regioni maggiormente raggiunte siano situate prevalentemente nel **Nord Italia**, con Piemonte (95%), Liguria (94%), Lombardia (92%) e Valle d'Aosta (91%) che figurano nelle prime 4 posizioni, mentre i minori tassi di copertura si registrano in Sicilia (35%), Molise (34%), Calabria (15%), Puglia (14%) e Basilicata (11%).

Inoltre, suddividendo il numero di famiglie coperte con tecnologia FWA in ogni regione rispetto al totale di famiglie coperte con la medesima tecnologia, si osserva come oltre la

[34] La regione Sardegna non è stata inclusa nella presente tabella per via di alcune incongruenze nei dati dovute al successivo accorpamento delle province di Carbonia e Medio Campidano nel Sud Sardegna, di Ogliastra nella Provincia di Nuoro e di Olbia in quella di Sassari.

Figura 6.12 Accessi a banda larga con tecnologia FWA (in mln e in % su tot linee bb/ubb)

Fonte: Elaborazioni I-Com su dati AGCOM, 2021



metà del target attualmente raggiunto si concentri in 4 regioni, Lombardia (22%), Lazio (12%), Piemonte (10%) e Veneto (10%).

A livello di abbonamenti (Fig.6.12) il FWA appare in continua espansione, giunto a oltre 1,6 milioni di sottoscrizioni e arrivato a servire quasi il 10% del totale delle utenze broadband attive in Italia (8,7% a marzo 2021). Osservando i tassi di crescita, inoltre, emerge come il trend di diffusione di questa tecnologia sia ancora in fase espansiva, passato da + 10% del 2020 a + 17% del 2021. La Tab. 6.4 contiene il *breakdown* degli abbonamenti FWA per regione, aggiornato a dicembre 2020. Tale comparazione mostra in particolare come quelle in cui tale la tecnologia

Tabella 6.4 Breakdown regionale degli accessi FWA (in migliaia e in%, dicembre 2020)

Fonte: Elaborazioni I-Com su dati AGCOM, 2021

Regione	Accessi FWA (.000)	Accessi BB/UBB totali (.000)	Accessi FWA su tot BB/UBB (%)	Accessi regionali FWA su tot FWA (%)
Abruzzo	37	332	11%	2%
Basilicata	9	119	8%	1%
Calabria	46	424	11%	3%
Campania	88	1.580	6%	6%
Emilia-Romagna	123	1.492	8%	8%
Friuli-Venezia Giulia	38	383	10%	2%
Lazio	127	2.011	6%	8%
Liguria	39	551	7%	3%
Lombardia	271	3.482	8%	18%
Marche	39	462	9%	3%
Molise	5	59	8%	0%
Piemonte	165	1.319	13%	11%
Puglia	132	1.041	13%	9%
Sardegna	23	424	5%	1%
Sicilia	112	1.189	9%	7%
Toscana	76	1.255	6%	5%
Trentino-Alto Adige	32	298	11%	2%
Umbria	36	154	14%	2%
Valle D'Aosta	8	37	22%	1%
Veneto	134	1.417	10%	9%
TOTALE	1.539	18.129	9%	100%

fisso-mobile risulta maggiormente utilizzata sono la Lombardia (271.000 utenti), il Piemonte (165.000), il Veneto (134.000) e la Puglia (132.000).

Inoltre, analizzando l'incidenza degli abbonamenti FWA rispetto agli abbonamenti in banda larga e ultralarga (BB/UBB) di ogni regione, si osserva come questa modalità di connessione sia particolarmente utilizzata in Valle d'Aosta (dove il 22% delle utenze broadband utilizza una connessione FWA) e in Umbria (14%), ma anche negli stessi Piemonte e Puglia (entrambi con un'incidenza del 13%).

In termini percentuali, oltre **il 18% delle utenze FWA italiane sono attive in Lombardia** e **l'11% in Piemonte**, mentre Puglia e Veneto presentano una quota del 9% ciascuna.

Come mostra la figura 6.13, i principali operatori nel segmento FWA risultano attualmente Linkem ed Eolo, rispettivamente con 680.000 e circa 540.000 utenti. Molto più staccati Tiscali (42.000), BBBel 25.000) e Go Internet (22.000), mentre Tim e Vodafone, anch'essi attivi nel settore, presentano rispettivamente 91.000 e 22.000 utenti attivi. Non trascurabile, quindi, la quota di tutti gli altri piccoli operatori, che arrivano complessivamente a circa 120.000 utenti.

Figura 6.13 Accessi FWA per operatore (in migliaia, dicembre 2020)

Fonte: Elaborazioni I-Com su dati AGCOMcom, 2021

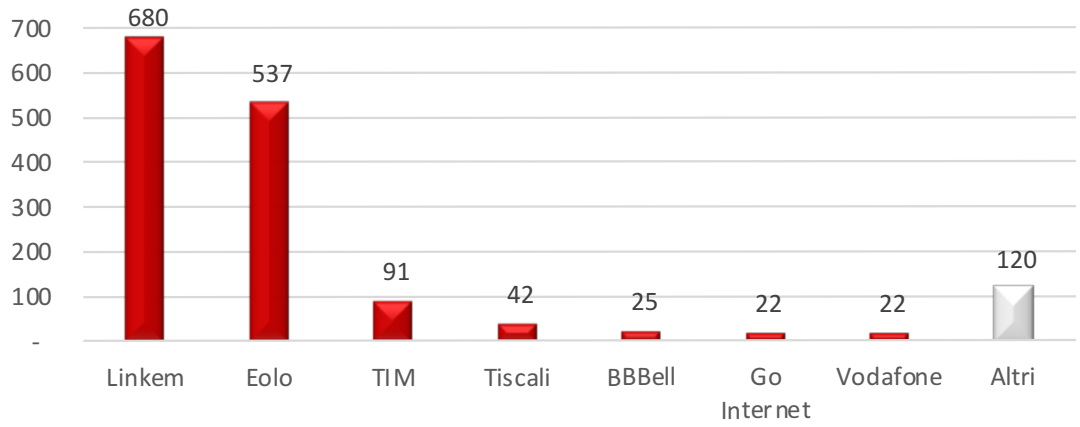
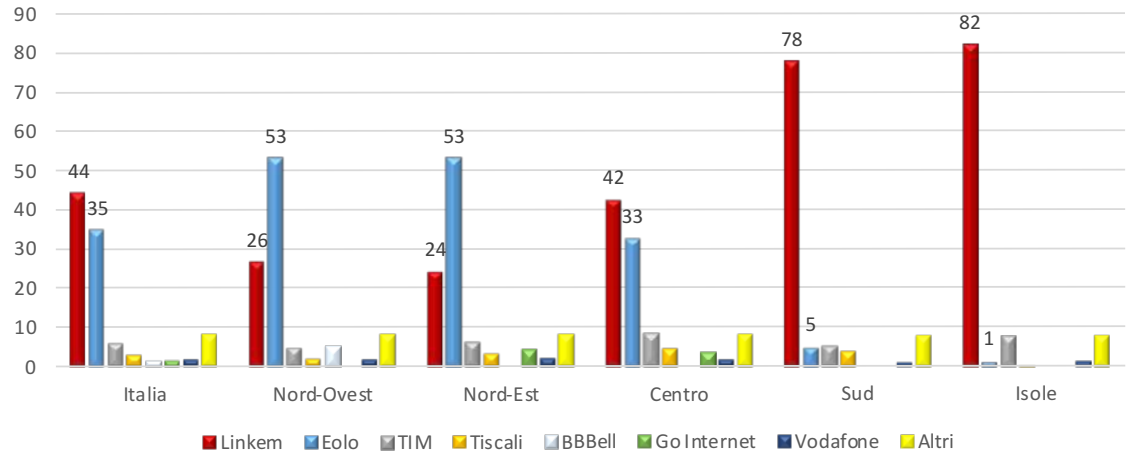


Figura 6.14 Accessi FWA per operatore per regione (in %, dicembre 2020)

Fonte: Elaborazioni I-Com su dati AGCOM, 2021



In termini percentuali (Fig. 6.14), Linkem detiene circa il 44% del mercato, con una presenza rilevante nel Centro Italia e in particolare nel Sud e nelle Isole. Eolo detiene poco più di un terzo del mercato italiano (35%) ed è presente soprattutto nell'Italia settentrionale (attestandosi al 53% sia nel Nord Ovest che nel Nord Est). Si osserva inoltre come il recente ingresso dei *player* di maggiori dimensioni (Tim e Vodafone lo scorso dicembre rappresentavano il 7,3%) avrà verosimilmente un impatto degli scenari competitivi di questo segmento di mercato.

La natura ibrida della tecnologia *fixed-wireless* ha introdotto un ulteriore elemento di valutazione all'interno della consultazione del 2021 condotta da Infratel, in particolare relativa alla copertura effettiva offerta al 2026 con capacità 300 Mbps, e quindi al contributo che il FWA potrà fornire nel portare a compimento **l'ambizioso Piano Italia 1 Giga**.

Quest'ultimo, in particolare, ha l'obiettivo di fornire connettività "*ad almeno 1 Gbps in download e 200 Mbps in upload alle unità immobiliari che, a seguito della mappatura delle infrastrutture presenti o pianificate al 2026 dagli operatori di mercato, sono risultate non coperte da almeno una rete in grado di fornire in maniera affidabile velocità di connessione in download pari o superiori a 300 Mbps*".

Poiché il servizio FWA viene fornito tramite celle radioelettriche, i civici raggiunti dal segnale fisso-mobile non sono direttamente equiparabili a quelli raggiunti via cavo, per via di fattori quali dispersione e ripartizione della capacità delle singole celle tra gli utenti effettivamente connessi.

Nel Piano Italia a 1 Giga si parla di differenza tra **utenti raggiunti**, ovvero "*passed*", e **utenti effettivamente serviti** o "*served*".

Per queste ragioni, per gli operatori FWA è più complicato fornire una precisa indicazione di quanti utenti verranno effettivamente serviti a 300 Mbps nel 2026, anche perché tale valore dipende anche da quanti utenti si abboneranno ed utilizzeranno effettivamente la rete nel corso del quinquennio in esame.

Secondo quanto riportato nel Piano Italia 1 Giga, si ritiene ragionevole applicare il **criterio del 10%**, che consiste nel considerare effettivamente serviti con tutta la banda richiesta circa il 10% degli utenti coperti dalle celle elettromagnetiche (o "*passed*"). L'entità del contributo che il FWA potrebbe apportare alla copertura arriva al 2,6% dei circa 21,3 milioni di civici in consultazione, equivalenti a circa 554.000. Tale cifra ammonta a quasi il 9% del totale dei **6,2 milioni di civici** che, allo stato attuale, vengono ritenuti sguarniti al 2026 e su cui verrebbero effettuati i bandi di gara. Verranno comunque effettuati ulteriori approfondimenti per verificare quanti civici potranno essere effettivamente serviti entro tale data con queste caratteristiche, di concerto anche con la Commissione europea[35].

La relazione di Infratel sulla consultazione di maggio-giugno 2021 offre una panoramica della copertura al 2026, con le proiezioni relative alle normali dinamiche di investimento degli operatori, per le tre fasce di velocità 100 Mbps, 200 Mbps e 300 Mbps (Tab.6.5). Per ciascuna di esse, e per ogni regione, vengono indicate tre proiezioni di copertura (in %): la copertura dei

[35] Tra le caratteristiche figurano la velocità di 300 Mbit/s stabile in download entro quattro settimane dalla richiesta del cliente, senza costi addizionali o straordinari. Nel dettaglio, secondo le Guidelines del Berec, "*A premise is considered passed if, on request from an end-user, the relevant operator can provide broadband services (regardless of whether these premises are already connected or not connected to the network) at the end-user premises. The provision of broadband services at the end users premises should not exceed normal connection fees, i.e. without any additional or exceptional cost if it is the standard commercial practice and, in any case, not exceeding the usual cost in the country. The reference for "normal connection fees" should be determined by the relevant NRA/OCA. Furthermore, the operator must be able to technically connect the end user, usually within 4 weeks from the date of the request*".

Tabella 6.5 Percentuale dei civici oggetto di investimenti privati al 2026 per ciascuna regione in base alla velocità stabile in download nell'ora di picco del traffico (considerando una velocità massima di almeno 300 Mbit/s)

Fonte: Infratel, Relazione di sintesi della Mappatura delle Reti Fisse 2021

REGIONI	TOTALI CIVICI MAPPATURA 2021	VELOCITÀ DI PICCO ≥ 100 Mbps			VELOCITÀ DI PICCO ≥ 200 Mbps			VELOCITÀ DI PICCO ≥ 300 Mbps		
		SENZA FWA	CON FWA SERVED	CON FWA PASSED	SENZA FWA	CON FWA SERVED	CON FWA PASSED	SENZA FWA	CON FWA SERVED	CON FWA PASSED
ABRUZZO	646.334	47%	51%	82%	47%	49%	67%	47%	47%	49%
BASILICATA	297.784	56%	60%	84%	56%	58%	74%	56%	56%	59%
CALABRIA	1.669.114	51%	55%	84%	51%	53%	71%	51%	51%	54%
CAMPANIA	1.357.191	70%	74%	92%	70%	72%	85%	70%	71%	75%
EMILIA-ROMAGNA	1.563.860	71%	74%	90%	71%	73%	82%	71%	72%	73%
FRIULI-VENEZIA GIULIA	479.397	84%	86%	96%	84%	85%	91%	84%	84%	85%
LAZIO	1.728.220	77%	79%	93%	77%	78%	86%	77%	77%	79%
LIGURIA	602.709	76%	79%	94%	76%	78%	87%	76%	77%	80%
LOMBARDIA	2.185.382	82%	84%	96%	82%	83%	90%	82%	82%	84%
MARCHE	446.628	78%	80%	95%	78%	79%	88%	78%	78%	80%
MOLISE	69.757	76%	79%	97%	76%	78%	90%	76%	76%	77%
PIEMONTE	928.489	71%	73%	91%	71%	72%	83%	71%	71%	73%
PUGLIA	2.302.160	73%	77%	97%	73%	75%	91%	73%	73%	78%
SARDEGNA	985.274	38%	44%	84%	38%	41%	69%	38%	38%	41%
SICILIA	2.454.755	83%	85%	97%	83%	84%	93%	83%	83%	86%
TOSCANA	1.618.678	68%	72%	91%	68%	70%	82%	68%	68%	70%
BOLZANO	41.523	87%	89%	97%	87%	88%	94%	87%	87%	88%
TRENTO	86.590	84%	85%	95%	84%	84%	89%	84%	84%	84%
UMBRIA	307.060	73%	75%	89%	73%	74%	82%	73%	73%	75%
VALLE D'AOSTA	20.044	54%	59%	91%	54%	57%	79%	54%	55%	59%
VENETO	1.532.929	77%	79%	94%	77%	78%	85%	77%	77%	78%
TOTALE	21.323.878	71,00%	73,90%	92,30%	71,00%	72,60%	84,20%	71,00%	71,20%	73,60%

civici senza il supporto del FWA, la copertura dei civici anche con il supporto del FWA, relativo ad una percentuale considerata servita (served), e la copertura con il pieno supporto del FWA, qualora la totalità dei civici raggiunti dal segnale (ovvero "*passed*") sia considerata effettivamente servita ("*served*"). Nel valutare l'entità dell'impiego del FWA nel Piano Italia 1 Giga, sarà opportuno considerare anche due ulteriori fattori.

In primo luogo, **la tecnologia wireless evolve in media una volta ogni 5 anni**, a differenza del cavo che presenta in genere un'innovazione tecnologica ogni 10. Di conseguenza, mantenendo un approccio che includa la prospettiva temporale, è opportuno tenere presente, nelle valutazioni su copertura e capacità, anche gli upgrade di cui l'FWA o altre tipologie di connettività mobile beneficeranno nei prossimi 5-10 anni.

Inoltre, occorre valutare **l'effettiva praticabilità dell'infrastrutturazione per raggiungere ogni tipo di indirizzo civico**, anche il più remoto, con tecnologie via cavo. A tal proposito, il trend evolutivo del piano aree bianche, in cui è progressivamente aumentata (fino al 24%, per circa 2,2 milioni di unità immobiliari) la percentuale di civici coperti in FWA rispetto all'FTTH (anche a fronte di una riduzione complessiva dei civici da raggiungere) mostra come, a conti fatti, il *fixed-wireless* sia una tecnologia su cui continueremo a fare affidamento anche nel medio-lungo termine.

6.2 LE RETI MOBILI E L'IMPORTANZA DEL 5G

6.2.1 Le infrastrutture di rete mobile

Sin dagli anni '90 le reti mobili italiane sono sempre risultate tra le più diffuse e performanti a livello europeo. Secondo i dati AGCOM, se da tempo la connettività di terza generazione ha raggiunto la stragrande maggioranza della popolazione, giunta nel 2018 alla quasi totalità (99,8%), anche la rete 4G negli ultimi anni ha mostrato un rapido progresso, andando a colmare quasi del tutto il 10% di popolazione che non risultava coperta nel 2014 e raggiungendo quota 98,9% della popolazione.

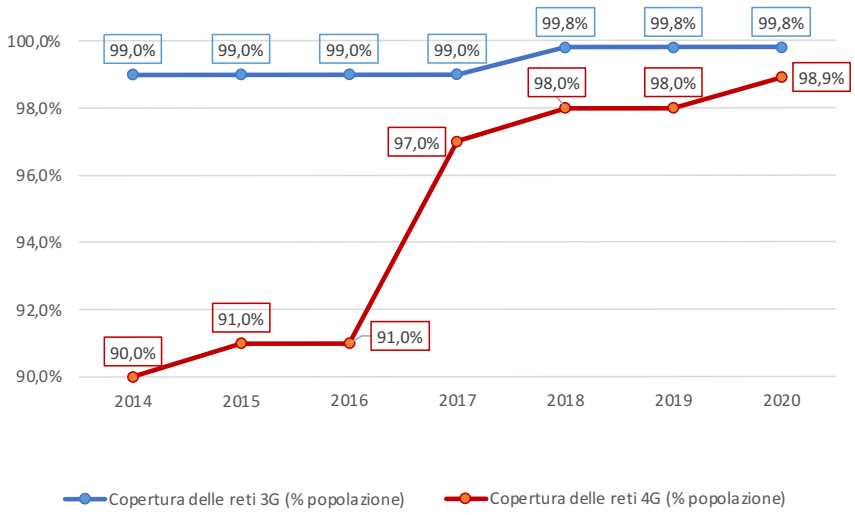
Allo stato attuale, **la rete 4G sembra presentare anche ottime performance**. La stessa autorità indica che le velocità rilevate a livello statistico in 10 città ammontano rispettivamente a 68,2 Mbps in download e 28,9 Mbps in upload.

Un'ulteriore analisi, che raccoglie dinamicamente i dati in 35 città, riporta valori leggermente più bassi ma comunque soddisfacenti, equivalenti ad oltre 60 Mbps in download e oltre 26 Mbps in upload (Fig. 6.16).

Discorso più complesso per il **5G,** rispetto al quale, oltre ad apposite iniziative e stanziamenti di risorse previste nell'ambito del PNRR, nella **nuova Strategia italiana per la banda ultralarga** e nel

Figura 6.15 La copertura delle reti mobili (% popolazione)

Fonte: Elaborazioni I-Com su dati AGCOM, 2021



Piano "*Italia 5G*", quest'ultimo ha previsto anche una **consultazione *ad hoc*** per verificare lo stato delle reti al 31 maggio 2021[36].
La mappatura, che inizialmente doveva terminare il 26 luglio, è stata estesa al 31 luglio e, al momento della scrittura del presente capitolo, i risultati della consultazione non sono ancora stati pubblicati.

Lo scopo principale della consultazione consiste nell'effettuare una mappatura delle reti mobili di ultima generazione correlandola ai piani di infrastrutturazione degli operatori per i prossimi cinque anni (ovvero il lasso di tempo su cui insiste il PNRR), specificando anno per anno gli interventi previsti e le fonti di finanziamento, tenendo conto anche degli obblighi di copertura associati ai diritti d'uso delle frequenze utilizzate ed evidenziando gli elementi che ne giustifichino l'attuabilità[37].

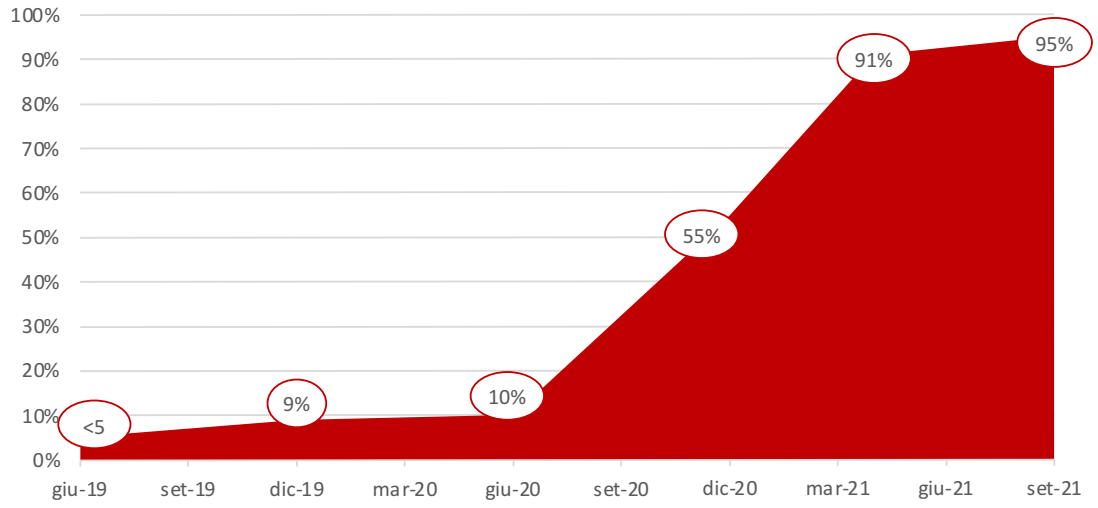
In assenza di dati ufficiali – e anche in considerazione del fatto che, a differenza di quanto accade per le reti fisse, ad oggi non è mai stato effettuato una consultazione completa della rete mobile nel Paese – si riporta l'analisi della copertura effettuata da EY, aggiornata a settembre 2021 (Fig. 6.17).

