icom
istituto per la competitività

RAPPORTO OSSERVATORIO
RETI E SERVIZI DI NUOVA GENERAZIONE

IL DIGITALE CHE VOGLIAMO

Le sfide del sistema Paese tra politiche UE e nuove frontiere tecnologiche

OTTOBRE 2023

icom
istituto per la competitività

RAPPORTO OSSERVATORIO
RETI E SERVIZI DI NUOVA GENERAZIONE

IL DIGITALE CHE VOGLIAMO

Le sfide del sistema Paese tra politiche UE e nuove frontiere tecnologiche

OTTOBRE 2023

CURATORI
Stefano da Empoli
Silvia Compagnucci
Domenico Salerno

AUTORI
Stefano da Empoli
Silvia Compagnucci
Alessandro D'Amato
Maria Rosaria Della Porta
Enrica Lipilini
Domenico Salerno
Daniela Suarato
Valerio Vinco

SI RINGRAZIA
ByTek per il paragrafo 2.4, contenente l'approfondimento sull'interesse degli utenti verso l'Intelligenza Artificiale

Il presente report è aggiornato alla data del 15 ottobre 2023

I-Com Edizioni

ISBN 9791280680105
Ottobre 2023

INDICE

EXECUTIVE SUMMARY

CAPITOLO 1

Nel 2022 il processo di digitalizzazione ha continuato a mostrare una tendenza positiva, confermata dai tassi di crescita nell'adozione delle tecnologie digitali, sia da parte dei cittadini che delle imprese a livello dell'Unione Europea. Osservando la **percentuale di individui che utilizzano internet tutti i giorni in Europa**, notiamo come questa sia significativamente cresciuta passando **dal 46% del 2009 all'85% nel 2022**. Soprattutto negli ultimi anni, si registra un netto aumento nell'utilizzo di internet per svolgere una serie di attività specifiche**,** tra cui fruire di **contenuti video on demand; giocare o scaricare videogiochi, seguire corsi online; accedere a materiale didattico e partecipare a programmi di formazione.** L'aumento nell'utilizzo di internet ha anche innescato una **crescente adozione di dispositivi connessi**, contribuendo così a ridefinire il nostro modo di interagire con la tecnologia nella quotidianità. Questi dispositivi includono **smart TV**, **assistenti virtuali**, e una **vasta gamma di dispositivi IoT**. Si è anche assistito a una significativa evoluzione nelle preferenze degli utenti riguardo ai **dispositivi digitali**: i dati recenti indicano un drastico calo nell'uso di PC e tablet, a favore di un **crescente utilizzo degli smartphone.** Nel 2022, circa il 52% del totale delle pagine web è stato visualizzato tramite cellulare, il 46% tramite computer portatile o fisso e solo il 2% tramite tablet.

L'accelerazione nel processo di digitalizzazione ha riguardato anche le imprese. Tuttavia, al 2022, la percentuale di imprese con 10 o più addetti che presenta un **livello di intensità digitale "molto alto"** è ancora piuttosto bassa in tutti i paesi europei. La transizione digitale porta inevitabilmente con sé un **aumento della superficie di attacco e nuove forme di minacce cibernetiche**, che possono causare una serie di ripercussioni potenzialmente gravi non solo per il soggetto pubblico o privato colpito, bensì per l'intera supply chain. L'ultimo rapporto del Clusit (marzo 2023) consente di affermare che **il 2022 è stato l'anno peggiore di sempre per la cibersicurezza a livello globale**, dato che tra 2021 e il 2022 si è registrato un aumento delle azioni malevole del 21,5%, oltre il doppio di quello riscontrato nel periodo precedente. In tale contesto, **l'Europa si posiziona al terzo posto, attraendo il 24% delle azioni degli attori malevoli, in crescita del 3% rispetto all'anno precedente.** Ciò premesso, l'ultima versione dell'ENISA *"NIS Investments report"* (novembre 2022), consente di analizzare gli investimenti in cybersecurity delle imprese ricomprese nell'ambito di applicazione della Direttiva NIS. Tali soggetti **hanno destinato mediamente il 7,82% del proprio budget IT alla cybersicurezza nel 2021, evidenziando una netta diminuzione rispetto al 2020 (anno nel quale il dato era pari all'8,8%).** Un altro importante indicatore circa l'andamento degli investimenti in cibersicurezza può essere rappresentato dal volume di ricavi che ha generato questo mercato globalmente. Infatti, le ultime stime effettuate da Statista attestano i ricavi globali in cybersicurezza a circa €139,5 miliardi, mostrando un trend in forte crescita, che dovrebbe far registrare un importante raddoppio entro il 2026. **Quanto al mercato europeo, esso occupa stabilmente il secondo posto dal 2016, avendo raggiunto €20,9 miliardi di ricavi nel 2022, quasi il doppio della Cina**.

Infine, per quanto concerne la **digitalizzazione dei servizi pubblici**, i dati della *Digital Agenda Scoreboard* del 2022 mostrano una **situazione nel complesso favorevole**, sia in relazione ai servizi offerti ai cittadini, sia per quanto riguarda i servizi offerti alle imprese. L' offerta di servizi pubblici digitali è fondamentale per garantire a imprese e cittadini un'efficiente interazione con la Pubblica Amministrazione, ma da sola non è sufficiente. Per sfruttare appieno le opportunità offerte dalla

trasformazione digitale del settore pubblico, è **fondamentale che l'offerta si evolva parallelamente alla domanda**. In Italia, la percentuale di individui che nel 2022 ha utilizzato internet per interagire con le pubbliche autorità, è pari al **76,3%**, leggermente superiore alla **media europea del 74,2%.**

CAPITOLO 2

L'**intelligenza artificiale** è sicuramente una delle più strabilianti frontiere tecnologiche degli ultimi tempi e i suoi ambiti applicativi sono davvero innumerevoli e spaziano dal campo della sanità a quello dell'internet of Things, dal campo del fintech e dell'insurtech, fino a quello della privacy e della sicurezza informatica, con impatti importanti sulle attività di imprese e pubbliche amministrazioni, oltre che sulla vita delle persone.

Basti pensare, ad esempio, ai benefici dell'IA in ambito sanitario, ambito nel quale diventa un supporto fondamentale per i medici nel prendere le decisioni e consente diagnosi più precise grazie all'analisi dei dati clinici dei pazienti, favorendo così sempre di più una medicina personalizzata.

Le potenzialità dell'IA si esprimono anche in ambito fintech e insurtech così come nell'e-commerce ma anche nel settore della cybersecurity le tecnologie intelligenti giocano un ruolo fondamentale nella risposta alle minacce informatiche.

Dunque tante sono le opportunità legate all'intelligenza artificiale, insieme a non poche sfide, di ordine etico e legale (tra cui questioni legate alla privacy, sicurezza, responsabilità) che necessitano di essere considerate per poter sfruttare pienamente il potenziale di questa tecnologia.

Il crescente interesse nei confronti delle numerose applicazioni IA è confermato anche dai dati. Stando ad alcune stime, si prevede che il **mercato mondiale dell'intelligenza artificiale** toccherà i $241,80 miliardi entro la fine del 2023 e crescerà ad un tasso di crescita annuale (CAGR 2023-2030) del 17,3%, raggiungendo un volume di mercato di $738,80 miliardi entro il 2030.

A trainare principalmente tale crescita saranno le applicazioni basate sulle tecniche di machine learning.

Nel confronto globale, gli **Stati Uniti** coprono il 36% del mercato IA, seguiti da **Cina** (12%), **Germania** (4%) e **Regno Unito** (4%). L'**Italia** non va oltre il 2%, posizionandosi comunque all'ottavo posto a pari merito con l'Australia. Tuttavia, tenendo conto delle dimensioni della popolazione di ciascun paese, la **Danimarca** è il più grande mercato dell'IA a livello globale, con un valore di mercato per 100.000 abitanti di circa 39 milioni di dollari, seguita da **Finlandia** e **Irlanda.**

Negli ultimi anni il mercato complessivo dell'IA è fortemente trainato dall'**IA generativa** che, copre, infatti, il 19% del mercato IA totale nel 2023 e secondo le stime arriverà ad un'incidenza del 28% entro il 2030. Tra i principali Stati membri, la **Germania** è il più grande mercato dell'IA generativa (22% del mercato totale europeo), seguita da **Francia** (14%) e **Italia** (10%).

Sul fronte degli **investimenti venture capital in IA**, gli **Stati Uniti**, investono circa cinque volte l'importo investito in **Cina** e undici volte l'importo investito nell'**UE**. Tra i Paesi UE, la **Francia**, la **Germania** e la **Svezia** si collocano sul podio con un volume di investimenti venture capital che complessivamente copre circa il 65% degli investimenti VC totali in UE. L'**Italia** si classifica in ottava posizione dietro a paesi come **Romania**, **Spagna** e **Irlanda**.