In base a tale analisi, **la copertura 5G ha raggiunto il 95% della popolazione italiana e oltre 7.500 comuni italiani**. In particolare, l'andamento rilevato mostra una decisa accelerazione tra giugno 2020, in cui risultava coperto appena il 10% della popolazione, e giugno 2021, mese in cui tale valore ha superato quota 90%, per poi attestarsi al **95%** rilevato a settembre.

Nel dettaglio, il dato rilevato da EY indica la copertura di almeno un operatore, in

Figura 6.17 Evoluzione della copertura 5G in Italia (in % sulla popolazione)

Fonte: Osservatorio Ultrabroadband EY, 30 settembre 2021



[36] Mappatura 2021 reti a banda ultralarga connessioni mobili: consultazione degli operatori, 10 giugno 2021 https://www.infratelitalia.it/archivio-documenti/documenti/mappatura-2021-reti-a-banda-ultralarga-connessioni-mobili_consultazione-degli-operatori

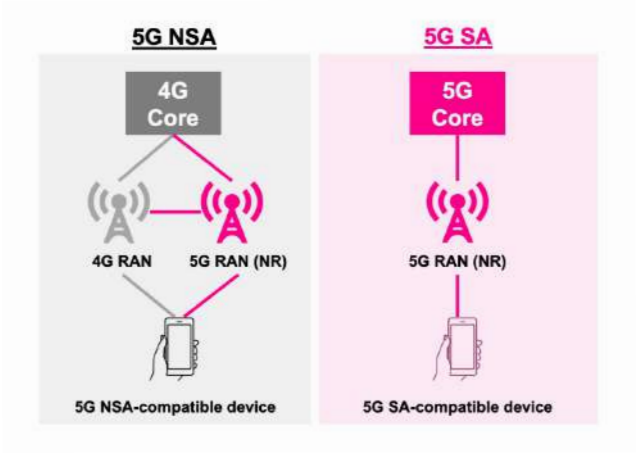
[37] A tal proposito, se consideriamo la rapida evoluzione delle tecnologie e le possibili variazioni negli scenari di mercato in un lasso di tempo così lungo (il piano strategico di Tim sulla Bul, ad esempio, ha generalmente un orizzonte triennale), si osserva la volontà di Infratel di trovare la quadra tra la necessità di rispettare la pianificazione quinquennale del Recovery Fund, evitare che qualche soggetto modifichi i propri piani per ricevere finanziamenti per aree che avrebbe coperto comunque e scongiurare che qualche operatore dichiari di investire in alcune aree per poi lasciarle di fatto sguarnite. Al fine di prevenire dichiarazioni mendaci che generino impatti negativi in termini di concorrenza, Infratel si propone di effettuare verifiche periodiche onde individuare interventi che vadano contro a quanto dichiarato dagli operatori e che questi ultimi non siano motivati da una giustificazione oggettiva.

sovrapposizione tra la modalità 5G "*non stand alone*" (NSA, ovvero su una rete in parte 5G) e quella 5G vera e propria (*stand alone*).

Per quanto concerne la prima, gli operatori utilizzano delle tecniche che permettono di offrire servizi 5G "*parzialmente 5G*" grazie all'upgrade delle reti di accesso (*Radio Access Network o RAN*) di quarta generazione al 5G, mantenendo invece invariata la rete *core* (4G). Questa ibridazione della rete consente quindi di aumentare notevolmente le performance, pur non arrivando a quelle massime offerte dal pieno dispiegamento delle reti 5G, che comporta l'implementazione di architetture e apparecchiature di nuova generazione sia delle rete di accesso, sia della rete *core* (Fig. 6.18).

Figura 6.18 Architettura 5G standalone (SA) vs non standalone (NSA)

Fonte: Diagramma esplicativo delle differenze tra reti 5G SA e NSA di Rakuten



Per quanto concerne le coperture dichiarate dai singoli operatori, Wind dichiara una copertura della popolazione in 5G NDA (*non stand alone*) superiore al 95.4% in DSS[38] e del 38% in modalità 5G TDD in banda 3.6 GHz[39]. Vodafone è presente attualmente in 25 città italiane (di cui coperte al 90% risultano Milano, Torino, Bologna, Roma, Napoli, Genova, Verona, Firenze, Palermo e Bari) e punta a raggiungere circa 50 città entro la fine del 2021[40]. Iliad copre alcune aree di Alessandria, Bari, Bologna, Brescia, Cagliari, Como, Ferrara, Firenze, Genova, La Spezia, Latina, Messina, Milano, Modena, Padova, Perugia, Pesaro, Pescara, Piacenza, Prato, Ravenna, Reggio Calabria, Reggio Emilia, Roma, Torino, Verona e Vicenza.

TIM ha dichiarato che per il 2021 è previsto un sensibile ampliamento della copertura in modalità SA (*stand alone*) in oltre 20 città. Attualmente la copertura ufficiale, con prestazioni fino a 2 Gbps in download e fino a 150 Mbps in upload, include il 90% delle seguenti città: Roma, Torino, Firenze, Napoli, Benevento, Ferrara, Bologna, Genova, Sanremo, Brescia e Monza, oltre ad alcune località turistiche come Cortina d'Ampezzo, Livigno e Selva di Val Gardena.

Anche Linkem ha lanciato un servizio 5G commerciale completamente stand alone in tecnologia FWA su frequenze a 26 GHz[41]. Secondo quanto dichiarato dal provider, il 50% dei propri impianti è già predisposto per l'adozione su base nazionale della nuova tecnologia.

A livello regionale (Fig. 6.19), la copertura complessiva stimata da EY vede tutte le regioni classificate in un range molto elevato, compreso **tra il 93% e il 98%** della popolazione raggiunta.

[38] Dynamic Spectrum Sharing, una tecnica che permette di usare dinamicamente lo stesso spettro FDD in modalità condivisa sia per connessioni 4G che per connessioni 5G.

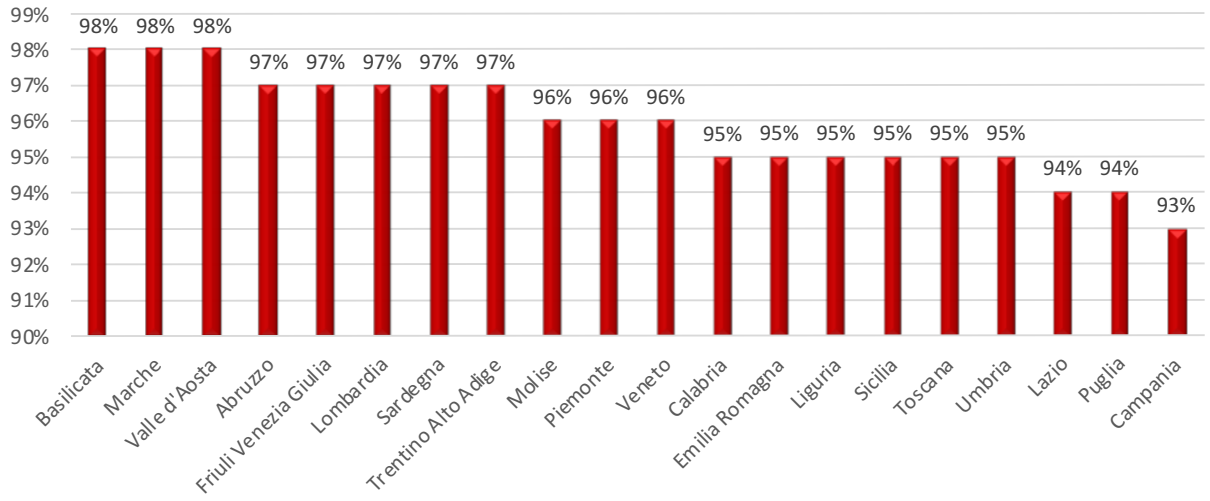
[39] La tecnologia 5G TDD necessita dell'accensione di nuovo spettro riservato alle sole connessioni 5G. Il roll-out della tecnologia 5G TDD è in corso, con priorità nelle zone ad alto traffico.

[40] Attualmente le città ufficialmente coperte in 5G da Vodafone sono Milano, Torino, Bologna, Roma, Napoli, Genova, Bergamo, Brescia, La Spezia, Monza, Novara, Verona, Padova, Parma, Rimini, Trento, Trieste, Venezia, Firenze, Cagliari, Prato, Palermo, Bari, Catania e Reggio Calabria. La copertura outdoor 5G della popolazione delle città è al 90% nelle città di Milano, Torino, Bologna, Roma, Napoli, Genova, Verona, Firenze, Palermo, Bari, sulle restanti città invece al 70%.

[41] Cfr. "*5G Fwa: Linkem lancia il primo servizio commerciale standalone*" CorCom, 30 settembre 2021. https://www.corrierecomunicazioni.it/telco/5g/5g-fwa-linkem-lancia-il-primo-servizio-commerciale-standalone/

Figura 6.19 Copertura 5G in Italia, breakdown regionale (in % sulla popolazione, settembre 2021)

Fonte: Osservatorio Ultrabroadband EY, 30 settembre 2021



Tra le prime figurano Basilicata, Marche e Val d'Aosta, tutte con una percentuale di abitanti coperti del 98%. Sotto il 95% si trovano soltanto Lazio (94%), Puglia (94%) e Campania (93%).

6.2.2 Il 5G per le industrie verticali

Come osservato nel paragrafo precedente, al momento i dati sulla copertura effettiva 5G sono piuttosto frastagliati, ed emerge una evidente necessità di chiarezza, in particolare per quanto concerne la copertura delle reti *stand alone* di nuova generazione. Questa è tanto più necessaria per due ordini di ragioni, direttamente connesse l'una con l'altra.

In primo luogo, la consultazione sullo sviluppo delle reti 5G appare fondamentale per individuare le "*aree a fallimento di mercato*" in cui lo Stato, tramite i fondi previsti, andrà a finanziare la copertura delle zone dove gli operatori privati non ritengono profittevole investire. La mappatura sarà quindi utile a fornire un **disegno chiaro della connettività mobile in Italia**, in particolare nelle aree extra urbane, e a favorire la copertura anche nei territori che altrimenti rimarrebbero sguarniti.

In secondo luogo, solo un pieno dispiegamento su gran parte del territorio di tutte le potenzialità tecniche del 5G *stand alone* può garantire il conseguimento di tutti i benefici collegati alla sua diffusione, in particolare provenienti dalle c.d. industrie verticali.

Per quanto concerne il primo aspetto, è opportuno ricordare come **la versione finale del PNRR abbia destinato al digitale oltre il 25% delle risorse totali tra digitalizzazione di PA e imprese, e per il potenziamento delle reti tlc fisse e mobili**, riservando a queste ultime circa 6,7 miliardi[42]. La **nuova Strategia Bul**, che sostituisce quella approvata nel 2015, articola gli interventi in 7 azioni, di cui una, il **Piano "*Italia 5G*"**, completamente dedicata alle reti mobili di quinta generazione. A tale azione sono stati destinati complessivamente **2,02 miliardi di euro**, ripartiti su tre voci principali:

1. la copertura di 10.000 chilometri di strade extraurbane per la realizzazione del *backhauling* in fibra (600 milioni di euro);
2. i corridoi di trasporto europei (420 milioni di euro), con l'obiettivo di incentivare lo

[42] A seguito della ripartizione delle risorse tra le varie componenti della missione alle "*Reti Ultraveloci*", ovvero banda ultra-larga e 5G.

sviluppo di servizi e applicazioni 5G dedicate a sicurezza stradale, mobilità, logistica e turismo;

3. il potenziamento della rete mobile nelle aree a fallimento di mercato, ovvero quelle zone del Paese in cui gli operatori non hanno interesse ad investire, cui è dedicata la maggior parte delle risorse stanziate (1 miliardo di euro).

La consultazione in corso appare dunque fondamentale per far sì che i fondi stanziati attraverso il Piano siano complementari e non sostitutivi rispetto agli interventi in capo agli operatori privati, evitando il c.d. "*effetto spiazzamento*", ovvero l'alterazione con fondi pubblici delle normali dinamiche di investimento degli operatori privati, con una sostituzione dunque dei capitali privati con quelli pubblici.

Per quanto concerne il secondo aspetto, relativo all'impatto economico dei vertical, secondo le stime di GSMA **gli investimenti nelle reti 5G porteranno benefici per l'economia mondiale di circa 2,2 trilioni di dollari** tra il 2024 e il 2034 (Fig.6.20). La crescita maggiore potrebbe interessare gli Stati Uniti (oltre 650 miliardi di dollari), seguiti da Europa (480 miliardi di dollari) e Cina (460 miliardi di dollari). A livello di verticali, la Cina potrebbe ricevere i maggiori benefici da manifattura e utilities (fino a 270 miliardi di dollari) mentre Usa ed Europa vedrebbero crescere i ricavi da servizi professionali e finanziari rispettivamente fino a 250 e 170 miliardi di dollari. Interessante notare inoltre come, a livello di servizi pubblici, l'Europa potrebbe generare benefici fino a 3 volte superiori a quelli della Cina (90 vs 30 miliardi) ma comunque sensibilmente inferiori agli Usa (circa 150 miliardi di dollari).

Una parte rilevante della crescita imputabile al 5G potrebbe essere raggiunta grazie all'utilizzo delle **mmWave (onde millimetriche)** ovvero la porzione di spettro che va dai 24 GHz agli 86 GHz. L'utilizzo di queste frequenze consente di sfruttare canali di comunicazioni molto più ampi rispetto alle bande minori, garantendo quindi maggiori velocità di trasferimento dati e minore latenza. In termini economici, l'utilizzo delle onde millimetriche parteciperebbe a livello globale per 565 miliardi di dollari entro il 2034 (Fig. 6.21). Le applicazioni che si prevede generino il maggior contributo sono l'**automazione industriale**, il **controllo da remoto dei dispositivi** e la **realtà virtuale**, mentre a livello settoriale, le stime indicano che i maggiori benefici dovrebbero

Figura 6.20 Contributo del 5G alla crescita economica globale per area geografica e settore (in miliardi di $, 2034)

Fonte: GSMA, 2020

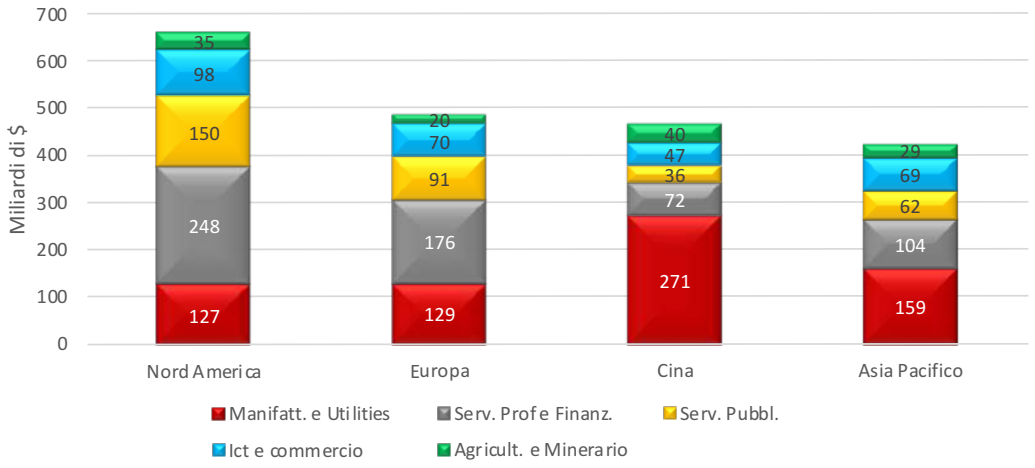


Figura 6.21 Impatto economico dell'utilizzo delle onde mmWave nel 2034 a livello globale (miliardi di $)

Fonte: Elaborazioni I-Com su dati GSMA 2020

provenire **dalla manifattura e dalle utilities** (215 miliardi di dollari), **dai servizi professionali** e finanziari (141 miliardi) e **dai servizi pubblici** (96 miliardi).

Tuttavia, tale orizzonte di lungo termine non deve far pensare che le operazioni non siano urgenti. Secondo la ricerca condotta da Interdigital[43], su 345 professionisti della filiera delle comunicazioni mobili e dei vertical intervistati, **oltre il 70% intende utilizzare applicazioni 5G industriali entro due anni** (Fig. 6.22). In particolare, poco più di una su 10 ne fa già uso (12%), circa un'impresa su 3 le adotterà entro 12 mesi e un ulteriore 28% entro 24 mesi. Solo il **15%**, infine, non prevede di adottare applicazioni industriali 5G da qui a 5 anni. A livello di verticali, il comparto che dovrebbe ricevere i maggiori benefici dalle applicazioni 5G sarà l'**automotive** (sia come prima scelta, con il 24%, sia sul totale delle prime tre, con il 58%), seguito dalla manifattura (46%), media (39%) ed energia & trasporti (37%) (Fig. 6.23).

Per favorire al massimo lo sviluppo dei verticali e il raggiungimento dei benefici auspicati, assumono un'importanza centrale il modello o i modelli di business che prevarranno nell'implementazioni delle nuove applicazioni 5G

[43] Interdigital, *Great Expectations: Sizing the Opportunity for 5G in Vertical Industries*, 2020. Il campione è composto per il 41% da appartenenti ad imprese europee, per il 28,6% nordamericane, per il 21,3% asiatiche, per il 4% mediorientali, per il 3,4% africane e per l'1,4% sudamericane. Rispetto alla appartenenza settoriale, quasi il 20% lavora presso un operatore mobile, poco più del 20% fa capo a fornitori di apparecchiature di rete, il 14% a system integrator e a società di consulenza e quasi il 15% alle industrie verticali (education, servizi finanziari, energia e utilities, media, trasporti e logistica). I restanti provengono dai software vendors (13%), dai produttori di device (8%), da altri tipi di fornitori di prodotti e servizi di rete (5,5%) e dagli operatori virtuali (MVNO, 3,7%).

Figura 6.22 Intenzione di adottare o applicare tecnologie industriali 5G in azienda (% dei rispondenti)

Note: Il campione è composto da 345 professionisti della filiera delle comunicazioni mobili e dei vertical
Fonte: Interdigital, 2020

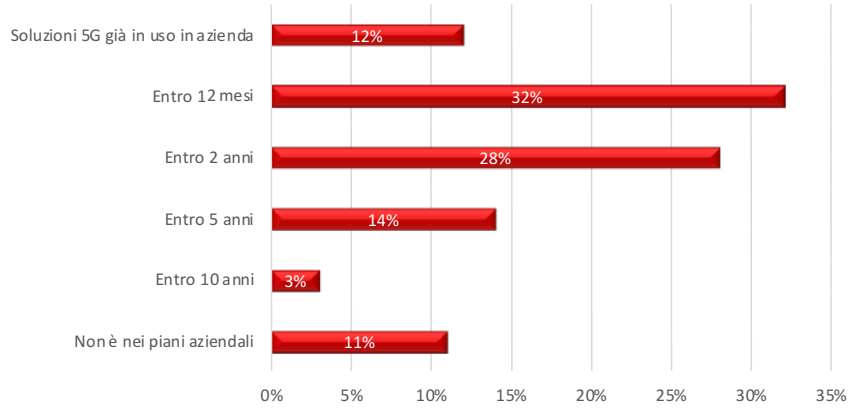
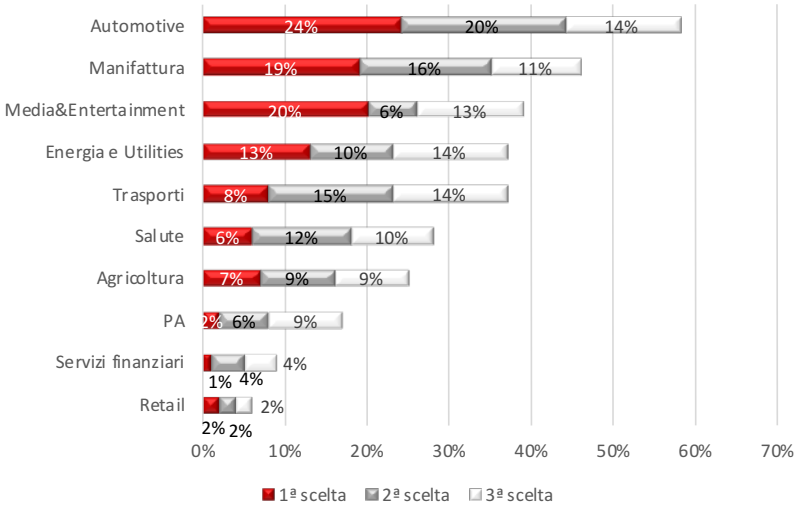


Figura 6.23 Industrie che beneficeranno maggiormente del 5G nei prossimi 2 anni (% dei rispondenti)

Note: Il campione è composto da 345 professionisti della filiera delle comunicazioni mobili e dei vertical
Fonte: Interdigital, 2020

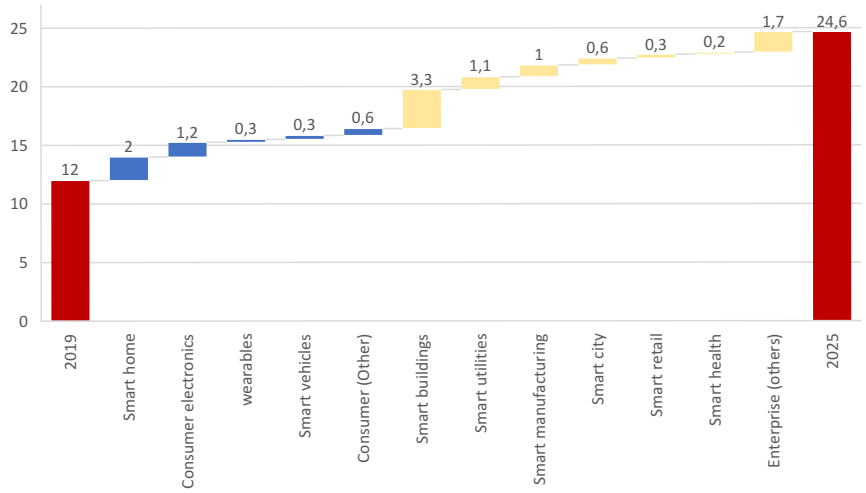


a livello industriale. Infatti, a differenza delle quattro generazioni precedenti, il 5G è dotato di caratteristiche in grado di abilitare catene del valore piuttosto differenti rispetto a quanto avvenuto sin ora nelle reti di seconda, terza e quarta generazione, in cui il servizio era prevalentemente dedicato ai telefoni e alla comunicazione interpersonale (poi divenuti smartphone e connettività mobile). Grazie a peculiarità quali **URLLC**, **mMTC** ed **eMBB**[44], il 5G probabilmente interesserà in misura consistente le industrie verticali, grazie a una massiccia

[44] L'*Ultra-reliable low latency* (URLLC) comporta la capacità di supportare latenze end-to-end a partire da 5 ms, che può scendere fino ad a 1 ms. Il servizio mMTC (*massive Machine Type Communications*) consentirà di gestire in modo economico e affidabile la connessione di miliardi di dispositivi senza sovraccaricare la rete (con il 5G dovrebbe essere possibile gestire fino a 1 milioni di dispositivi per km2). L'*Enhanced Mobile Broadband* (e-MBB) consentirà di supportare un *throughput* estremamente elevato (anche +10Gbps) e una latenza inferiore ai 5 millisecondi, fornendo al tempo stesso servizi affidabili.