Anche in termini di **startup IA**, gli **Stati Uniti** continuano a guidare la classifica mondiale con 542 fondate nel 2022. Seguono **Cina** e **Regno Unito**, rispettivamente con 160 e 99 startups IA.

I **principali Paesi UE per numero di startup (Francia**, **Germania**, **Paesi Bassi** e **Svezia)** seguono a netta distanza con un numero di nuove imprese finanziante nel 2022 che non rappresentano nemmeno ¼ di quelle statunitensi. L'**Unione Europea** continua pertanto a far fatica a stare al passo con Stati Uniti e Cina, nonostante stia mostrando una maggiore specializzazione nell'intelligenza artificiale rispetto al passato.

Nel 2021, stando agli ultimi dati Eurostat, solo **l'8%**

delle imprese UE ha adottato almeno una tecnologia IA. Il tasso di adozione più elevato si registra in **Danimarca**, dove circa un'impresa su quattro ha fatto uso di almeno una tra le tecnologie intelligenti più comuni. Contrariamente, in **Romania** si riscontra il livello più basso di adozione IA con solo l'1,5% di imprese che ha utilizzato almeno una tecnologia. L'**Italia** si colloca al di sotto della media UE, con circa il 6% delle imprese che ha adottato almeno una tra le tecnologie IA a disposizione. Tuttavia, nella **robotica di servizio** il nostro Paese supera la media UE e il boom di installazioni di robot di servizio, soprattutto nel settore dell'hospitality, è confermato anche dall'IFR (la Federazione Internazionale di Robotica).

L'attrattività dell'IA non si esaurisce solo nell'ambito imprenditoriale ma coinvolge la società nel suo complesso.

Un'indagine realizzata da Bytek e I-Com e che prende in considerazione cinque Paesi (**Italia**, **Stati Uniti**, **Francia**, **Germania** e **Spagna**) **ha avuto l'obiettivo di comprendere quanto sia centrale il tema dell'intelligenza artificiale** soprattutto in un momento storico, come quello attuale, molto particolare, in cui il lancio di ChatGPT di Open AI e poi quello di Google Bard hanno acceso i riflettori, come mai prima di oggi, su questa nuova frontiera tecnologica e influenzato la percezione degli individui. L'analisi, basata su **dati raccolti in rete da Bytek**, valuta la dinamica del volume delle ricerche effettuate sul motore di ricerca di Google in termini di argomenti relativi all'IA.

Il primo dato interessante che emerge è relativo al **numero totale di ricerche** effettuate in rete sull'intelligenza artificiale, che ha subito una vera e propria impennata in tutti i Paesi oggetto dell'analisi (eccetto la Germania) tra il terzo e il quarto trimestre 2022, periodo coincidente con il lancio di ChatGPT. Gli Stati Uniti guidano la classifica con il maggior numero di ricerche in termini assoluti. Parametrando le ricerche totali sull'IA rispetto alla popolazione, nel primo semestre 2023 gli Stati Uniti continuano a rappresentare il paese in cui si è registrato il maggior interesse generale verso l'argomento, con oltre 60 mila ricerche ogni 100.000 abitanti. Seguono la **Francia** e l'**Italia** con rispettivamente 51.506 e 33.950 ricerche pro-capite effettuate nel corso del primo semestre dell'anno in corso.

L'interesse nei confronti dell'intelligenza artificiale sta sicuramente aumentando grazie all'avvento dell'**intelligenza artificiale generativa** che sta influenzando il settore sotto tanti punti di vista. Interesse davvero sorprendente negli **Stati Uniti**, dove le ricerche online del termine "generative AI" sono cresciute in modo esponenziale a partire da ottobre 2022 e pongono la prima superpotenza mondiale in vetta anche in termini relativi. Laddove, invece, in **Italia**, **Spagna** e **Francia** l'interesse è molto meno diffuso anche se negli ultimi mesi la tendenza a ricercare informazioni online sull'IA generativa è in aumento.

Altro aspetto interessante che emerge dall'analisi delle ricerche effettuate sul web relativamente al tema dell'intelligenza artificiale riguarda la **formazione**. In tutti i Paesi analizzati si nota a partire dal secondo trimestre 2022 un aumento delle ricerche online relative a corsi di formazione di vario tipo (inclusi quelli universitari) sull'IA. Anche in questo caso, gli **Stati Uniti** guidano la classifica. Tuttavia, in termini relativi, anche la **Francia** mostra particolare interesse nei confronti della formazione in IA con 7 ricerche online ogni 100.000 abitanti collocati nella fascia d'età lavorativa.

L'interesse nei confronti della formazione in IA è sicuramente correlato alle **opportunità** specie lavorative che questa nuova frontiera tecnologica può offrire (oltre alla necessità di dover adeguare le proprie competenze per non rimanere indietro). In particolare, in **Italia**, **Spagna**, **Francia** e **Germania**, la stragrande maggioranza delle ricerche relative alle opportunità IA riguarda appunto il mondo del lavoro, quindi **possibilità di impiego nel settore dell'IA**. Solo negli Stati Uniti, le ricerche si concentrano prevalentemente su informazioni relative ad **opportunità di investimento** nel settore dell'IA.

Il dibattito sull'intelligenza artificiale non si ferma però solo alle opportunità, ma analizza a fondo anche i **rischi** ad essa associati, pertanto non è scontato che si diffonda nella società un **sentimento di paura nei confronti delle tecnologie IA**. Dall'analisi delle ricerche online correlate alla paura verso l'IA, emerge che queste sono in aumento in tutti i Paesi analizzati, pur mantenendosi a un livello ancora piuttosto basso. Ecco dunque che negli **Stati Uniti**, 27 ricerche su 100.000 abitanti riguardano un sentimento di paura legato al fenomeno IA. Seguono la **Francia** e la **Spagna** con rispettivamente 20 ricerche correlate alla paura dell'IA ogni 100.000 abitanti. Mentre in **Italia** il numero di ricerche correlate alla paura si ferma a 17 ogni 100.000 abitanti. Nel nostro Paese il 34% delle ricerche relative alla paura dell'IA riguarda il **rischio di perdere il posto di lavoro** a causa dell'avvento delle tecnologie intelligenti.

CAPITOLO 3

Nonostante **ad oggi non esista ad oggi una definizione univoca di cosa sia il metaverso**, gli utenti del web sembrano avere già un'idea chiara di quali potrebbero essersene **i principali benefici**. Da una survey effettuata da Tidio intervistando 1.050 utenti di internet a livello globale, è emerso come **il 39% dei rispondenti ritiene che nel metaverso potranno fare esperienze altrimenti irrealizzabili nel mondo reale**, mentre il 37% crede che si potrà girare il mondo senza muoversi, nonché migliorare la creatività e immaginazione. Tuttavia, le principali ragioni per entrare nel metaverso da parte dei consumatori fanno pensare che **questo non venga percepito semplicemente come uno spazio destinato a fini ludici**, bensì anche come **un'opportunità professionale e di investimento**. Lo studio di Tidio citato in precedenza indica come la motivazione prioritaria per entrare nel metaverso sia costituita dalle **opportunità di lavoro** che potrebbero scaturire da questo nuovo ecosistema (52%), seguite al terzo posto da investimenti in NFT e criptovalute (44%) e al quarto dalla "Formazione Scolastica", selezionata da ben il 40% dei rispondenti.

Nonostante rappresenti ancora un concetto piuttosto astratto, il metaverso (pur nei differenti perimetri che gli vengono attribuiti) sembra avere già una dimensione economica di rilievo: **secondo le previsioni di mercato diffuse ad agosto 2023 da Statista, il metaverso presenta ad oggi ricavi a livello globale pari a €42,4 miliardi**, che potrebbero diventare €471,3 entro la fine del decennio. Tra le tecnologie che permetteranno ai consumatori di vivere a pieno l'esperienza immersiva del metaverso ci sono certamente la **realtà virtuale e la realtà aumentata**. La correlazione tra questi mondi appare chiarissima soprattutto guardando le previsioni di mercato collegate alla diffusione di questi device. Secondo Statista, nei prossimi anni **i ricavi dell'AR e della VR a livello globale potrebbero vedere una netta impennata, passando dai €23,9 miliardi del 2022 a quota €49,9 miliardi nel 2026**.

Nella corsa al metaverso, **l'Italia non performa bene rispetto alle altre principali economie UE**. Infatti, non solo si posiziona dietro Germania e Francia in relazione ai ricavi in valori assoluti ma viene superata anche dalla Spagna in termini di ricavi sul PIL.