Figura 6.24 *Connected device* **a livello mondiale nel 2025 (mld di unità)**

Fonte: GSMA, Mobile Economy Global, 2020



diffusione e potenziamento dell'**Internet of Things** (Fig. 6.24).
Secondo GSMA, entro i prossimi quattro anni il numero di device connessi arriverà a **quota 25 miliardi**, trainati in particolare da quelli di livello enterprise (*smart buildings*, *smart utilities* e *smart manufacturing*).

È verosimile che il modello di gestione della rete passerà dalla focalizzazione su di una copertura il più possibile completa del territorio, con un modello di business quasi interamente B2C, a un nuovo contesto in cui la copertura potrebbe divenire sempre **più localizzata**, destinata a servire imprese o distretti industriali e l'integrazione di reti private aziendali, e con un modello di business primariamente B2B in cui il fattore primario potrebbe consistere nell'affidabilità delle applicazioni. In definitiva, con il 5G le reti potrebbero focalizzarsi decisamente verso lo sviluppo dei maggiori settori industriali e, conseguentemente, il fattore del successo potrebbe divenire sempre più il *know-how* specifico di ogni settore.

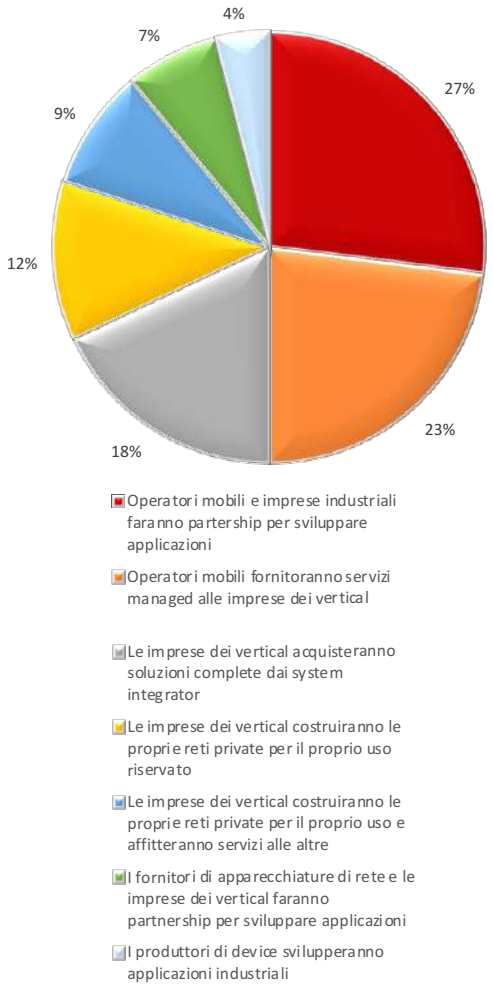
In questo contesto potrebbero emergere diverse soluzioni e modelli di business, che vanno dalla fornitura delle applicazioni industriali da parte degli stessi operatori, da soli o in partnership con terze parti che utilizzano la rete, o con le stesse imprese dei verticali, fino alla creazione e gestione di reti private per le aziende fornite da intermediari o sviluppate in proprio dalle aziende stesse su porzioni di spettro riservato, passando per altre tipologie di modelli ibridi.

A tal proposito, i risultati dell'analisi effettuata da Interdigital indicano che, secondo la metà dei professionisti intervistati, **gli operatori di rete continueranno a ricoprire un ruolo di primo piano**, sviluppando applicazioni in partnership o offrendo servizi *managed* alle imprese verticali (Fig. 6.25). Se per il 18% potrebbero trovare spazio anche i *system integrator*, per quasi 1 su 3 (28%) le imprese dei vertical saranno in prima linea, costruendo reti private per il proprio utilizzo esclusivo, affittandone servizi a terzi e sviluppando applicazioni in partnership con i fornitori di apparecchiature di rete (oltre alle possibilità di partenariato con gli stessi operatori di rete).

Proprio al fine di consentire maggiore flessibilità nella gestione dello spettro e dell'affermazione di nuovi modelli di business, Paesi come Germania e Regno Unito hanno già previsto policy *ad hoc*.

In Germania il regolatore delle reti BNetzA ha riservato 100 MHz di spettro in banda 3.7-3.8 GHz a livello locale per le imprese private, acquistate

Figura 6.25 Possibili modelli di implementazione delle applicazioni industriali 5G
Fonte: Interdigital, 2020



in particolare da BMW, Bosch, Lufthansa, Mercedes, Siemens e Volkswagen[45].
Nel Regno Unito l'Ofcom ha previsto la possibilità di utilizzare licenze per l'accesso locale nelle bande 700 MHz e nella banda 3.6-3.8 GHz, licenze per l'accesso condiviso (shared access licence) nella bande 1800 MHz, 2.4 GHz, 3.8-4.2 GHz e 24.25-26.5 GHz sulla base del principio *first come first served* e un regime di *light licensing* (o *no licensing*) per ulteriori 500 MHz per il Wi-Fi indoor e per l'outdoor a bassa intensità, così come per le banda 100-200 GHz.

In Italia, d'altra parte, lo sviluppo di un modello di offerta (o gestione) localizzato potrebbe incontrare delle difficoltà, in particolare per via di due fattori: l'alto costo di assegnazione dei diritti d'uso delle frequenze 5G raggiunto nel nostro Paese, che potrebbe determinare un problema di costo unitario dello spettro per le imprese che volessero farne richiesta, e la scarsa domanda di servizio dovuta al tessuto industriale italiano che, a differenza ad esempio della Germania, è generalmente costituito da PMI. Di conseguenza, potrebbero rivelarsi necessarie delle **forme di incentivazione della domanda a livello industriale**[46].

A tal proposito, si osserva come un interessante passaggio del PNRR, ripreso anche dalla Strategia per la Banda Ultralarga, sia relativo alla volontà del Governo di sostenere la domanda di connettività 5G attraverso l'erogazione di incentivi per "*l'adozione di servizi e applicazioni 5G, anche a favore dei settori verticali per lo sviluppo di casi d'uso previsti dall'ITU, inclusi i settori pubblici della sanità, scuola, mobilità e sicurezza*".

A ciò si aggiunge la possibilità di mettere a

[45] BMW ha acquistato lo spettro nella banda 3.7-3.8 GHz per lo stabilimento di Lipsia, e sta lavorando insieme Ericsson e Deutsche Telekom per lo sviluppo di soluzioni 5G stand alone. Anche Bosch ha acquisito una licenza locale nella banda 3.7-3.8 GHz e ha iniziato a costruire una rete 5G industriale privata presso la propria fabbrica di semiconduttori a Reutlingen, per testare applicazioni 4.0 insieme a partner quali ABB, Ericsson, Orange e T-Systems. Lufthansa ha acquisito una licenza locale in banda 3.7-3.8 GHz per i propri stabilimenti di Amburgo, mentre Ericsson e Telefónica Germany stanno sviluppando una rete per lo stabilimento della Mercedes a Sindelfingen, che dovrebbe consentirgli di abbattere le emissioni di carbonio e aumentare l'efficienza produttiva dei propri impianti del 25%.

[46] Cfr. l'audizione del Prof. Vatalaro alla Camera nell'ambito dell'esame del PNRR https://www.camera.it/application/xmanager/projects/leg18/attachments/upload_file_doc_acquisiti/pdfs/000/004/939/Commenti_Next_Gen_EU_Vatalaro_.pdf

disposizione ulteriori risorse spettrali non ancora assegnate e favorire la condivisione delle infrastrutture.

In questo senso, appare estremamente interessante anche l'avvio da parte dell'AGCOM dell'indagine conoscitiva su possibili nuove modalità di utilizzo dello spettro radio per favorire lo sviluppo dei verticali, inclusa la possibilità di riservare porzioni di spettro 5G per reti locali e reti private. Questa opportunità è sottolineata in particolare dal **toolbox per la connettività europeo**, pubblicato lo scorso 25 marzo 2021 dal *Connectivity Special Group*. Secondo quanto emerge dal documento, gli Stati membri dovrebbero prendere in considerazione l'opportunità di riservare porzioni di spettro 5G in modalità *local licensing*, con particolare riferimento alle onde millimetriche. Agire in questa direzione potrebbe incentivare lo sviluppo di soluzioni che prevedono l'interazione del 5G con le altre principali tecnologie abilitanti come l'IoT, l'intelligenza artificiale, l'*edge computing*, la robotica e la realtà aumentata, aprendo allo sviluppo di soluzioni industriali per settori chiave come il manifatturiero (rendendo finalmente possibile la creazione di ***smart factory***), l'edilizio, il sanitario, l'agricoltura e la mobilità (in particolare la mobilità connessa e automatizzata). Inoltre, il toolbox incoraggia gli Stati membri ad effettuare una revisione regolare dei propri piani nazionali sullo spettro, con l'obiettivo di identificare la domanda anche in una prospettiva di lungo termine. Per quanto concerne la situazione italiana, parrebbe opportuno avviare le **consultazioni sulle licenze in scadenza**, sia nell'ottica di un allineamento del loro termine (al momento fissato per quasi tutte al 31 dicembre 2029), sia per dare certezza agli investimenti degli operatori, fattore fondamentale per favorire lo sviluppo di servizi concorrenziali e allo stesso tempo sostenibili.

CAPITOLO 7

FINTECH: IL FUTURO DELLA FINANZA È DIGITALE

7.1 LE TENDENZE DEL FINTECH IN ITALIA E NEL MONDO

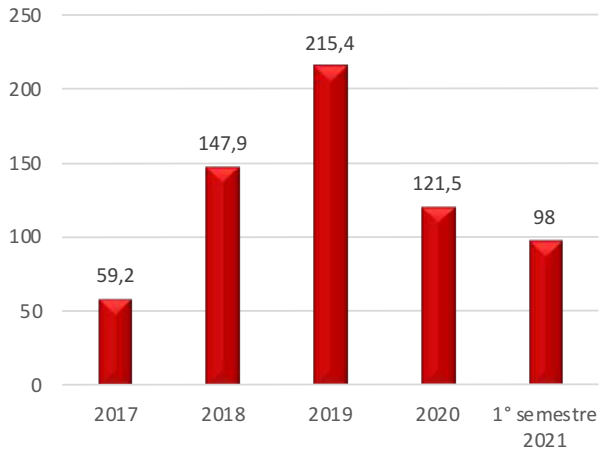
Con il termine «**Fintech**» si indicano genericamente tutte le applicazioni tecnologiche che negli ultimi anni hanno cambiato il modo in cui gli utenti si interfacciano con il mondo bancario e finanziario.

Lo sviluppo tecnologico degli ultimi decenni ha profondamente modificato buona parte delle nostre abitudini quotidiane, tra cui il modo in cui gestiamo le nostre finanze ed effettuiamo pagamenti. Con il passare del tempo gli strumenti che servono a tale scopo sono diventati sempre più complessi, offrendo agli utenti alternative tecnologiche ai mezzi tradizionali, idonee per favorire la velocità, l'efficienza e la tracciabilità delle operazioni. Portali web e app per smartphone stanno infatti rimpiazzando le filiali fisiche degli istituti portando a una profonda trasformazione del settore. Questa rivoluzione coinvolge non solo soggetti bancari e intermediari finanziari ma anche soggetti specializzati in soluzioni tecnologiche, in particolare le aziende che operano nel mondo dei device mobili.

Secondo quanto emerge dai dati contenuti nel rapporto redatto da KPMG dal titolo "*Pulse of Fintech*", **gli investimenti globali in Fintech nei primi sei mesi del 2021 hanno totalizzato 98 miliardi di dollari**. Osservando l'andamento temporale possiamo notare che l'anno d'oro per il Fintech è stato il 2019 quando gli investimenti annuali hanno raggiunto 215 miliardi di dollari (Fig.7.1).

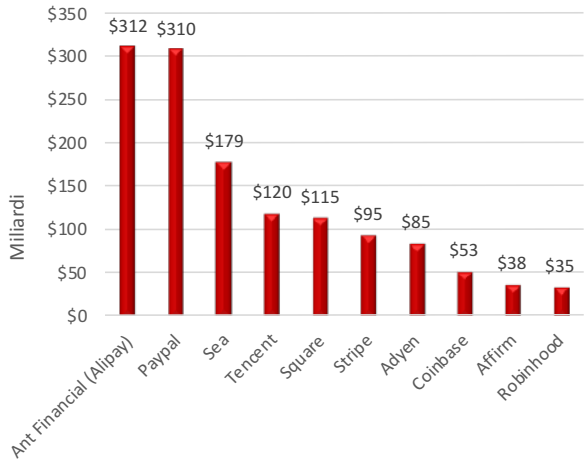
Nel 2020 si assiste invece a un **importante flessione** causata evidentemente dai timori scaturiti dal dilagare della pandemia di Covid-19 che hanno colpito duramente anche i mercati finanziari. **I primi sei mesi dell'anno in corso segnano un'importantissima ripresa degli investimenti nel settore** che hanno quasi raggiunto il valore annuale del 2020 e triplicato il capitale investito nello stesso periodo dell'anno precedente (34,4 miliardi di dollari).

Figura 7.1 Investimenti globali in Fintech ($ miliardi)
Fonte: KPMG



Il Centre for Finance, Technology and Entrepreneurship effettua un monitoraggio continuo della capitalizzazione delle principali società fintech al mondo: in base ai dati estratti l'8 ottobre 2021 **le prime dieci società del settore a livello globale hanno un valore superiore a 1,34 trilioni di dollari** (Fig.7.2). Interessante è inoltre notare che la classifica è dominata da compagnie statunitensi, che rappresentano la metà del totale a livello numerico e, con 550 miliardi, cubano il

Figura 7.2 Top 10 aziende fintech per capitalizzazione a livello globale (13 ottobre 2021)
Fonte: Elaborazioni I-Com su dati del Centre for Finance, Technology and Entrepreneurship

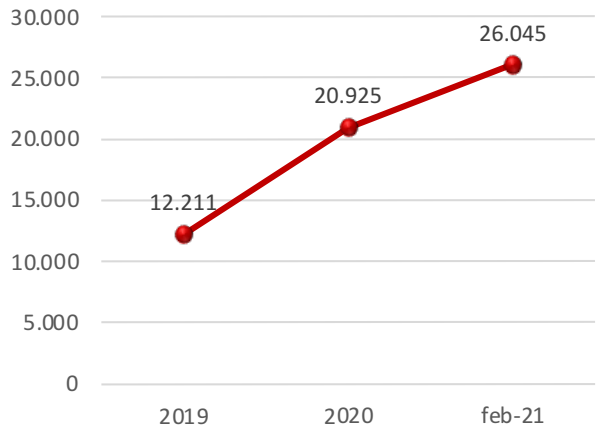


41% della capitalizzazione delle top dieci. Al secondo posto per volume economico troviamo la Cina che, anche se rappresentata da sole due società (Ant Financial e Tencent), ha una capitalizzazione di mercato superiore ai 432 miliardi. L'Europa a sua volta trova posto tra le top dieci con due rappresentanti, Stripe e Adyen, il cui valore del capitale è però notevolmente inferiore ai competitor americani e asiatici (179,9 miliardi).

Il numero di società che si occupano di fintech è comunque in continuo aumento, tanto che neppure l'insorgere della crisi pandemica ha frenato eccessivamente la crescita esponenziale del settore. Secondo gli ultimi dati (Fig.7.3) diffusi dalla Fintech Control Tower, un framework di ricerca sviluppato congiuntamente da Boston Consulting Group ed Expand Research che studia iniziative, tecnologie e aziende in ambito finanza digitale a livello globale, le **start-up fintech sono più che raddoppiate nel corso di 26 mesi** (da gennaio 2019 a febbraio 2021).

Figura 7.3 Numero di start-up fintech a livello globale

Fonte: Boston Consulting Group ed Expand Research

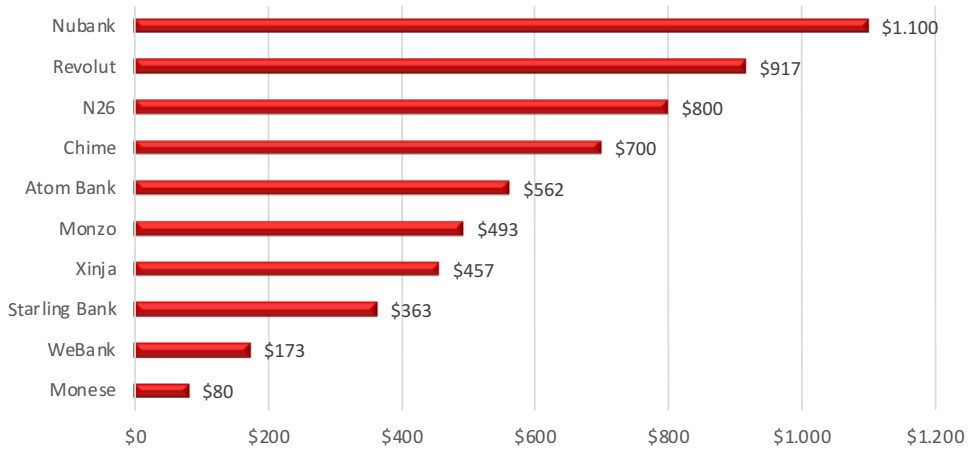


La *digital transformation* sta coinvolgendo profondamente anche il mondo bancario. Negli ultimi anni accanto agli istituti di credito tradizionali, che hanno avviato un processo di digitalizzazione della maggior parte delle proprie attività cercando di offrire ai propri clienti un'esperienza *omnichannel*, sono nate le cosiddette ***digital bank***, ovvero banche che non hanno una presenza fisica sul territorio ma operano esclusivamente sui canali digitali. Secondo gli ultimi dati diffusi da FinTech Magazine, relativi ad ottobre 2020, le dieci principali banche digitali al mondo hanno raccolto complessivamente capitali per oltre 5,6 miliardi di dollari (Fig.7.4). A primeggiare, con circa 1,1 miliardi, è la brasiliana Nubank, seguita dalla britannica Revolut (917 milioni) e dalla tedesca N26 (800 milioni).

La digitalizzazione non sta cambiando esclusivamente le modalità tramite cui le banche

Figura 7.4 Top 10 banche digitali a livello globale per capitale raccolto ($ milioni, ottobre 2020)

Fonte: FinTech Magazine



offrono servizi ai propri clienti ma anche il modo in cui gli stessi si approcciano al mondo finanziario. Uno dei fenomeni più interessanti che si sono sviluppati negli ultimi anni riguardano le nuove modalità di investimento online, e in particolare il ***crowdfunding*** e il ***crowdinvesting*** (o *equity crowdfunding*).

Nel crowdfunding gli utenti della rete partecipano tramite un finanziamento collettivo allo sviluppo di un prodotto o di un servizio ricevendo come ricompensa il bene stesso per cui si è contribuito allo sviluppo. Il crowdinvesting è un'evoluzione del crowdfunding in cui il finanziamento collettivo serve a costituire una nuova società per il quale si riceve in ricompensa una partecipazione nella società stessa. La particolarità di queste nuove forme di investimento è che si svolgono completamente tramite canali digitali **senza l'ausilio di intermediari finanziari**. Chi intende avviare una campagna di raccolta fondi posta la propria idea su una delle numerose piattaforme specializzate e richiede direttamente agli utenti del web di supportare il proprio progetto tramite l'investimento di somme di modesta entità.

I dati contenuti nel rapporto Statista Digital Market Outlook 2021 mostrano come i fenomeni del crowdfunding e del crowdinvesting siano cresciuti esponenzialmente negli ultimi 5 anni passando dai poco meno di 4 miliardi di dollari raccolti a livello globale nel 2017 agli oltre 7,7 miliardi previsti per il 2021 (Fig.7.5).

Un altro fenomeno che mostra come la rivoluzione digitale stia mutando le modalità di approccio alla finanza degli individui è quello dei **Robo-Advisors**, ovvero software che gestiscono i portafogli tramite algoritmi configurati individualmente. Il monitoraggio e le decisioni su come allocare i capitali, in un ristretto range di possibili scelte, vengono quindi effettuati da un sistema automatizzato e non dall'utente o da un consulente umano. Tra il 2018 e il 2021, il valore degli asset gestiti a livello globale da Robot-Advisors è quasi triplicato, passando da 521 a 1.427 miliardi di dollari (Fig.7.6).

Focalizzando l'attenzione sull'Italia, l'ultimo studio condotto dal Politecnico di Milano, in collaborazione con Nielsen, ha fotografato un mercato in forte crescita. **Nel corso del 2019, il 29% della popolazione italiana tra i 18 e i 74 anni, circa 12,7 milioni di individui, ha utilizzato almeno una volta un servizio finanziario digitale**. Particolarmente attratti da questo tipo di servizi sono i giovani tra i 18 e 24: l'89% degli individui in questa fascia di età ha familiarità con i sistemi di

Figura 7.5 Fondi raccolti tramite campagne di crowdfunding e crowdinvesting a livello globale ($ milioni)

Fonte: Statista Digital Market Outlook 2021
* dati previsionali

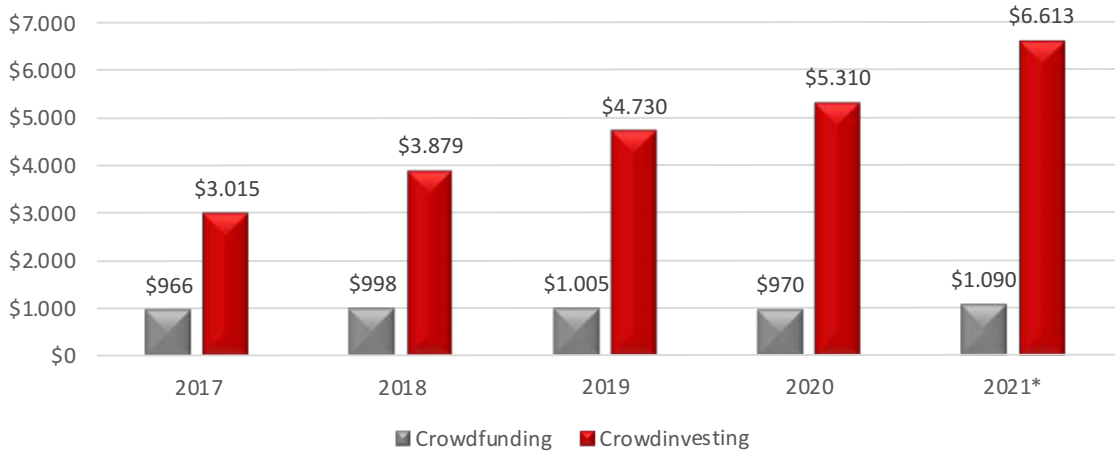
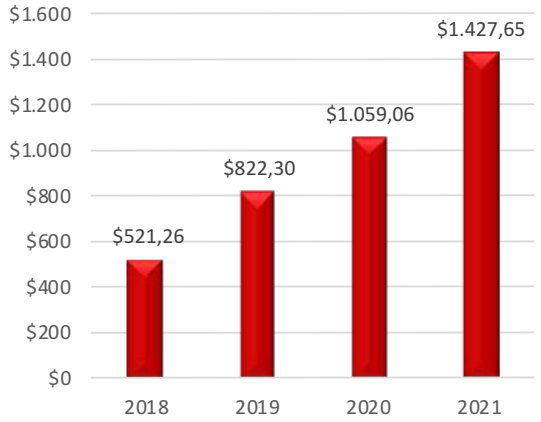


Figura 7.6 Fondi raccolti tramite campagne di crowdfunding e crowdinvesting a livello globale ($ milioni)

Fonte: Statista Digital Market Outlook 2021
* dati previsionali



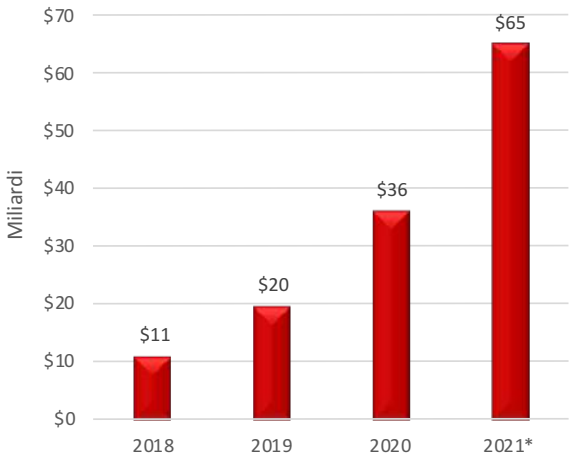
Fintech in circolazione e il 72% ne utilizza almeno uno. I servizi tecnologici maggiormente conosciuti e utilizzati dagli italiani sono le piattaforme online degli istituti di credito e delle assicurazioni (68%) e le applicazioni per smartphone (62%).

Dagli ultimi dati diffusi da Statista emerge come il valore delle transazioni effettuate tramite banche digitali in Italia abbia subito una crescita continua negli ultimi anni e in particolare nell'ultimo biennio (Fig.7.7).

Contestualmente al valore delle transazioni è aumentato in maniera esponenziale anche il

Figura 7.7 Valore delle transazioni effettuate tramite banche digitali in Italia

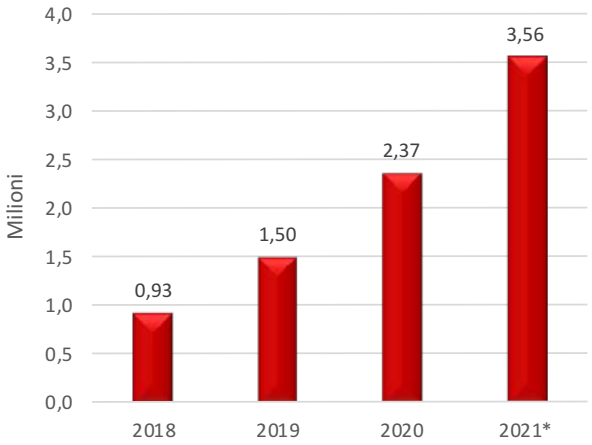
Fonte: Statista Digital Market Outlook 2021
* stime



numero di italiani che scelgono di depositare i propri soldi sulle *digital bank*. Nonostante la tendenza ad avvicinarsi al mondo delle banche digitali fosse evidente anche prima della pandemia, dopo la diffusione del Covid-19 tale fenomeno, probabilmente anche a causa delle limitazioni alla circolazione e al funzionamento contingentato delle filiali bancarie, è esploso portando nel 2020 il numero di clienti italiani a 2,37 milioni, con un'ulteriore crescita del 33% prevista per il 2021 (Fig.7.8).

Figura 7.8 Clienti di banche digitali in Italia

Fonte: Statista Digital Market Outlook 2021
* stime



L'interessamento degli italiani verso le nuove tecnologie legate al mondo della finanza traspare anche dai dati riguardanti l'utilizzo di sistemi di Robo-Advisor. Nel 2020 il numero di utenti che lasciavano gestire almeno parte dei propri risparmi in maniera automatizzata da un software ha superato il milione (Fig.7.9). È inoltre molto interessante notare come l'utilizzo di questi nuovi sistemi di investimento non sia di pertinenza esclusiva dei giovani. Dall'analisi emerge come vi sia un sostanziale equilibro tra le varie fasce di età (Fig.7.10).

I più propensi a utilizzare i Robo-Advisor sono gli individui che vanno dai 35 ai 44 anni (24%), seguiti a brevissima distanza dai 45-54 anni (23%). La classe di età più anziana, ovvero quella che va dai 55 ai 64 anni, pur detenendo la quota più bassa sul totale, rappresenta il 15% di utilizzatori di sistemi di investimento automatizzati.

Figura 7.9 Utilizzatori di Robo-Advisor in Italia

Fonte: Statista Digital Market Outlook 2021
* dati previsionali

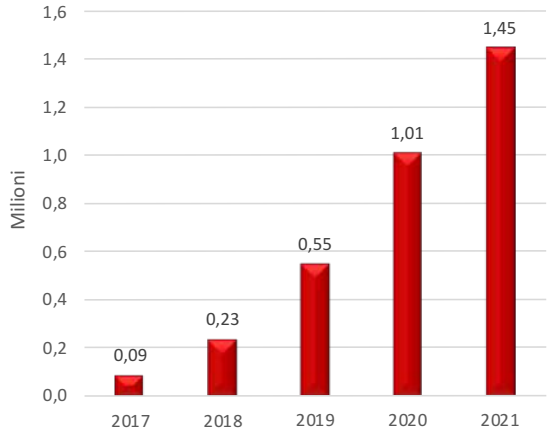
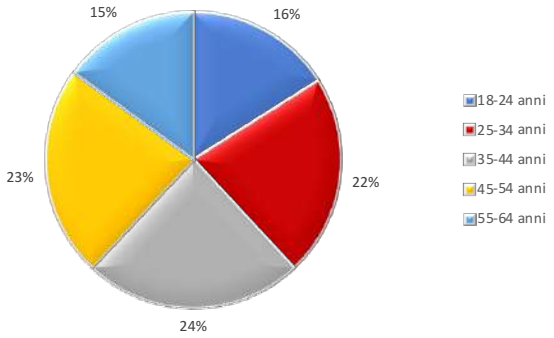


Figura 7.10 Classi di età utilizzatori di Robo-Advisor in Italia (2021)

Fonte: Statista Digital Market Outlook 2021



7.2 I PAGAMENTI ELETTRONICI IN ITALIA NELL'ERA DELLA PANDEMIA

I sistemi di pagamento sono da sempre una parte fondamentale ed estremamente delicata delle attività di scambio tra tutti i tipi di soggetti pubblici e privati. Con il passare del tempo gli strumenti che servono a tale scopo sono diventati sempre più complessi, offrendo agli utenti alternative tecnologiche ai mezzi tradizionali, idonee per favorire la velocità, l'efficienza e la tracciabilità della transazione. Questa rivoluzione coinvolge non solo soggetti bancari e intermediari finanziari ma anche soggetti specializzati in soluzioni tecnologiche, in particolare le aziende che operano nel mondo dei device mobili.

Lo sviluppo tecnologico degli ultimi decenni ha profondamente modificato buona parte delle nostre abitudini quotidiane, tra cui il modo in cui effettuiamo pagamenti. Sistemi di pagamento alternativi al contante sono infatti ormai in circolazione dagli anni Cinquanta, ma con l'avvento della digitalizzazione si sono moltiplicati esponenzialmente. Gli strumenti attualmente in uso possono essere ricondotti a due categorie generali ovvero i "*Sistemi di pagamento elettronici tradizionali*" e i "*New digital payments*". Dei sistemi tradizionali fanno parte le carte di credito e di debito con pagamento tramite POS, i bonifici bancari effettuati presso le filiali e i trasferimenti di valuta operati presso negozi fisici. I *new digital payments* racchiudono invece tutti i nuovi strumenti di pagamento che si sono sviluppati soprattutto grazie alla crescita dell'*e-commerce* e alla diffusione capillare degli smartphone e si dividono a loro volta in tre categorie:

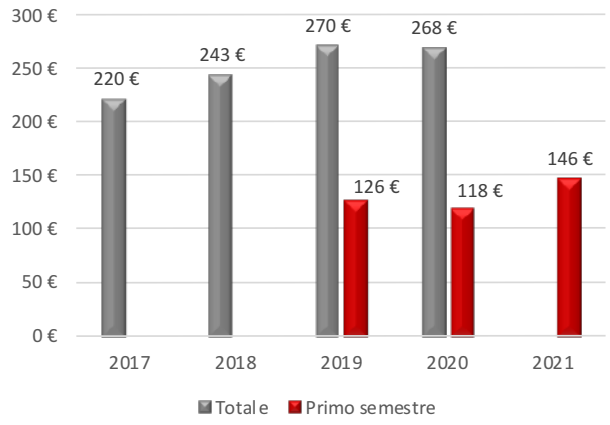
- mobile payments
- electronic payments
- contactless payments.

Nei ***mobile payments*** rientrano tutte le tipologie di pagamento che utilizzano dispositivi mobili - come smartphone, tablet e smart watch - per poter acquistare o vendere beni e servizi, abilitando trasferimenti di moneta elettronica tramite una rete di telecomunicazione mobile. Fanno parte di questa categoria sia gli acquisti a distanza (*mobile remote payment*), sia il pagamento di prossimità (*mobile proximity payment*). Questi ultimi si basano principalmente sulla **tecnologia NFC (Near Field Communication)**, che permette una comunicazione bidirezionale tra *initiator* e *target* (ovvero chi esegue la connessione e chi la riceve) quando questi vengono accostati in un raggio di 4 centimetri. Per **electronic payments** invece intendiamo tutti i sistemi che permettono di

effettuare pagamenti da remoto sui portali di *e-commerce*. In questo tipo di operazioni possiamo inviare le nostre informazioni di pagamento (ad esempio il numero di carta di credito) direttamente al venditore oppure utilizzare i cosiddetti ***e-wallet*** (o portafogli elettronici). Questi sistemi si pongono da intermediario tra il cliente e il venditore permettendo a chi acquista di effettuare la transazione più velocemente senza dover inserire le proprie informazioni a ogni operazione. Di questa categoria fanno parte sia portali specializzati come PayPal o Satispay, sia servizi offerti da giganti della tecnologia come Apple Pay e Google Pay. Per ***contactless payments*** si intendono invece tutti quei sistemi di pagamento che utilizzano particolari strumenti elettronici forniti di tecnologia **RFID (Radio Frequency Identification)** in grado di effettuare il pagamento senza utilizzare contatto diretto o inserimento.

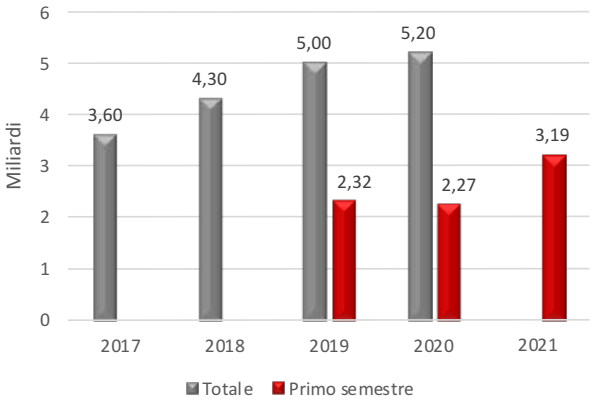
Il mercato dei pagamenti digitali è da alcuni anni in crescita in tutto il mondo e l'Italia non fa eccezione. Secondo gli ultimi dati diffusi dall'Osservatorio Innovative payments del Politecnico di Milano, nel 2020 in Italia i pagamenti digitali hanno transato 268 miliardi di euro, con una lieve decrescita (-2 miliardi) rispetto all'anno precedente (Fig.7.11). Il dato, anche se negativo, è comunque estremamente incoraggiante visti i 123 miliardi di euro di consumi totali persi nel 2020 a causa della crisi pandemica. Nel primo semestre del 2021 i pagamenti digitali nella penisola si sono assestati sui 146 miliardi, in netta crescita rispetto allo stesso periodo sia del 2020 (+19%) che del 2019 (+14%). Considerando che storicamente il secondo semestre è quello in cui si registrano i consumi maggiori e che all'inizio dell'anno in corso erano ancora in vigore forti restrizioni per il contenimento dei contagi, entro la fine del 2021, secondo le previsioni del Politecnico, **i pagamenti digitali potrebbero raggiungere quota 311 miliardi di euro**.

Figura 7.11 Pagamenti digitali in Italia per valore transato (miliardi di €)
Fonte: Osservatorio Innovative payments



Osservando il dato sul numero delle transazioni effettuate è evidente che la pandemia, più che ostacolare, ha stimolato l'utilizzo di sistemi di pagamento digitale, che infatti sono cresciuti anche nel 2020 (Fig.7.12).

Figura 7.12 Pagamenti digitali in Italia per numero di transazioni
Fonte: Osservatorio Innovative payments



Una forte crescita si è registrata anche nell'utilizzo dei sistemi di pagamento più innovativi come il *contactless* e i ***mobile*** e ***wearable payments*** (Fig.7.13). Il valore dei pagamenti senza contatto effettuati nei negozi fisici nel primo semestre 2021 (52,1 miliardi di euro) sono stati quasi il doppio di quelli registrati nel 2019 (27,2 miliardi) e circa il 40% in più rispetto al 2020 (31,4 miliardi). Per quanto riguarda i *mobile* e i *wearable payments*, anche se in valori assoluti i pagamenti nel 2021

Figura 7.13 Pagamenti effettuati in negozio tramite sistemi innovativi per valore transato (miliardi di €)

Fonte: Osservatorio Innovative payments

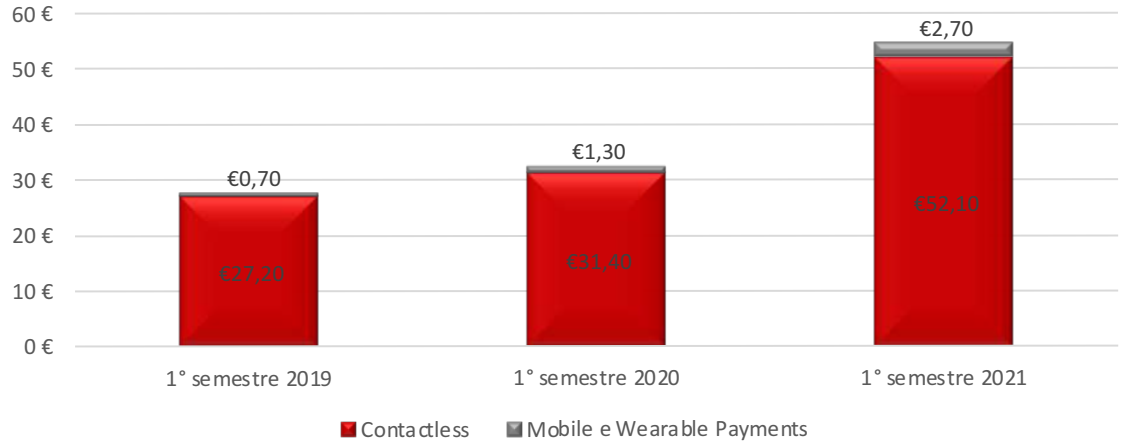
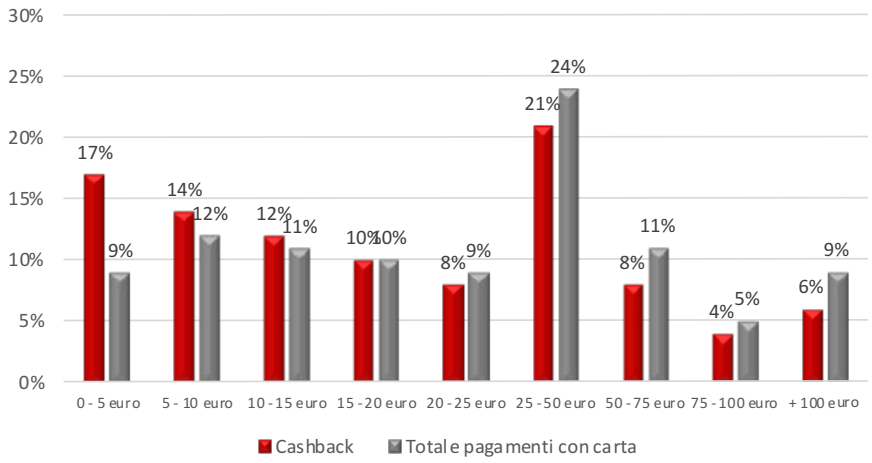


Figura 7.14 Distribuzione percentuale delle transazioni con carta per classi di importo effettuate dagli aderenti al cashback rispetto al totale (2021)

Fonte: Osservatorio Innovative payments



hanno raggiunto solo 2,7 miliardi di euro, è importante sottolineare una crescita del 52% rispetto all'anno precedente e del 74 rispetto al 2019.

Parlando di pagamenti digitali, una menzione particolare è dovuta alla principale iniziativa adottata dal Governo italiano per incentivare il passaggio dal contante a forme di pagamento di nuova generazione, ovvero il ***cashback***. Questa misura, insieme alla lotteria degli scontrini e all'abbassamento del limite di utilizzo del contante, è parte integrante del **Piano Italia Cashless**, ovvero la programmazione governativa tesa a promuovere l'uso di carte e app di pagamento, al fine di modernizzare il Paese e favorire lo sviluppo di un sistema più digitale, veloce, semplice e trasparente. Secondo i dati raccolti dall'Osservatorio Innovative payments, i cittadini che hanno aderito al *cashback* sono stati 8,49 milioni, ovvero il 18% della popolazione, di cui l'88% con almeno una transazione valida effettuata. Le operazioni totali elaborate dal sistema sono state oltre 759 milioni e hanno permesso a 6,11 milioni di cittadini italiani (il 77% degli utenti attivi) di ricevere il contributo del 10% previsto dalla misura. Molto utile per valutare gli effetti che ha avuto la misura sullo stimolare la

cittadinanza a utilizzare maggiormente le carte e i nuovi sistemi di pagamento è l'analisi della distribuzione percentuale delle transazioni con carta per classi di importo (Fig.7.14).

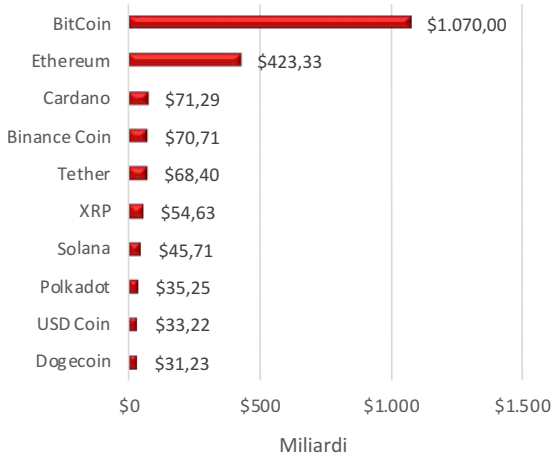
Confrontando le transazioni effettuate con carte degli aderenti al *cashback* rispetto al resto della popolazione è evidente come gli aderenti alla misura siano stati molto più propensi a non utilizzare il contante anche nelle transazioni di scarsa entità. Se osserviamo infatti la prima classe di importi, ovvero quella che va da 0 a 5 euro, possiamo notare come queste transazioni rappresentino il 17% del totale effettuato dagli aderenti al *cashback* contro il 9% della popolazione totale.

7.3 IL FUTURO DELLA MONETA: LE CRIPTOVALUTE ISTITUZIONALI E COMMERCIALI

La storia delle criptovalute è iniziata poco più di dieci anni fa, nel 2009, quando una o più persone operanti sotto lo pseudonimo di **Satoshi Nakamoto** hanno creato il primo esempio di moneta di questo tipo, ovvero il **BitCoin**. Da allora l'ecosistema delle *criptocurrency* è cresciuto in maniera esponenziale arrivando, alla data dell'11 ottobre 2021, a essere popolato da 6.823 valute per una capitalizzazione totale di oltre 2.343 miliardi di dollari. Nonostante il numero di monete digitali sia estremamente elevato, la maggior parte di esse ha un valore pressoché inesistente. Se osserviamo infatti le prime dieci criptovalute per capitalizzazione (Fig.7.15) possiamo notare come insieme cubino l'81% dell'intero indotto (1.903 miliardi).

Le criptovalute basano il proprio funzionamento su un registro digitale distribuito detto *blockchain* che funge da archivio delle transazioni effettuate tra gli utenti che decidono di entrare a far parte del sistema. L'aspetto distintivo di questa tecnologia è il non essere subordinata al controllo di una o più autorità di centrali, ma di basare il

Figura 7.15 Prime 10 criptovalute per capitalizzazione (dati estratti l'11 ottobre 2021)
Fonte: Investing.com



proprio funzionamento sul rapporto di fiducia che si instaura tra gli utenti stessi della rete. La mancanza di un'autorità centrale, se da una parte rende il sistema più libero e democratico,dall'altro espone le criptovalute ad un'eccessiva **volatilità**, infatti, la mancanza di un soggetto in grado di intervenire, ad esempio attivando azioni utili a calmierare le oscillazioni, di fatto lascia l'andamento della moneta completamente in balìa delle dinamiche di mercato. Questo rende le criptovalute più simili a uno strumento speculativo che a una riserva di valore. Osservando l'andamento del BitCoin negli ultimi 10 anni (Fig.7.16) risulta evidente come il valore della criptovaluta sia caratterizzato da una volatilità estrema. Nel solo periodo che va dall'11 ottobre 2020 allo stesso giorno del 2021 si sono palesate variazioni giornaliere sia positive che negative fino al 19%.

Nonostante questa criticità, numerosi Paesi stanno guardando con interesse al mondo delle criptovalute. Ad esempio, lo Stato centramericano di **El Salvador** è stato il primo a scegliere di utilizzare il BitCoin come valuta di corso legale. Dal 7 settembre 2021, tutti gli operatori economici del Paese sono tenuti ad accettare la criptovaluta e i prezzi di prodotti e servizi devono essere obbligatoriamente espressi sia in dollari che in

Figura 7.16 Andamento valore giornaliero BitCoin in dollari (11/10/2010 – 11/10/2021)

Fonte: Investing.com

Bitcoin. Il governo salvadoregno ha acquistato in prima istanza 400 BitCoin per un esborso totale di circa di 20,7 milioni di dollari. Purtroppo, questa prima esperienza non è partita nel migliore dei modi: dalla data ufficiale dell'insediamento del BitCoin come valuta di Stato la criptovaluta ha subito un crollo di mercato che l'ha portata a perdere oltre il 10%. Il caso di El Salvador è estremamente interessante per comprendere l'effetto che può avere l'adozione di una criptovaluta commerciale come valuta di corso legale di un Paese. Nonostante la perdita di valore iniziale, è infatti difficile predire quale impatto avrà sull'economia del Paese l'adozione del BitCoin. Il passaggio alla criptovaluta, oltre ai palesi effetti negativi, potrebbe stimolare l'ingresso di nuovi capitali nel Paese e abbattere i costi di transizione dei circa 6 miliardi di dollari di rimesse che ogni anno gli emigrati rimandano a casa (circa il 22% del Pil salvadoregno). Una vera valutazione potrà essere fatta solo nel medio termine quando, superata una fase di stabilizzazione, il Paese comincerà ad assimilare veramente questa nuova moneta e a sperimentarne gli effetti.

Se l'utilizzo di una criptovaluta commerciale come moneta corrente sembrerebbe essere ad oggi eccessivamente rischioso per l'economia di un Paese, numerosi Stati stanno cominciando a studiare la possibilità di emettere una criptovaluta di Stato. La Banca centrale europea, ad esempio, ha avviato un piano di lavoro della durata di 24 mesi utile a verificare la fattibilità dell'introduzione di una versione digitale dell'euro.

Il Paese che attualmente è più avanti su questo tema e ha già iniziato la sperimentazione della propria moneta digitale è la Cina. Come noto, qui la diffusione dei sistemi di pagamento digitale è già molto elevata, e nelle principali città del Paese i pagamenti sono quasi esclusivamente elettronici, con parte degli esercizi commerciali che già non accetta più denaro contante (anche se espressamente previsto dalla legge). Secondo il China Internet Network Information Center, nel 2020 il numero di cittadini cinesi che utilizzano sistemi di *mobile payments* ha raggiunto gli 852 milioni, ovvero il 61% della popolazione. La sperimentazione dello **yuan digitale**, comunemente conosciuto come **DC/EP (Digital Currency Electronic Payment)**, è stata avviata dalla Banca Centrale Cinese a partire dal mese di aprile del 2021 in 4 città: Shenzhen, Chengdu, Suzhou e Xiongan. Il funzionamento della valuta è basato su blockchain e, a differenza degli altri sistemi di pagamento elettronico, è utilizzabile

anche in assenza di connessione a Internet. Al fine di incentivarne un utilizzo locale (la moneta è infatti nella fase iniziale interdetta agli stranieri), il Governo ha deciso di indire una lotteria che ha assegnato 200 yuan digitali a 50.000 cittadini, per un montepremi totale di 10 milioni (equivalenti a circa 1,5 milioni di dollari). In totale verranno messi in circolazione 40 milioni di DC/EP, tramite i quali i possessori potranno acquistare beni e servizi in tutti gli esercizi commerciali fisici e presso gli *e-shop* abilitati (in un primo momento 10.000 ma aumenteranno progressivamente) utilizzando un'apposita app. La fase di test dovrebbe comunque completarsi entro il 2023 per poi vedere il lancio ufficiale della moneta in tutto il Paese tra il 2024 e il 2025.

CAPITOLO 8

LA STRATEGIA ITALIANA PER LE TECNOLOGIE EMERGENTI

8.1 INTELLIGENZA ARTIFICIALE

L'**intelligenza artificiale (IA)** continua ad affermarsi, a livello mondiale, come tecnologia chiave e nemmeno la pandemia ne ha arrestato l'avanzata.

Secondo l'ultimo aggiornamento di IDC (International Data Corporation)[47] i ricavi mondiali per il mercato dell'intelligenza artificiale (IA), inclusi software, hardware e servizi, sono stimati in crescita del **15,2% nel 2021** arrivando a sfiorare i 342 miliardi di dollari. Si prevede che il mercato accelererà ulteriormente nel 2022 con una crescita del 18,8% e rimarrà su un andamento positivo per superare la soglia dei 500 miliardi di dollari entro il 2024 (Fig. 8.1). Tra le tre categorie tecnologiche, quella Software ha occupato l'88% del mercato complessivo dell'IA. Tuttavia, in termini di crescita, si stima che l'Hardware crescerà più velocemente nei prossimi anni. Dal 2023 in poi, si prevede che AI Services diventerà la categoria in più rapida crescita.

Anche il mercato italiano dell'IA ha mostrato resilienza durante l'emergenza sanitaria e l'interesse verso queste tecnologie è aumentato come nel resto d'Europa e tanti sono stati i progetti e le iniziative IA implementate in Italia per affrontare la crisi Covid-19.

Soluzioni IA sono state pensate non solo per la diagnosi e predizione degli sviluppi clinici della malattia causata da SARS-CoV-2, oppure per la ricerca in ambito farmaceutico ma anche per combattere la disinformazione su Covid-19, oppure nel marketing per migliorare la customer engagement durante la pandemia e continuare a garantire esperienze e comunicazioni efficaci secondo le aspettative degli utenti.

Tuttavia, già prima della pandemia erano note le **grandi potenzialità** di impiego dell'IA e tante sono ormai le imprese italiane che considerano l'IA un'opportunità da cogliere per migliorare qualsiasi aspetto del proprio business, dai processi di produzione alla relazione con la clientela. Pertanto si evidenzia un maggior livello di diffusione delle soluzioni intelligenti nelle diverse realtà organizzative del nostro Paese. Sempre più aziende italiane utilizzano tecnologie IA o avviano progetti di sperimentazione, studi di fattibilità e approfondimenti per individuare metodi di applicazione e skill necessari per il

Figura 8.1 Ricavi mondiali per il mercato dell'IA (valori stimati, miliardi di $)

Fonte: IDC (2021)

[47] IDC (2021)
https://www.idc.com/getdoc.jsp?containerId=prUS48127321#:~:text=NEEDHAM%2C%20Mass.%2C%20August%204,Corporation%20(IDC)%20Worldwide%20Semiannual%20Artificial

lancio di attività in quest'area. Dallo studio "*Il digitale in Italia 2021*" a cura di Anitec-Assinform e Confindustria Digitale[48] emerge un aspetto molto interessante che riguarda il numero crescente di aziende appartenenti ai settori non ICT che cominciano a entrare nei nuovi scenari abilitati dall'innovazione digitale specie dall'intelligenza artificiale.

Questo interesse, si può dire oramai consolidato, è testimoniato anche dalla crescita del mercato che nel 2020 ha registrato un incremento del 15% rispetto al 2019 e raggiunto un valore di 300 milioni di euro, di cui il 77% commissionato da imprese italiane (230 milioni) e il 23% come export di progetti (70 milioni). A trainare il mercato è soprattutto la componente dei software, che vale il 62%, seguita dai servizi e marginalmente dalla componente hardware[49].

Invece, i progetti e le applicazioni IA che attirano maggiori investimenti sono gli **algoritmi per analizzare ed estrarre informazioni dai dati** (*Intelligent Data Processing*), che coprono il 33% della spesa, seguiti dalle **soluzioni per l'interpretazione del linguaggio naturale** (*Natural Language Processing*) e gli **algoritmi per suggerire ai clienti contenuti in linea con le singole preferenze** (*Recommendation System*) che coprono rispettivamente il 18% del mercato. I chatbot e i *virtual assistant* pur raggiungendo insieme il 20% degli investimenti, rientrano tra le iniziative che sono cresciute di più in termini di risorse (+28%) (Fig. 8.2).

Tra i settori, infine, più attivi in termini di investimenti in IA rientrano quello **finanziario** (23%), seguito da **energia/utility** (14%), **manifattura** (13%), **telco e media** (12%) e **assicurazioni** (11%) (Fig. 8.3)[50].

Il settore dell'intelligenza artificiale è, dunque, in continuo fermento ed è chiaro ormai che non bisogna perdere occasione di investire su questa nuova frontiera tecnologica, che rappresenta una leva fondamentale per accelerare la crescita digitale dell'Italia con benefici che, oltre a riguardare il mondo industriale, interessano la società nel suo complesso.

Sicuramente le risorse del Piano Nazionale di Ripresa e Resilienza (PNRR) che ammontano a 191,5 miliardi di euro sommate a quelle rese disponibili dal REACT-EU nonché a quelle

Figura 8.2 I progetti IA che attirano più investimenti in Italia

Fonte: Osservatori.net Politecnico di Milano, School of Management

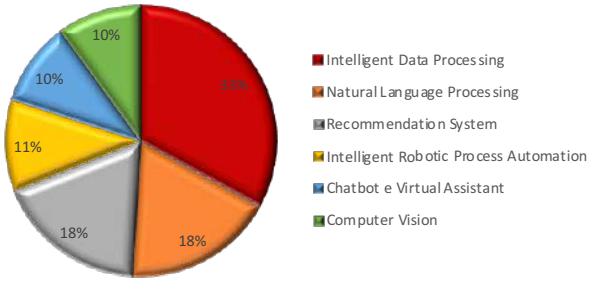
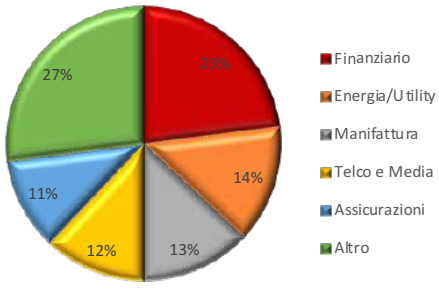


Figura 8.3 Investimenti in IA, per settore (2020)

Fonte: Osservatori.net Politecnico di Milano, School of Management



[48] Anitec-Assinform, IL DIGITALE IN ITALIA 2021. Mercati, Dinamiche, Policy, Luglio 2021 - https://ildigitaleinitalia.it/il-digitale-in-italia-2019/il-digitale-in-italia-2021.kl

[49] https://blog.osservatori.net/it_it/artificial-intelligence-italia-mercato-progetti-tecnologie

[50] *Ibidem*

derivanti dalla programmazione nazionale aggiuntiva, rappresentano un'occasione irripetibile per giocare la partita sull'intelligenza artificiale e sulle altre tecnologie emergenti (cloud, blockchain, 5G), ossia fattori imprescindibili per rilanciare il Paese e migliorare radicalmente la competitività della nostra economia.

Tuttavia, nel PNRR[51] si parla poco di intelligenza artificiale, se non altro come strumento utile a migliorare la qualità e l'efficacia della PA, e sembra dunque mancare una chiara strategia adeguatamente finanziata, che indichi come il Paese intenda sfruttarne le potenzialità a 360° per ripartire nella fase post-Covid.

Eppure, l'intelligenza artificiale avrebbe dovuto essere la pietra angolare su cui fondare la ripartenza del Paese, grazie anche alle numerose iniziative contenute nella bozza di **Strategia Nazionale per l'Intelligenza Artificiale**[52], elaborata dal ministero dello Sviluppo economico, tuttavia mai finalizzata e dunque attuata.
Tra le iniziative principali si ricordano il rafforzamento delle competenze manageriali, il sostegno alla collaborazione tra imprese attraverso incentivi finanziari ad hoc, il rifinanziamento dei centri di competenza e la promozione di forme di sperimentazione con strumenti ad hoc.

Su questo lavoro preesistente, si innesta il gruppo di lavoro di nove esperti designati dal Ministero dell'Università e della Ricerca, dal Ministero dello Sviluppo economico e dal Ministero per l'Innovazione tecnologica e la Transizione digitale, chiamati ad aggiornare la strategia nazionale sull'intelligenza artificiale per renderla coerente con il Piano Nazionale di Ripresa e Resilienza e gli sviluppi più recenti a livello UE[53].

Sicuramente per spingere di più sull'intelligenza artificiale al nostro Paese serve un quadro regolatorio chiaro, adeguato e basato sui diritti fondamentali, così come previsto dalla recente proposta di regolamentazione europea (cfr. Capitolo 1). Inoltre, bisogna incrementare gli investimenti, specie quelli in ricerca e sviluppo, incentivare la creazione dei *Digital Innovation Hub* al fine di rafforzare il livello di conoscenza e di consapevolezza delle imprese rispetto alle opportunità offerte dall'intelligenza artificiale e creare un ponte con la ricerca. Occorre inoltre facilitare l'accesso delle piccole e medie imprese ai sistemi di intelligenza artificiale, anche mediante forme di incentivazione alla condivisione.

È inoltre cruciale migliorare la qualità dei percorsi di studio di alta formazione (master universitari, dottorati, ecc.), agire anche sulle competenze di base e aumentare le esperienze di apprendistato sul campo.

Sarebbe sicuramente apprezzabile l'**istituzione di un Istituto italiano per l'Intelligenza artificiale**, rispondendo all'esigenza di incrementare l'offerta di alta formazione, potenziare la ricerca e il trasferimento tecnologico.

8.2 BLOCKCHAIN

La **blockchain** è la più nota tra le tecnologie che fanno parte della famiglia delle *distributed ledger*, ovvero una tecnologia che permette di implementare un archivio distribuito in grado di gestire transazioni tra gli utenti di una rete. Al fine di comprendere concretamente il funzionamento di questa tecnologia è necessario analizzare come si svolge effettivamente una **transazione**: per operare nel sistema è necessario dotarsi di un software che ci identifica come utenti della rete e

[51] https://www.governo.it/sites/governo.it/files/PNRR.pdf.
[52] https://www.mise.gov.it/images/stories/documenti/Strategia_Nazionale_AI_2020.pdf.
[53] https://innovazione.gov.it/notizie/articoli/nasce-il-gruppo-di-lavoro-sulla-strategia-nazionale-per-l-intelligenza-artificial/.

genera una coppia di chiavi, una privata e una pubblica; la chiave privata è un codice generato in maniera casuale che può contenere fino a 64 caratteri alfanumerici, la chiave pubblica viene invece generata tramite una funzione irreversibile a partire dalla chiave privata e permette di firmare effettivamente la transazione.

Data l'irreversibilità della funzione non è possibile ottenere la chiave privata a partire da quella pubblica, pertanto è possibile dimostrare la propria identità alla rete senza dover condividere entrambe le credenziali personali agli altri utenti. I dati riguardanti la transazione con l'aggiunta della marca temporale (un'operazione che associa una data ed un orario alla transazione che non potranno essere successivamente modificate) verranno poi elaborati insieme a quelli dei blocchi precedenti creando un nuovo anello della catena (Fig. 8.4).

Nei sistemi distribuiti la validazione e la conservazione dei dati non viene eseguita da un unico soggetto centrale ma da numerosi "nodi" che fanno parte della rete. I nodi sono computer connessi alla rete che partecipano al processo di verifica delle transazioni, trasmettono i nuovi blocchi alla blockchain e conservano una copia aggiornata di tutto il registro. Queste operazioni vengono eseguite da tutti i nodi in maniera congiunta quindi più cresce il loro numero più il sistema diventerà sicuro, un attacco informatico ad un singolo nodo non avrebbe infatti alcun effetto sulla catena. Per questo motivo i dati conservati sulla blockchain vengono considerati immutabili, per modificarne il contenuto infatti si dovrebbe ottenere il consenso della maggior parte dei nodi della stessa.

Nonostante la blockchain sia stata implementata circa dodici anni fa per essere il libro mastro delle transazioni in BitCoin solo negli ultimi anni gli analisti hanno cominciato a valutarne applicazioni estranee all'ambito delle criptovalute. Gli investimenti globali in questa tecnologia, secondo un'analisi condotta da IDC, dovrebbero attestarsi sui $6,6 miliardi nel 2021 e sono destinati a crescere nel prossimo triennio fino a raggiungere $19 miliardi nel 2024 (Fig. 8.5).

L'Osservatorio Blockchain & Distributed Ledger della School of Management del Politecnico di Milano in un suo studio pubblicato a gennaio 2021 ha censito 1242 progetti sulla blockchain provenienti dal mondo delle aziende e dai governi nel periodo 2016-2020. La classifica globale dei

Figura 8.4 Funzionamento di una transazione in Blockchain

Fonte: Elaborazioni I-Com

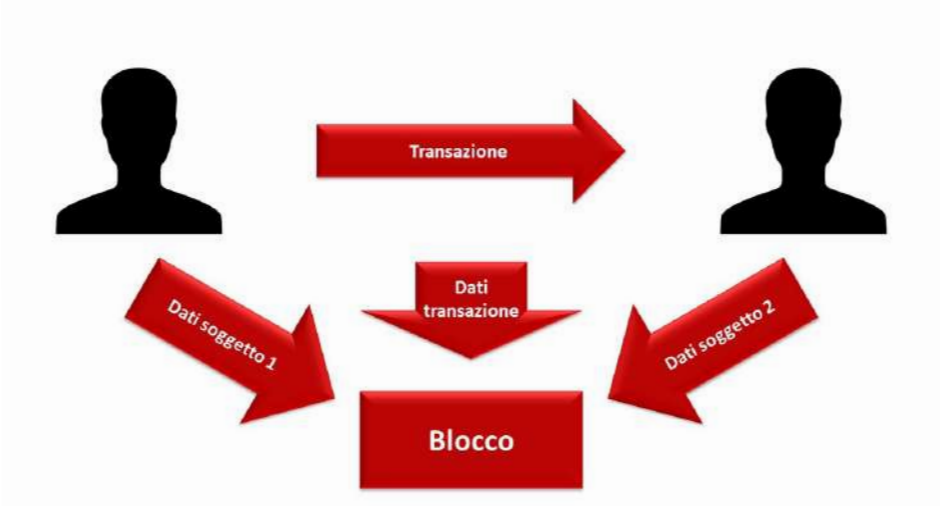


Figura 8.5 : Investimenti globali in progetti blockchain (miliardi di $)

Fonte: IDC
Note: Dati previsionali

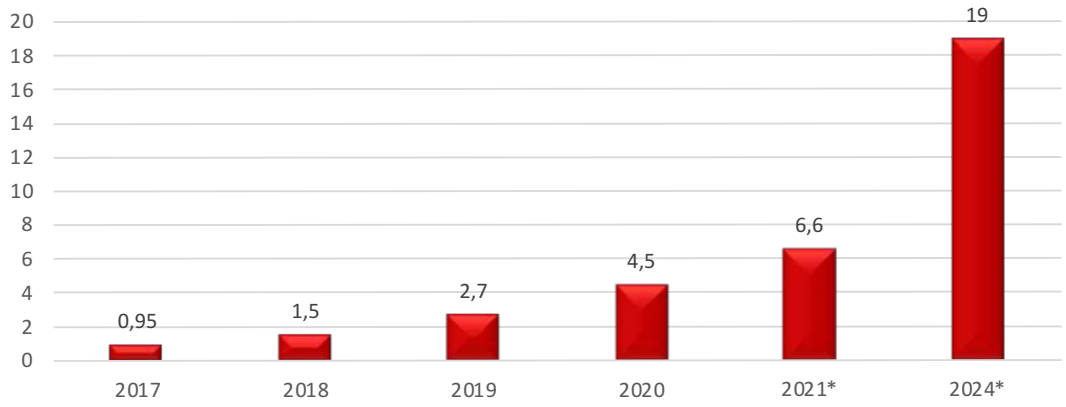
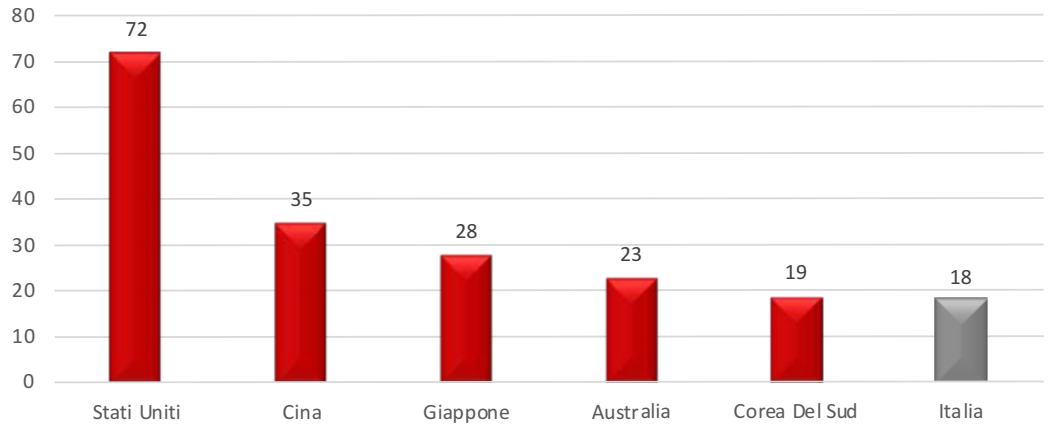


Figura 8.6 Top 6 paesi per progetti blockchain

Fonte: Osservatorio Blockchain & Distributed Ledger (2021)

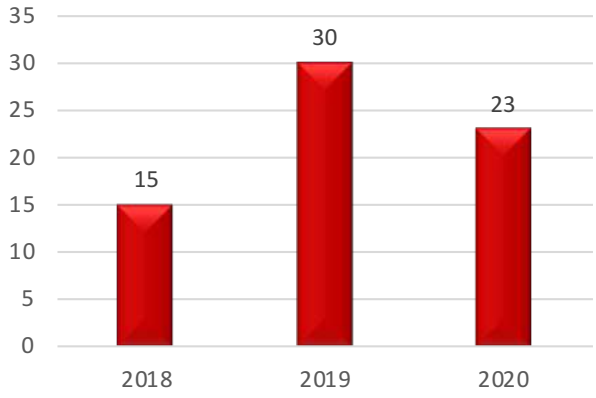


progetti blockchain attivati nel corso del 2020 (Fig.8.6) è guidata dagli Stati Uniti, che ne ospitano 53, seguiti da Cina (25) e Giappone (28). L'Italia, che può contare su 18 iniziative pur essendo lontana dalla vetta, è il primo Paese dell'UE27 ad entrare nella classifica occupando il sesto posto a livello globale.

Concentrando l'attenzione sul panorama nazionale è possibile notare come gli investimenti italiani in blockchain nel 2020 si siano attestati sui €23 milioni, in leggera discesa rispetto ai €30 milioni del 2019 (Fig.8.7). L'effetto di questa flessione è probabilmente addebitabile solo in parte alla crisi pandemica. Infatti, con l'attenuarsi dell'hype mediatico che ha caratterizzato questa

Figura 8.7 Investimenti su progetti blockchain in Italia (milioni di €)

Fonte: Osservatorio Blockchain & Distributed Ledger (2021)



tecnologia nel 2019, gli innumerevoli annunci, diminuiti del 80%, hanno lasciato il passo ai soli progetti che potevano avere effettivamente un futuro. Questa tesi trova riscontro anche nel monitoraggio effettuato dall'Osservatorio sullo stato di avanzamento dei progetti blockchain sviluppati in Italia (Fig.8.8). Il 60% degli investimenti effettuati in Italia su questa tecnologia nel 2020 è stato destinato a iniziative già in fase operativa, il 28% a progetti pilota, l'11 % a proof of concept e solo l'1% a profetti di formazione.

Per quanto riguarda i principali settori di provenienza degli investimenti in blockchain in Italia (Fig.8.9) a primeggiare è, come presumibile, la finanza, che rafforza la sua posizione passando dal 42% del 2019 al 58% del 2020. Gli altri settori che rappresentano una quota rilevante di investimenti in questa tecnologia nel panorama nazionale sono l'agroalimentare (11%), le utility (7%) e la pubblica amministrazione (6%).

Per quanto riguarda i principali settori di provenienza degli investimenti in blockchain in Italia (Fig.8.9) a primeggiare è, come presumibile, la finanza, che rafforza la sua posizione passando dal 42% del 2019 al 58% del 2020. Gli altri settori che rappresentano una quota rilevante di investimenti in questa tecnologia nel panorama nazionale sono l'agroalimentare (11%), le utility

Figura 8.8 Stato avanzamento progetti blockchain in Italia (2020)

Fonte: Osservatorio Blockchain & Distributed Ledger (2021)

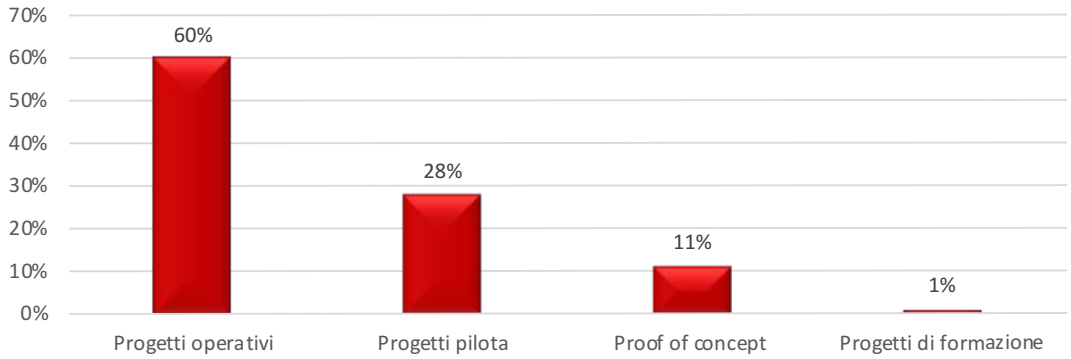
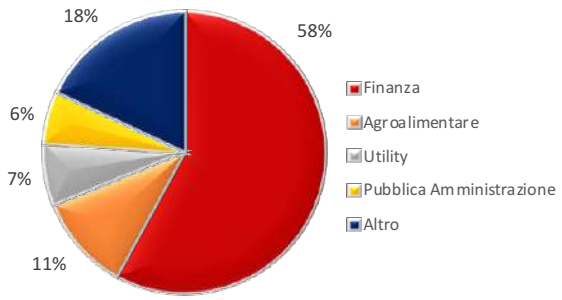


Figura 8.9 Principali settori che investono in blockchain (2020)

Fonte: Osservatorio Blockchain & Distributed Ledger (2021)



(7%) e la pubblica amministrazione (6%).

8.2.1 Le principali iniziative pubbliche italiane su blockchain e registri distribuiti

La blockchain, in virtù delle sue caratteristiche, potrebbe rappresentare una grande opportunità per lo sviluppo dell'economia italiana e per la modernizzazione delle funzioni pubbliche.

Per cogliere queste opportunità il Ministero dello Sviluppo economico, a dicembre 2018, ha nominato un gruppo di esperti affidandogli il compito di definire la "***Strategia italiana in***

materia di tecnologie basate su registri condivisi e Blockchain". Le proposte elaborate dal gruppo di lavoro[54], pubblicate a giugno 2020, mirano a raggiungere i seguenti obiettivi:

1. dotare il Paese di un quadro regolamentare competitivo nei confronti degli altri Paesi;
2. incrementare gli investimenti, pubblici e privati, nella Blockchain/DLT e nelle tecnologie correlate (IoT, 5G);
3. proporre campi applicativi della tecnologia al fine di indirizzare correttamente i possibili investimenti, in coerenza con i settori chiave dell'economia italiana
4. migliorare efficienza ed efficacia nell'interazione con la pubblica amministrazione tramite l'adozione del principio Once-Only e della decentralizzazione;
5. favorire la cooperazione europea ed internazionale tramite adozione della comune infrastruttura Europea in via di definizione da parte dell'EBSI (European Blockchain Systems Infrastucture);
6. utilizzare la tecnologia per favorire la transizione verso modelli di economia circolare, in linea con l'Agenda 2030 per lo sviluppo sostenibile;
7. promuovere l'informazione e la consapevolezza della Blockchain/DLT tra i cittadini.

Il documento raccomanda, per prima cosa, l'istituzione di **una struttura unitaria di Governance nazionale per le tecnologie innovative** utile a definire, in termini coordinati, politiche e interventi concreti nel rispetto del principio della neutralità tecnologica. Secondo gli esperti, una guida unica aiuterebbe a coordinare gli investimenti in un disegno di intervento unitario e sinergico oltre che a favorire il dialogo e la collaborazione tra istituzioni nazionali ed europee. I principali settori di interesse individuati nel documento sono:

- **Manifatturiero** - La blockchain, in questo caso applicata all'industria, può contribuire alla creazione della "Fabbrica Intelligente" ottimizzando, congiuntamente con le tecnologie IoT e l'intelligenza artificiale, sia i processi produttivi che la logistica;
- **Agroalimentare** - in cui le DLT possono favorire la trasparenza e rafforzare le garanzie di origine e sicurezza alimentare;
- **Made in Italy** - questa tecnologia, aumentando la tracciabilità dei prodotti, potrebbe aiutare a contrastare il fenomeno della contraffazione che affligge i prodotti italiani;
- **Infrastrutture critiche** - ambito in cui la blockchain, essendo un registro immutabile, potrebbe garantire il corretto svolgimento delle attività di monitoraggio e manutenzione;
- **Energia** - l'utilizzo delle DLT in ambito energetico permetterebbe di creare mercati decentralizzati di compravendita di energia minimizzando gli sprechi e incrementando il ruolo dei prosumer sulle reti;
- **Sustainable Development Goals (SDG)** - la blockchain, attraverso l'utilizzo di token, potrebbe sostenere la creazione di ecosistemi in grado di incentivare i comportamenti virtuosi, in ambito sostenibile, adottati da cittadini e imprese;
- **Proprietà intellettuale** - l'utilizzo delle DLT in quest'ambito permetterebbe di superare il modello attuale di tutela dei diritti d'autore permettendo ai titolari del diritto di verificare in maniera certa e senza intermediari l'utilizzo delle proprie opere di ingegno;
- **Terziario avanzato e modelli cooperativi** - questo settore potrebbe beneficiare della disintermediazione offerta dalla blockchain

[54] https://www.mise.gov.it/images/stories/documenti/Proposte_registri_condivisi_e_Blockchain_-_Sintesi_per_consultazione_pubblica.pdf

riducendo la centralità delle piattaforme;

- **Fintech e pagamenti digitali** - questo è il settore in cui la blockchain trova la sua naturale collocazione e in cui trova la maggior parte delle applicazioni.

Oltre alla definizione della Strategia Nazionale, negli ultimi anni sono state attivate numerose iniziative di impulso pubblico volte alla diffusione della tecnologia blockchain in Italia. Con il **decreto legge n. 135/2018 (c.d. decreto Semplificazioni)**[55] il nostro Paese è stato il primo in Europa che ha formalizzato la definizione giuridica di blockchain e smart contract. L'atto ha infatti definito "*tecnologie basate su registri distribuiti*", le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili; dall'altro, ha inteso lo smart contract come un programma informatico che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse.

Nel marzo 2019 è stato invece lanciato dal MiSE un importante **Progetto Pilota** per promuovere il ricorso alla tecnologia blockchain per la tutela del made in Italy. La sperimentazione, affidata ad IBM, prevede uno studio di fattibilità che costituirà un modello di base per i settori di riferimento del Made in Italy, al fine di cogliere appieno i vantaggi della tecnologia blockchain in termini di tracciabilità dei prodotti lungo la filiera, certificazione al consumatore della loro provenienza, contrasto alla contraffazione, garanzia della sostenibilità sociale ed ambientale delle produzioni Made in Italy. Il progetto prevede una fase di esplorazione e *design thinking* per l'individuazione, insieme alle imprese, di casi specifici per analizzare alcuni processi produttivi ai quali applicare la blockchain ed infine la realizzazione di uno studio di riepilogo delle condizioni di fattibilità per le filiere del settore sulla base delle risultanze dell'esplorazione.

Dal punto di vista finanziario, la legge di bilancio 2019 ha previsto l'istituzione di un fondo per interventi volti a favorire lo sviluppo di tecnologie di intelligenza artificiale, blockchain e IoT con una dotazione di 15 milioni di euro per ogni anno dal 2019 al 2021.

Oltre alle iniziative centrali si sono sviluppate numerose implementazioni di questa tecnologia a livello locale. Nel **Comune di Napoli** in seguito ad una delibera che istituiva un gruppo di lavoro allo scopo di elaborare e proporre obiettivi legati alla tecnologia blockchain, è stato presentato un metodo innovativo di ***e-voting***, per superare le problematiche rilevate attraverso le esperienze effettuate all'estero (ad esempio in l'Estonia). La caratteristica principale del sistema di Napoli è l'utilizzo di una *blockchain permissionless* (Ethereum) direttamente nel seggio, che scinde il momento dell'identificazione (lasciata al Presidente del Seggio) dal momento dell'esercizio effettivo della preferenza elettorale e della registrazione in blockchain. Ciò permette di anonimizzare il meccanismo di gestione delle preferenze, dato che il soggetto votante non è in alcun modo riconducibile alla preferenza espressa. In questo modo il voto elettronico – non a distanza – rimane rigorosamente segreto, diventa costituzionalmente legittimo ed anche immutabile, perché appoggiato su blockchain anonima *permissionless*.

Il **Comune di Bari** ha invece sperimentato questa tecnologia in un progetto per la digitalizzazione del processo di gestione delle polizze fideiussorie.

[55] Convertito in legge n. 12 dell'11 febbraio 2019

Tramite l'uso di una *blockchain permissioned* (SIAchain), il Comune permette di gestire la polizza tra contraente e fideiussore direttamente nella chain, mentre i rapporti impresa-banca e impresa-assicurazione rimangono *off-chain*. Il fine di questo progetto, oltre alla dematerializzazione del ciclo ordine-pagamento, consiste nel deframmentare e rendere più facilmente rintracciabili le informazioni sulle polizze fideiussorie.

Il **Comune di Cinisello Balsamo**, in collaborazione con Regione Lombardia, ha sviluppato un progetto che prevede l'utilizzo della tecnologia blockchain nell'iter di concessione delle agevolazioni previste dalla misura "*Nidi gratis*". Durante la discussione sono stati illustrati i notevoli risultati raggiunti durante la sperimentazione: Il tempo medio di presentazione di una nuova domanda è stato di 7 minuti e 40 secondi; il 90% dei requisiti sono stati verificati automaticamente dal sistema e già inseriti su blockchain; i tempi di istruttoria residua per gli aderenti alla sperimentazione è ridotto significativamente e non richiederà per nessuno un passaggio di verifica da parte del Comune; sono stati risparmiati circa 2190 minuti di lavoro del personale amministrativo.

L'AgID, a marzo 2021, in collaborazione Cimea, Csi Piemonte, Enea, Inail, Infratel Italia, Inps, Politecnico di Milano, Poste Italiane, Rse, Gse, Sogei e Università di Cagliari, ha lanciato il **progetto IBSI (Italian Blockchain Service Infrastructure)**. L'iniziativa, in linea con la Strategia Europea che sta realizzando (anche con il contributo italiano) un'infrastruttura analoga nell'ambito della **European Blockchain Partnership**, prevede la creazione della prima rete italiana basata sulla blockchain per l'erogazione di servizi di interesse pubblico. L'IBSI porterà avanti attività di ricerca e sviluppo sulla blockchain, per approfondirne le potenzialità, come ad esempio gestire i certificati pubblici in modo completamente digitale, tracciare la filiera del Made in Italy, sviluppare modelli energeticamente sostenibili e rinnovabili e contribuire alla lotta al cambiamento climatico.

8.3 CLOUD COMPUTING PER LA PA E LE IMPRESE

8.3.1 La centralità del Cloud nel PNRR

I pilastri su cui si basa la trasformazione digitale del Paese, e su cui l'Italia deve accelerare per poter competere alla pari con le principali economie globali, sono le cosiddette "*piattaforme abilitanti*", ovvero quelle innovazioni tecnologiche che permettono di fruire di tutti i nuovi servizi digitali "*avanzati*". Tra questi fattori, nel contesto della pandemia di Covid-19, il cloud computing ha assunto una particolare valenza strategica, permettendo a imprese, PA e cittadini europei di continuare a erogare e/o a fruire di servizi a distanza, anche abilitando lo smart working e consentendo la prosecuzione di gran parte delle attività economiche anche nelle fasi di maggiore limitazione della mobilità. Adesso che l'emergenza sembra ormai superata l'importanza dello sviluppo di tali fattori risulta forse ancor più importante in virtù dell'auspicata ripresa economica post pandemica.

La **strategicità del Cloud** viene evidenziata anche dalla centralità che le viene assegnata nel quadro del PNRR. La prima componente della Missione 1, nella previsione di digitalizzare la Pubblica Amministrazione, prevede al primo punto di supportare la migrazione al cloud delle amministrazioni centrali e locali, creando un'infrastruttura nazionale e supportando le amministrazioni nel percorso di trasformazione.

Nel complesso, alla digitalizzazione della Pubblica Amministrazione sono destinati € 6,14 miliardi nel prossimo quinquennio, di cui € 900 milioni alle infrastrutture digitali, 1 miliardo di euro all'abilitazione e facilitazione della migrazione al cloud e 600 milioni alla digitalizzazione delle

Tab.8.1: Missione 1 Componente 1 del PNRR. Digitalizzazione, Innovazione e Sicurezza nella PA (mld di €)

Fonte: Piano Nazionale di Ripresa e Resilienza, maggio 2021

Ambiti di intervento/Misure	Totale
1. Digitalizzazione PA	6,14
Investimento 1.1: Infrastrutture digitali	0,9
Investimento 1.2: Abilitazione e facilitazione migrazione al cloud	1
Investimento 1.3: Dati e interoperabilità	0,65
Investimento 1.4: Servizi digitali e cittadinanza digitale	2,01
Investimento 1.5: Cybersecurity	0,62
Investimento 1.6: Digitalizzazione delle grandi amministrazioni centrali	0,61
Investimento 1.7: Competenze digitali di base	0,2
Riforma 1.1: Processo di acquisto ICT	-
Riforma 1.2: Supporto alla trasformazione della PA locale	0,16
Riforma 1.3: Introduzione linee guida "cloud first" e interoperabilità	-

grandi amministrazioni centrali.

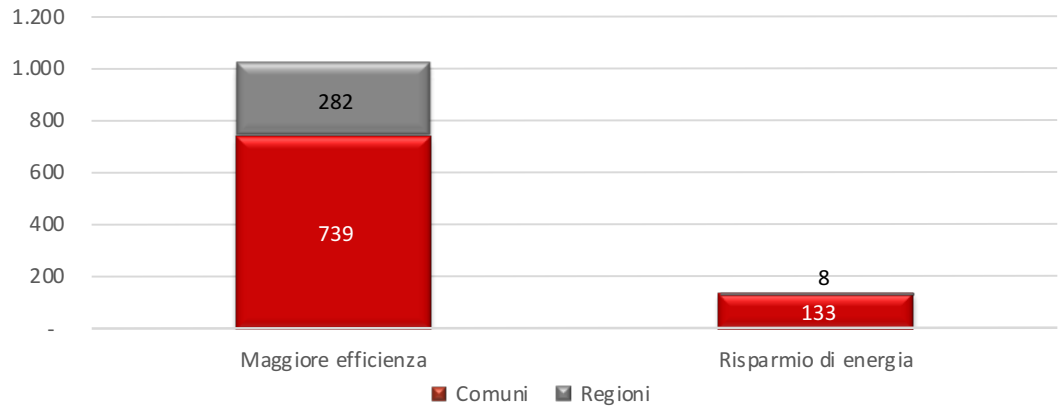
La **digitalizzazione della PA** dovrà seguire un approccio "*cloud first*" orientato alla migrazione dei dati e degli applicativi informatici delle singole amministrazioni verso un ambiente cloud. Questa tecnologia consente infatti alle amministrazioni di migliorare notevolmente l'erogazione di servizi, in particolare nelle aree remote (elemento cruciale per salute e scuola), creare nuove applicazioni virtualizzate e sviluppare modelli di gestione che permettono una rapida espansione dell'utilizzo delle infrastrutture in periodi di intensa attività.

Le soluzioni di *cloud computing* appaiono estremamente vantaggiose in particolare per gli enti locali. Infatti, oltre ad evitare la realizzazione e la gestione in casa delle infrastrutture IT (riducendo in maniera drastica i costi di progettazione, installazione e gestione di queste ultime) abbattono notevolmente i tempi di acquisizione delle tecnologie, richiedendo semplicemente la sottoscrizione di un contratto con il cloud service provider.

In quest'ottica, lo studio dell'Istituto per la Competitività (I-Com) dal titolo "*Una strategia cloud per un'Italia più competitiva e sicura*"[56] ha stimato un potenziale **risparmio** derivante

Figura 8.10 Risparmio stimato per le amministrazioni comunali e regionali italiane (milioni di €)

Fonte: Elaborazione I-Com su dati Istat e SIOPE)



[56] Lo studio – presentato lo scorso 21 aprile – è scaricabile a questo link https://www.i-com.it/wp-content/uploads/2021/04/Studio-I-Com_Una-strategia-cloud-per-unItalia-piu-competitiva-e-sicura.pdf

dall'adozione del cloud computing nelle PA locali quantificabile in circa 1,16 miliardi di euro, di cui oltre 1 miliardo in termini di maggiore produttività e ulteriori 140 milioni in termini di minori spese di energia (Fig.8.10). Il passaggio al cloud computing risulta quindi estremamente conveniente non solo per migliorare i servizi offerti ai cittadini ma anche nell'ottica di efficientamento della spesa pubblica.

8.3.2 Il mercato del cloud in Italia

Nell'anno appena trascorso, il cloud si è rivelato un ottimo alleato per rispondere rapidamente ed efficacemente alla crisi generata dalla pandemia, in particolare in termini di mantenimento della produttività anche in presenza di una fortissima riduzione della mobilità. Non a caso, tra i maggiori vantaggi dell'adozione del cloud percepiti dalle aziende[57] figura al primo posto il supporto per i telelavoratori, seguito da un miglior controllo sull'utilizzo di risorse IT e dalla possibilità di migliorare la flessibilità per soddisfare le esigenze aziendali. Per lo stesso motivo, le aziende risultano soddisfatte anche in termini di miglioramento dell'assistenza ai propri clienti e dell'accresciuta rapidità nel per soddisfare le esigenze aziendali (Fig.8.11).

Figura 8.11 Le principali motivazioni per la migrazione a un'Infrastruttura abilitata al cloud

Fonte: Nutanix Enterprise Cloud Index 2020

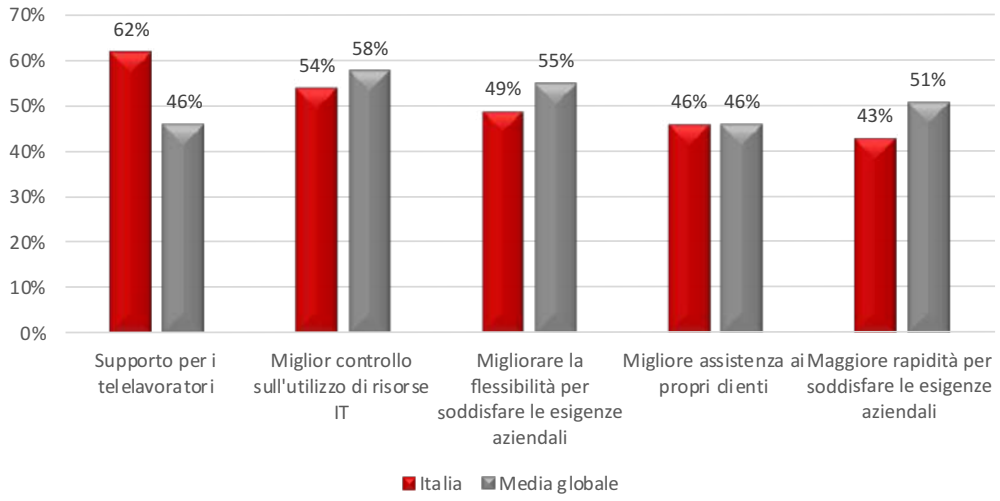
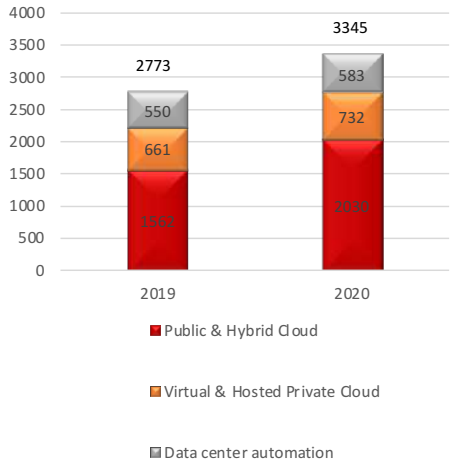


Figura 8.12 Il mercato del cloud computing in Italia, per tipologia (milioni di €)

Fonte: Politecnico di Milano



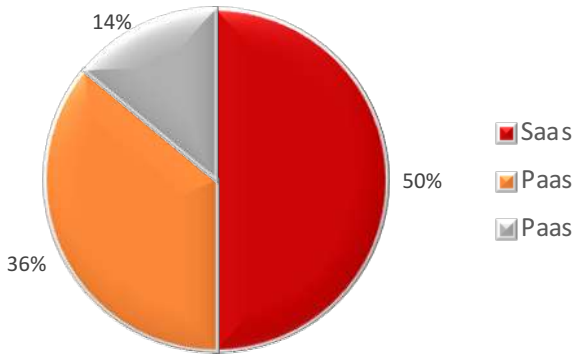
Anche grazie tali molteplici vantaggi, il mercato del cloud appare in continua crescita, sia a livello internazionale che a livello italiano. Per quanto concerne l'Italia, secondo i dati forniti dal Politecnico di Milano, nel 2020 il mercato del cloud ha raggiunto €3,34 miliardi, mostrando una crescita del +21% YoY (Fig. 8.12).

Per quanto concerne il breakdown per modelli di dispiegamento, il **segmento del Public & Hybrid**,

[57] Nutanix, Vanson Bourne, "*Enterprise Cloud Index - I dati dell'Italia*" (2021).

Figura 8.13 Il mercato del cloud computing in Italia, per modelli di servizio (2020)

Fonte: Politecnico di Milano



ovvero l'insieme dei servizi forniti da provider esterni e l'interconnessione tra cloud pubblici e privati, si conferma quello maggiormente in crescita (+30%), giungendo sopra quota 2 miliardi di euro. Il cloud privato virtuale è passato da 661 milioni di euro del 2019 a 732 milioni del 2020 (+11%), mentre cresce meno (da 550 a 583 milioni) la modernizzazione delle infrastrutture on-premise (+6%). In termini di ricavi per modelli di servizio, ovvero **IaaS**, **PaaS** e **SaaS**, le stime del Politecnico indicano nel 2020 la predominanza del SaaS che, con un tasso di crescita di oltre il 40%, è arrivato a rappresentare una quota vicina alla metà della spesa complessiva in cloud pubblico e ibrido (oltre 1 miliardo, Fig. 8.13). Lo IaaS presenta un tasso di crescita del 16% che, seppur in diminuzione rispetto al 2019 (+25%), lo proietta oltre quota 700 milioni. Più staccato il PaaS, che si conferma il modello più specialistico, a quota 299 milioni (+22%).

8.3.3 La Strategia Cloud Italia

Sul piano delle **policy**, la pubblicazione della nuova Strategia nazionale sul cloud, pur non dando formalmente avvio alle attività implementative, chiarisce per alcuni aspetti la posizione governativa sul tema e detta i passi da seguire nei prossimi mesi. Il modello si basa su tre gambe: la classificazione dei dati e dei servizi; la qualificazione dei servizi cloud; il polo strategico nazionale.

La prima, quella maggiormente innovativa rispetto alla vision precedente, introduce, sulla scorta del modello britannico, una classificazione dei dati (Fig.8.14) – ordinario, critico, strategico – in base al potenziale danno che una loro esfiltrazione provocherebbe al sistema Paese. I dati "*ordinari*" sono quelli per cui un eventuale accesso terzo non provocherebbe l'interruzione di servizi dello Stato o un impatto negativo sul benessere economico e sociale del Paese. Sono considerati dati "*critici*" quelli che, se compromessi, potrebbero pregiudicare la continuità di funzioni dello Stato rilevanti per la società, la salute, la sicurezza. Infine, i dati "*strategici*" sono quelli che impattano direttamente sulla sicurezza nazionale.

Dati e servizi di grado diverso devono essere affidati a provider che garantiscono **livelli di sicurezza diversi**. Questo porta alla seconda gamba della strategia, ovvero la qualificazione dei servizi di *cloud computing*. Questo processo include a sua volta tre aspetti fondamentali, ovvero come il provider gestisce gli aspetti tecnico organizzativi del servizio, i requisiti di sicurezza e le condizioni contrattuali applicate. L'analisi degli aspetti sopracitati permette di individuare le seguenti categorie di servizi:

1. **Cloud pubblico non qualificato**, ovvero che non risponde ai criteri individuati in precedenza;
2. **Cloud pubblico qualificato**, ovvero che consente la localizzazione dei dati in Europa e il rispetto di requisiti sia di sicurezza che tecnico organizzativi;
3. **Cloud pubblico con controllo *on-premise* dei meccanismi di sicurezza**, che permette di criptare i dati e consente un maggior livello di autonomia dai provider extra-UE nella gestione operativa e il controllo delle

infrastrutture tecnologiche;

4. **Cloud privato e ibrido**, che permette la localizzazione dei dati in Italia e una separazione dalle altre region pubbliche utilizzate dal provider. Questa classificazione può a sua volta essere ulteriormente suddivisa in:

- **Cloud privato/ibrido su licenza**, ovvero soluzioni basate sulla tecnologia *hyperscaler* licenziata da uno o più provider;
- **Cloud privato qualificato**, ovvero soluzioni offerte da un provider (al momento non sembra specificato se italiano, con server in Italia o con un partner tecnologico italiano che funga da "*garante*" dei dati) basate su tecnologie commerciali qualificate mediante procedure di scrutinio e certificazione tecnologica.

Secondo quanto emerge dalla strategia italiana, i cloud pubblici non criptati, pur se qualificati, potranno ospitare solo dati e servizi ordinari. I servizi di Cloud Pubblico Criptato, Privato/Ibrido su licenza e Privato Qualificato potranno ospitare invece dati e servizi sia critici che ordinari, mentre quelli strategici potranno essere localizzati solo sugli ultimi due.

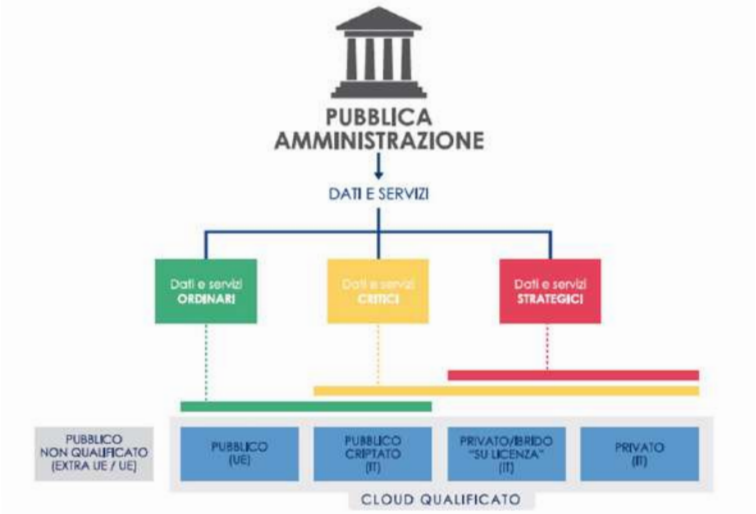
Secondo la pianificazione italiana questo processo dovrà culminare nella **realizzazione di un Marketplace che guidi le PA nella scelta e nell'acquisto del servizio cloud più adatto alle proprie esigenze**. Tale processo dovrebbe consistere in un aggiornamento di quello già previsto per la strategia "cloud first", sebbene non vi sia certezza su tale punto poiché nel nuovo documento non viene menzionato nel dettaglio il legame tra le due iniziative.

La terza gamba della strategia è dedicata allo sviluppo del **Polo Strategico Nazionale (PSN)**, ovvero le infrastrutture ubicate sul territorio italiano utili ad erogare servizi IT alle pubbliche amministrazioni. Il PSN previsto dal piano italiano dovrà offrire garanzie di affidabilità, resilienza e indipendenza. Per tale ragione le localizzazioni fisiche dei data center dovranno essere a basso rischio di disastri naturali e garantire la migliore connettività possibile.

Il Polo Strategico Nazionale verrà gestito da un fornitore identificato sulla base di opportuni requisiti tecnico-organizzativi, che sarà è tenuto a garantire il controllo sui dati in conformità con la normativa in materia, nonché e a rafforzare la

Figura 8.14 Dati, servizi e provider per la PA

Fonte: Strategia Cloud Italia, settembre 2021



possibilità della PA di negoziare adeguate condizioni contrattuali con i fornitori di servizi Cloud.

Il PSN dovrà garantire, sin dalla progettazione, il rispetto dei requisiti in materia di sicurezza, ad esempio PSNC e NIS, e di abilitare la migrazione, almeno inizialmente con un processo *lift-and-shif*t, verso tipologie di servizi Cloud IaaS e PaaS. Il PSN offrirà sia servizi di cloud pubblico criptato (IT), sia tutta la gamma di servizi Cloud privato/ibrido (Cloud Privato/Ibrido su licenza e il Cloud Privato Qualificato)[59].

8.3.4 Le proposte per il PSN e il nodo delle tempistiche

Allo scadere di settembre 2021, così come auspicato dal Ministro per l'innovazione tecnologica e la Transizione digitale Vittorio Colao al momento della presentazione della Strategia, sono pervenute le proposte per la realizzazione e la gestione del Polo Strategico Nazionale per il cloud. Si tratta di due iniziative che provengono da due cordate, e che sia affiancano alla manifestazione di interesse presentata a inizio agosto dal Consorzio Italia Cloud, composto da Seeweb, Sourcesense, Infordata, Babylon Cloud, Consorzio Eht e Netalia[60].

Una proposta di partenariato pubblico-privato per la creazione del Psn proviene dalla cordata costituita da Tim (45%), Leonardo (25%), Cassa Depositi e Prestiti (20%) e Sogei (10%) che in caso di aggiudicazione si costituirebbe come NewCo con tali quote societarie. L'obiettivo consiste nell'erogazione di soluzioni e servizi cloud a sostegno della PA nell'ottica di **assicurare il maggior livello possibile di efficienza, sicurezza e affidabilità dei dati**. Tra i soci, Tim si occuperebbe di fornire infrastrutture e piattaforme cloud, Leonardo metterebbe a disposizione servizi di cybersecurity, Sogei fornirebbe servizi di *business culture enablement* e formazione per il personale della PA, e CDP Equity opererebbe in qualità di socio finanziario.

Un'altra proposta per la realizzazione e gestione del Polo Strategico Nazionale è stata presentata dalla cordata Almaviva-Aruba, sempre in regime di partenariato pubblico-privato. La proposta evidenzia la totale italianità delle società coinvolte e l'immediata disponibilità delle infrastrutture, che consentirebbe il conseguimento dei risultati richiesti entro tempistiche migliorative rispetto alla pianificazione prevista nella Strategia Cloud.
A livello tecnico si punta sulla disponibilità di adeguati livelli di crittografia e gestione delle chiavi esterne alle diverse piattaforme, sull'apertura alla federazione verso con altri soggetti (pubblici, regionali e nazionali) e standard (in particolare europei, come l'iniziativa Gaia-X) e sul controllo della intera filiera, dal data center fino al servizio Cloud pubblico, privato, ibrido, insieme alle competenze nella conservazione, elaborazione e protezione delle diverse tipologie di dati nazionali (strategici, critici, ordinari, come richiesto dalla Strategia).

A livello infrastrutturale la proposta punta in particolare sulla disponibilità di una Green Cloud Factory con un'elevata capillarità di presenza territoriale, in particolare grazie a 4 Data Center di nuova generazione, *green-by-design* e con una

[59] Il documento non chiarisce però che ruolo avranno le 35 strutture in capo dalle amministrazioni regionali già classificati come candidabili a PSN).
[60] In data 1° ottobre, il Consorzio Italia Cloud ha annunciato che non presenterà alcuna proposta, non riconoscendosi nel modello indicato ed esprimendo una forte preferenza "*verso una infrastruttura Cloud federata che valorizzi le imprese italiane e le aziende pubbliche di settore, indipendente dal soggetto chiamato a gestirle, attenta al principio di 'sovranità digitale' che deve rimanere elemento imprescindibile di qualificazione, come avviene in modo prioritario negli altri Paesi europei*". Il Consorzio ha anche affermato che rimarrà in attesa di "*conoscere le determinazioni del governo sulle procedure di assegnazione*".

carbon footprint neutrale, e alla piena disponibilità di Data Center campus collocati in Regioni diverse, che consentono continuità operativa, tolleranza ai guasti e soprattutto la capacità di accelerare della fase di setup consentendo una velocità di migrazione superiore agli obiettivi prefissati dal governo.

A tal proposito, il documento pubblicato individua tre fasi: entro la fine del 2021 è prevista la conclusione della cosiddetta "*Fase 1*", ovvero la pubblicazione del bando di gara per la realizzazione del PSN. La Fase 2, che si sostanzia nell'aggiudicazione e nella realizzazione fisica del PSN, dovrà finire, secondo il cronoprogramma, entro il 2022. Infine, la Fase 3 prevede la migrazione di tutto l'ecosistema IT della PA italiana in cloud. Quest'ultima fase, che dovrebbe aprirsi dopo l'aggiudicazione a fine 2022, si chiuderà entro il 2025, in linea con gli obiettivi imposti dal PNRR.

I piani di migrazione saranno definiti in accordo con il risultato della classificazione dei dati e dei servizi. La classificazione e la redazione del piano di migrazione saranno definiti e supportati, per i rispettivi profili di competenza, dell'Agenzia per la Cybersicurezza Nazionale (ACN) e del Dipartimento per la Trasformazione Digitale (DTD).

In quest'ottica è utile fare due considerazioni: in primo luogo, l'Agenzia è ancora in fase di gestazione, pertanto le operazioni di classificazione e la stessa redazione del piano di migrazione saranno inevitabilmente condizionate dall'operatività della stessa. La seconda riguarda le tempistiche di migrazione, per le quali già esiste una programmazione contenuta nel "*Piano triennale AgID 20 – 22*"[61], rispetto al quale non viene chiarito se ci sarà un aggiornamento o una ricostruzione ex-novo.

In terzo luogo, analizzando in maniera combinata le tre fasi, si osserva come non venga specificato quanta parte del PSN dovrà essere realizzata da zero e quanta verrà mutuata dalle infrastrutture esistenti. Infatti, poiché l'aggiudicazione (fine 2022) e l'inizio della migrazione (inizio 2022) risultano consequenziali, i tempi di implementazione di nuove infrastrutture sembrerebbero molto brevi o persino non contemplati. Le operazioni potrebbero dunque consistere nel set-up e nel coordinamento di infrastrutture esistenti (o che verranno realizzate in corso d'opera).

Nel caso della proposta Tim-Cdp-Leonardo-Sogei, ove ritenuta di interesse, prevedrebbe l'avvio di una gara pubblica da parte della PA in tempi brevi. Secondo la nota della cordata, la Pubblica Amministrazione dovrà vagliare la proposta entro tre mesi dalla sua ricezione e, in caso di positiva valutazione, avviare la gara. A questa potranno partecipare, oltre al soggetto promotore, tutti gli operatori eventualmente interessati. In caso di aggiudicazione alla cordata, la NewCo verrebbe dotata delle competenze industriali necessarie per l'erogazione dei servizi (anche acquisendole presso i propri soci) ed effettuerebbe gli investimenti utili alla realizzazione dell'infrastruttura tecnologica.

La cordata Almaviva-Aruba, dal canto suo, mette in evidenza l'immediata disponibilità delle infrastrutture, che consentirebbe tempistiche persino migliorative rispetto alla pianificazione prevista. La pubblicazione di ulteriori dettagli relativi alle proposte fornirà certamente delle preziose indicazioni, così come la precisazione da parte del Ministero dell'Innovazione di ulteriori rilevanti dettagli.

[61] https://www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_linformatica_nella_pa_2020_2022.pdf

CONCLUSIONI
E
SPUNTI DI POLICY

GLI SCENARI DIGITALI EUROPEI

Il biennio 2020-2021 si sta caratterizzando per una fortissima accelerazione del processo di digitalizzazione conseguente alla necessità, imposta dalla pandemia, di ripensare nel complesso e in profondità le nostre vite. L'esigenza di contenimento dei contagi, gli alternati periodi di lockdown, l'imposizione del distanziamento sociale hanno infatti costretto autorità, individui e imprese a ripensare le proprie abitudini, i propri sistemi organizzativi e modelli di business per realizzare, in tempi rapidi e secondo modalità efficaci, un vero e proprio *switch* dall'analogico al digitale. In un contesto di così radicale cambiamento che, nella tragedia che si è consumata, di positivo ha senza dubbio avuto l'acquisizione di un ruolo da protagonista da parte del canale digitale, alleato indispensabile per garantire la continuità delle attività socio-economiche, le istituzioni europee hanno da un lato messo in campo risorse finanziarie senza precedenti con il **Piano Next Generation EU** per assicurare la ripresa dell'UE; dall'altro, hanno lanciato un **poker di proposte** - Digital Governance Act, Digital Services Act, Digital Market Act e Artificial Intelligence Act - con l'obiettivo di ripensare e modernizzare la cornice normativa del digitale alla luce delle straordinarie opportunità e potenziali criticità connesse all'utilizzo dei dati ed allo sviluppo dell'intelligenza artificiale, nonché dell'importanza sempre crescente assunta dalle piattaforme con conseguente necessità di ridefinirne le responsabilità.

Rispetto a tale ultimo tema, ossia **il regime di responsabilità e il set di obblighi e divieti che DSA e DMA propongono**, se da un lato le intenzioni appaiono pregevoli nel provare a fornire risposte a criticità effettive e potenziali derivanti dalla rivoluzione digitale, dall'altro, quanto alle scelte metodologiche, impongono di verificare, anche nel dialogo tra istituzioni, se effettivamente la scelta di disegnare un sistema normativo improntato a una logica *ex ante* che fissi regole uniformi per soggetti con modelli di business, obiettivi, strutture operative e organizzative profondamente diversi sia in grado di far fronte, in maniera efficace e senza rappresentare un ostacolo all'innovazione, alle sfide del futuro in un settore a elevatissima rapidità di sviluppo. Nell'operare tale doverosa riflessione, non va sottovalutata la necessità di bilanciare due esigenze in parte contrapposte: da una parte, quella di **garantire uniformità, certezza del diritto e prevedibilità delle condotte**, dall'altra, di **valutare innanzitutto la sostenibilità degli obblighi posti a carico degli operatori** e inoltre di **prevedere un grado di differenziazione** che tenga adeguatamente conto delle specificità dei singoli casi oggetto di analisi e dell'impatto che determinati obblighi o divieti può esercitare sulle leve competitive degli operatori oltre che su profili più strettamente connessi alla *privacy* e alla sicurezza. Uno strumento senza dubbio funzionale allo scopo è il dialogo regolatorio che, sebbene già presente nella proposta della Commissione, potrebbe essere ulteriormente valorizzato come strumento idoneo ad assicurare un margine di personalizzazione delle valutazioni e a operare come elemento di mitigazione rispetto agli ampi e pervasivi poteri attribuiti alla Commissione (magari attraverso la fissazione di termini precisi che non rendano inefficace l'azione della stessa). Rispetto al **modello di governance**, è opportuno chiarire, in una logica di garanzia di efficacia d'azione, le modalità della cooperazione tra Commissione e Stati membri, forse anche mediante una maggiore valorizzazione del ruolo delle autorità nazionali di regolamentazione, oltre alle autorità antitrust.

Rispetto al **tema infrastrutturale**, rappresentando la diffusa disponibilità di reti performanti e sicure precondizione per la piena e definitiva affermazione del digitale, con la Comunicazione "*Bussola per il digitale 2030: il modello europeo per il decennio digitale*" la Commissione ha alzato l'asticella, fissando come obiettivo al 2030 la

copertura gigabit per tutte le famiglie europee e lo sviluppo di reti 5G in tutte le zone abitate. Se questi sono gli ambiziosi obiettivi fissati, in considerazione dell'ampia gamma di atti normativi che sono stati adottati nel tempo, si pone certamente un tema di **armonizzazione delle diverse discipline** e di **garanzia di chiarezza applicativa oltre che di uniformità a livello di scelte operate da parte dei singoli Stati membri**.

In tale logica si muove il lancio di una **nuova strategia in materia di cibersicurezza** e l'iniziativa di **revisione della direttiva NIS** intrapresa dalla Commissione al fine di superare l'attuale frammentazione normativa. La nuova strategia, in particolare, mira a rafforzare la resilienza collettiva dell'Europa contro le minacce informatiche e a contribuire a garantire che tutti i cittadini e tutte le imprese possano beneficiare al meglio di servizi e strumenti digitali affidabili. A tal fine, si individuano tre aree d'azione e numerose iniziative che mirano a rafforzare la resilienza e la sovranità tecnologica dell'UE e a sviluppare capacità operative di prevenzione, dissuasione e risposta. La proposta di modifica della direttiva NIS mira a rimuovere quelle differenze anche importanti in termini di applicazione dei principi e delle regole fissate dalla direttiva che esigono un'opera di armonizzazione. Il tutto per assicurare quella certezza e quell'uniformità indispensabili ad assicurare la competitività e l'attrattività dell'UE.

In questa logica, certamente condivisibili appaiono gli obiettivi strategici fissati, così come il superamento della distinzione tra operatori e fornitori di servizi essenziali e la scelta di introdurre una chiara distinzione tra soggetti essenziali e importanti, così come l'individuazione di misure minime di gestione dei rischi di cibersicurezza. Indispensabile appare l'**estensione dell'ambito applicativo a soggetti ulteriori** rispetto a quelli attualmente sottoposti alla direttiva NIS mentre rilevante risulta la predisposizione, da parte degli Stati membri, di piani nazionali di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala, la previsione di un registro delle vulnerabilità e di procedure di divulgazione coordinata delle vulnerabilità e l'istituzione del Gruppo di cooperazione che dovrebbe favorire la cooperazione e lo scambio di informazioni.

Molto rilevante anche la **proposta di direttiva sulla resilienza dei soggetti critici** che va a modificare la direttiva sulle infrastrutture critiche europee del 2008 estendendone sia l'ambito di applicazione, sia la profondità e che, andando ad innestarsi in un quadro normativo composito ad elevata complessità, impone un'attenta opera di chiarificazione dei contenuti delle discipline poste dai singoli atti normativi vigenti per scongiurare incertezze e dubbi applicativi.

Rispetto allo **sviluppo del 5G** e alla garanzia di elevati standard di sicurezza per tale evoluzione tecnologica, l'approccio europeo è certamente "*future oriented*" nella logica di garantire un ruolo da protagonista all'UE. Se il pacchetto di strumenti dell'UE (5G Toolbox) del febbraio 2020 ha individuato e descritto una serie di misure strategiche e tecniche, nonché di corrispondenti azioni di sostegno volte a rafforzare la loro efficacia e che possono essere attuate per attenuare i rischi, con il ***Connectivity Toolbox*** del 25 marzo scorso sono state indicate una serie di migliori pratiche per ridurre questi costi, promuovere l'accesso alle infrastrutture fisiche e snellire le procedure di concessione delle autorizzazioni per eseguire lavori civili. Si tratta di un risultato importante che ancora una volta persegue il fine di ridurre le differenze tra gli Stati membri e assicurare che l'UE riesca a competere tra i grandi nella partita del 5G.

Se rispetto agli ambiti appena analizzati appare profonda la consapevolezza e la maturità raggiunte a livello UE, c'è ancora molto da fare rispetto al **Fintech**, che sta assumendo un ruolo sempre più di primo piano sugli scenari globali. In

quest'ambito gli stati europei, e in particolare l'Italia, dovrebbero sostenere lo sviluppo del settore che altrimenti rischia di rimanere ad appannaggio esclusivo di aziende extra-europee.

Importante è anche l'ambito dei **pagamenti digitali** che hanno vissuto una forte crescita nell'ultimo anno ma che sono ancora residuali rispetto al contante. Ultima partita, che anche in questo caso, come continente, ci vede partire in ritardo, è quella delle **criptovalute di Stato**. In attesa che le *criptocurrency* commerciali rappresentino una realtà sufficientemente solida, le valute digitali emesse da una banca centrale potrebbero rappresentare il vero futuro della moneta. L'Unione europea in quest'ambito è ancora bloccata in una fase di studio mentre la Cina è già passata a una sperimentazione pratica che dovrebbe portare al lancio effettivo della nuova moneta entro il 2025.

GLI SCENARI DIGITALI ITALIANI

Scendendo ora al contesto nazionale italiano, le iniziative europee tese ad accelerare lo sviluppo delle **infrastrutture di TLC fisse e mobili** sono state declinate nella **nuova Strategia per la Banda Ultralarga** e nelle relative azioni, il **Piano Italia 1 Giga** per le reti fisse e il **Piano Italia 5G** per quelle mobili.

Per quanto concerne le reti fisse, l'iniziativa del governo appare particolarmente ambiziosa sia in termini di prestazioni, alzate fino a 1 Gbps, sia in termini di copertura (tutti i civici del Paese). L'obiettivo, migliorativo rispetto a quanto previsto dal **Digital Compass**, consiste nel raggiungere questo traguardo entro il 2026, sviluppando reti "*a prova di futuro*" che permetteranno a cittadini, imprese e pubblica amministrazione di fruire di servizi avanzati (video streaming HD, realtà virtuale e aumentata, smart working e formazione a distanza, *cloud computing*, *online gaming*, telemedicina, etc.). In effetti ne è passato di tempo dal Piano Banda larga del 2009, quando l'obiettivo consisteva nel dotare tutta la popolazione di una connessione ad almeno 2Mbps. Particolarmente lodevole, in questo senso, appare l'esercizio del Governo di ragionare in un'ottica "*quadri-dimensionale*", includendo anche la variabile temporale, nel progettare le reti non pensandole con gli occhi e con le esigenze di oggi, ma con quelle che potremo avere da qui a 10 anni almeno.

Guardando al bicchiere mezzo pieno, secondo i risultati della consultazione Infratel, **di qui al 2026 ben il 68% degli indirizzi civici italiani beneficerà, senza intervento pubblico, di una rete con prestazioni superiori a 1 Gbps**. Si tratta di un dato importante che mostra quante energie e risorse gli operatori italiani stiano investendo nella rete. Inoltre, grazie al lavoro di Infratel, si osserva come le consultazioni abbiano assunto un carattere più vincolante che in passato tanto che, al netto delle normali evoluzioni degli investimenti di mercato nel corso del tempo, è ragionevole ritenere che, ceteris paribus, le opere di infrastrutturazione da qui al 2026 si dovrebbero evolvere verosimilmente nella direzione emersa dalla consultazione.

Tra i nodi ancora da approfondire, occorrerà verificare l'oggettivo contributo che la tecnologia **Fixed Wireless Access (FWA)** potrà apportare da qui al 2026 in termini di connettività ad almeno 300 Mbps. Nel valutarne l'entità sarà opportuno considerare la maggiore (quasi doppia) rapidità di evoluzione delle tecnologie *wireless*, che si aggiornano in media ogni 5 anni, e l'effettiva praticabilità dell'infrastrutturazione per raggiungere ogni tipo di indirizzo civico, anche il più remoto, con tecnologie via cavo. A tal proposito, il trend evolutivo del **Piano aree bianche**, in cui è progressivamente aumentata (fino al 24%, per circa 2,2 milioni di unità immobiliari) la percentuale di civici coperti in FWA rispetto all'FTTH, indica come, a conti fatti, il FWA sia una tecnologia su cui continueremo a fare affidamento anche nel medio-lungo termine.

D'altra parte se, come mostrato dalla consultazione Infratel, si tratta di intervenire su oltre 6 milioni di indirizzi complessivi, quasi il 30% di quelli monitorati, di lavoro da fare ce ne sarà parecchio. Le risorse finalmente ci sono, sebbene siano ancora in discussione i meccanismi di assegnazione, che al momento verterebbero su di un modello *gap funding* che privilegerebbe consorzi e coinvestimenti. Tuttavia, al netto dei tempi burocratici che occorreranno all'espletamento e all'assegnazione dei bandi, i restanti 4 anni a disposizione per l'infrastrutturazione costituiscono un tempo assai limitato, in cui rischiano persino di non essere sufficienti le imprese e le risorse umane necessarie per effettuare tutte le opere e gli scavi che occorrerebbero.

Proprio per fronteggiare un tale *shortage* di competenze, potrebbe essere utile prevedere meccanismi incentivanti per ottimizzare il numero degli interventi e favorire la condivisione delle opere tra i diversi operatori, così come valutare opportune politiche di *reskilling* aziendale finalizzate ad aumentare la forza lavoro impegnata in queste mansioni.

Per quanto concerne le reti mobili, la sfida del 5G costituisce un momento epocale per comprendere chi governerà gran parte della nuova economia nel prossimo decennio, proprio nella fase in cui un'integrazione tra industria "*software*" e industria "*hardware*" appare sempre più verosimile.

Le caratteristiche proprie del 5G *stand alone* consentiranno un progressivo spostamento di settori tradizionali quali manifattura, agricoltura e sanità verso l'Internet delle cose, e presentano tutte le carte in regola per produrre l'auspicata rivoluzione industriale 4.0. In palio, secondo le stime GSMA ci sono circa 2,2 trilioni di dollari a livello mondiale tra il 2024 e il 2034, di cui 565 milioni provenienti dall'utilizzo delle bande sopra i 24 GHz. Le applicazioni che si prevede generino il maggior contributo sono l'**automazione industriale**, il **controllo da remoto dei dispositivi** e la **realtà virtuale**, mentre a livello settoriale, le stime indicano che i maggiori benefici dovrebbero provenire dalla **manifattura** e dalle **utilities**, dai **servizi professionali e finanziari** e dai **servizi pubblici**.

È una sfida che l'Italia giocherà a livello globale, in particolare nei confronti di Usa e Cina, ma anche a livello europeo, in termini di posizionamento all'interno dell'Unione. A tal proposito, occorrerà galoppare nell'implementazione delle reti 5G *stand alone* (laddove la copertura del 5G attualmente disponibile ha le caratteristiche di 4G "*potenziato*" ma non di un vero e proprio 5G), dettagliando inoltre apposite misure di sostengo alla domanda industriale, al momento accennate all'interno di PNRR e nuova Strategia BUL. In particolare, occorrerà agire tanto a livello economico, incentivando la domanda delle PMI e dei distretti industriali, quanto a livello normativo, per consentire la flessibilità necessaria alla costituzione del terreno fertile per favorire il coinvolgimento delle imprese provenienti dalle industrie verticali, insieme con la diffusione e l'affermazione di nuovi modelli di business e di nuove applicazioni industriali.

L'Italia si trova a giocare una partita importante anche rispetto alle **tecnologie abilitanti**. In attesa che le Strategie nazionali sull'intelligenza artificiale e sulla blockchain arrivino finalmente in porto, dopo un percorso di quasi tre anni dall'inizio dei lavori, a settembre è stata presentata la **Strategia cloud**, vero architrave del capitolo del PNRR dedicato alla digitalizzazione della pubblica amministrazione. Più in generale, nel contesto della pandemia, il ***cloud computing*** ha assunto una particolare valenza strategica, permettendo a imprese, pubbliche amministrazioni e cittadini europei di poter erogare e fruire servizi a distanza, e abilitando la diffusione dello smart working, che ha permesso

a gran parte delle attività economiche di continuare a operare nonostante le limitazioni imposte dai governi. Il *cloud computing* ha inoltre assunto una doppia veste sia in termini di abilitatore di servizi avanzati portatori di notevoli benefici economici, sia per la caratterizzazione geopolitica che ne è stata data anche in ambito europeo, con la volontà di favorire l'affermazione del principio di sovranità sui dati e il lancio del progetto Gaia-X.

La Strategia Cloud Italia, che si colloca proprio nel solco europeo, presenta alcuni profili di interesse sia per quanto concerne le classificazioni dei dati, sia in relazione alla creazione del **Polo Strategico Nazionale** (o all'identificazione dei soggetti titolari delle strutture già esistenti che lo comporranno). Per quanto concerne il primo aspetto, peraltro già auspicato da I-Com nello studio sul cloud che abbiamo pubblicato ad aprile, si osserva come questo avvenga sulla scorta del modello britannico, distinguendo tra dati ordinari, critici e strategici, in base al potenziale danno che una loro esfiltrazione provocherebbe al sistema Paese. Un tale approccio è considerato favorevolmente perché consentirà di tutelare tutte quelle funzioni che, se compromesse, potrebbero pregiudicare la continuità di funzioni dello Stato rilevanti per la società, senza però sfociare in derive autarchiche che avrebbero nel complesso indebolito la competitività e la resilienza del sistema-Italia.

A tal proposito, la competenza della classificazione spetterà alla nascente **Agenzia per la Cybersicurezza Nazionale**, il che lascia immaginare come i tempi non saranno brevissimi. Tale aspetto si collega a una seconda considerazione, relativa alle **tempistiche**. Alla presentazione della Strategia, avvenuta lo scorso 7 settembre, il Ministro Colao aveva auspicato l'arrivo di proposte per il PSN entro fine mese, puntualmente pervenute nei giorni scorsi. Nello specifico, analizzando in maniera combinata le tre fasi, si osserva come la Strategia non specifichi quanta parte del PSN dovrà essere realizzata da zero e quanto verrà mutuata dalle infrastrutture esistenti. Infatti, poiché l'aggiudicazione (fine 2022) e l'inizio della migrazione (inizio 2022) risultano consequenziali, sembrerebbero non contemplati i tempi di implementazione di nuove infrastrutture, e che quindi le operazioni potrebbero consistere nel *set-up* e nel coordinamento di infrastrutture esistenti (o che verranno realizzate in corso d'opera). Non è forse casuale, dunque, che le proposte puntino sul proprio potenziale infrastrutturale. Quella del consorzio Almaviva-Aruba fa esplicito riferimento – oltre che alla totale italianità delle società coinvolte – all'immediata disponibilità delle infrastrutture, che consentirebbe il conseguimento dei risultati richiesti entro tempistiche persino migliorative rispetto alla pianificazione prevista nella Strategia Cloud. È evidente che, se non un'accelerazione, almeno un preciso rispetto dei tempi appaia ampiamente auspicabile, anche in considerazione della portata che l'iniziava assumerà, soprattutto a livello di Pubblica Amministrazione. Il passaggio al cloud per certi aspetti assumerà i connotativi di una vera e propria **rivoluzione**, capace di generare, oltre a notevoli benefici economici in termini di risparmi, anche un deciso salto della PA verso la digitalizzazione, sull'onda della propulsione generata dal Covid e delle molteplici iniziative previste dal PNRR.

Inoltre, non è chiaro il rapporto tra il Polo Strategico Nazionale e il *marketplace* e quanto il primo si sostituirà o avrà priorità sul secondo. Escludendo ovviamente il tema dei dati più sensibili, che è giusto sottoporre al livello di protezione maggiore possibile, a prescindere da altre considerazioni, una scelta troppo dirigista rischierebbe di portare l'Italia in una direzione diversa da quella percorsa da altri Paesi, riducendo sia la concorrenza che l'innovazione.

Rispetto al t**ema sicurezza**, invece, è in fase di completamento, mancando all'appello un solo

DPCM, la procedura di adozione dei vari decreti che andranno a completare il puzzle normativo che consentirà la piena operatività della disciplina istitutiva del perimetro di sicurezza nazionale cibernetica. Si tratta di un *iter* a elevata complessità che, complice anche la pandemia ancora in atto, ha subito importanti ritardi che esigono di essere recuperati così da fornire al mercato e agli utenti quella certezza indispensabile a investire e a utilizzare con fiducia reti e servizi di ultima generazione. Oltre all'esigenza di accelerare e portare a compimento la procedura di adozione di tutti gli atti previsti dalla normativa primaria, si pone anche un tema di armonizzazione con l'attuale quadro normativo vigente che ruota intorno al *golden power* e che impone una riflessione sulle varie interazioni e punti di contatto esistenti al fine di scongiurare il rischio che tale complessità normativa possa tradursi in un ostacolo all'innovazione ed agli investimenti nel nostro Paese.

Quanto invece alla neocostituita Agenzia, è straordinariamente rilevante, per l'effetto semplificatore e chiarificatore che ad essa si accompagna, la ridefinizione del quadro normativo in materia di sicurezza operata con il **D.L. n. 82/2021** che finalmente ha consentito il superamento di un sistema altamente complesso che vedeva polverizzate tra una miriade di soggetti diversi le competenze in materia di cybersicurezza in favore di un nuovo modello incentrato su un unico soggetto munito di tutte le competenze in materia di cybersicurezza. Se la scelta è encomiabile e le finalità assolutamente condivisibili, a preoccupare sono le tempistiche necessarie a rendere effettivamente operativa l'Agenzia e, dunque, tutti i connessi rischi e le risorse, probabilmente non adeguate, da destinare all'esercizio delle numerosissime e complesse funzioni alla stessa assegnate.

i-com
reti & servizi di nuova generazione

PARTNER

eolo FACEBOOK

Google Hewlett Packard Enterprise

iliad linkem

open fiber

i-com
istituto per la competitività

Roma
Piazza dei Santi Apostoli 66 - 00187
+ 39 064740746
www.i-com.it

Bruxelles
Square de Meeûs 37 - 1000
+32 (0)2 791 9870
www.icomRU.eu

info@i-com.it