L'evoluzione e l'espansione del metaverso comporterà una serie di implicazioni per diverse aree del diritto. Al netto delle generali criticità e rischi connessi al tema della sicurezza, il primo ambito di assoluta rilevanza concerne senza dubbio la **privacy, la tutela dei dati personali**, oltre alla disciplina sull'**identità digitale**, sulla **proprietà intellettuale** e sull'utilizzo improprio dell'**immagine**, di **marchi** e di altri segni distintivi. È interessante evidenziare che alcuni usi dell'IA rilevanti per il metaverso saranno vietati se potenzialmente suscettibili di violare i diritti fondamentali degli individui, in osservanza delle regole descritte dall'**AI Act** per i sistemi di IA giudicati "**ad alto rischio**". Posto che infrastruttura essenziale per l'esistenza stessa del metaverso è il cloud computing e che il metaverso presenta il potenziale per diventare

un infinito ***marketplace***, si pone anche il tema dell'adeguamento alle nuove regole stilate dal legislatore europeo con l'adozione del **DMA**. Per giunta, il **DSA** ha introdotto un quadro orizzontale per tutte le categorie di contenuti, prodotti, servizi e attività sui servizi di intermediazione nel quale viene delineato un regime di responsabilità diversificato in base ai servizi offerti ed alla dimensione del fornitore ed ha introdotto obblighi di trasparenza, organizzativi e procedurali adattabili alle peculiarità del metaverso. Peraltro, dovrà essere posta particolare attenzione verso la **resilienza delle infrastrutture fisiche e digitali** che permettono l'operatività e il funzionamento del metaverso, per cui è auspicabile che si ragioni su standard e regole giuridiche inerenti la **sicurezza di reti, sistemi e servizi** sia da un punto vista prettamente cibernetico (sul modello della **Direttiva NIS2**), ma anche con riguardo alla **protezione fisica delle stesse** (**Direttiva CER**). Sarà di cruciale importanza garantire la **sicurezza dei dispositivi e dei sensori** che gli utenti dovranno necessariamente utilizzare per sfruttare appieno le opportunità del metaverso. Infatti, in quest'ottica, le istituzioni europee stanno finalizzando la proposta di **Cyber-Resilience Act**. A imprimere una prima svolta a livello comunitario è stata **la Commissione**, che **l'11 luglio scorso** ha presentato **la prima strategia sul Web 4.0 e i mondi virtuali**. Al suo interno viene fatta una differenza tra i concetti di **virtual worlds**, **Web 3.0** e **Web 4.0**, individuando quattro linee d'azione: affidare alle persone più potere e rafforzare le **competenze** per aumentare l'**awareness**, l'accesso a informazioni affidabili e costituire un centro di talenti capaci di giostrare il mondo virtuale; sostenere un **ecosistema industriale Web 4.0** per aumentare l'eccellenza delle **imprese** e combattere il grave problema della frammentazione; contribuire al pieno sostegno del **progresso sociale** e dei **servizi pubblici virtuali**; promuovere la creazione di **standard globali**, assicurando che i mondi virtuali e il Web 4.0 non siano dominati da pochi grandi attori.

CAPITOLO 4

In un contesto che si nutre di tecnologie sempre più sofisticate, la cui potenza risiede innanzitutto nella capacità di raccogliere e analizzare moli enormi di dati ed in un panorama internazionale che incentra gran parte della propria competitività sullo sviluppo e l'offerta delle nuove tecnologie e dei servizi ad esse correlati, lo **sviluppo di reti di telecomunicazione capillari e performanti costituisce una condizione imprescindibile** per l'Unione Europea in generale e per l'Italia in particolare. Partendo da tali constatazioni, l'UE ha fissato obiettivi ambiziosi per il 2030 che si sostanziano in una copertura gigabit per tutti e reti 5G performanti in tutte le aree popolate. Se questi sono gli obiettivi e le tempistiche per il raggiungimento degli stessi, emerge a livello europeo ancora una **forte disomogeneità** e, in generale, la necessità, per essere all'altezza dei competitor internazionali, primi tra tutti Cina e Stati Uniti, di **accelerare** lo sviluppo delle reti VHCN e del 5G. Rispetto alla **copertura VHCN**, infatti, il dato europeo si attesta, nel 2022, al 73,4% (53,7% in Italia) mentre per la **copertura FTTP** si ferma al 56,5% (la copertura italiana si attesta al 53,7). Ancor più allarmanti i dati relativi alle aree rurali dove la copertura VHCN 2022 si ferma al 45% e quella italiana addirittura al 26% mentre la copertura FTTP si attesta al 41% a livello UE (l'Italia registra un modesto 26%). Se si analizza il **take up** la situazione è decisamente più preoccupante, con una percentuale di abbonamenti ad almeno 100 Mbps sul totale di abbonamenti alla rete fissa che a livello europeo non va oltre il 55,1% (Il'Italia si pone poco sopra il dato europeo con una percentuale del 59,6%).

Lato 5G invece, se da un lato appaiono confortanti i dati relativi alla 5G readiness che dimostrano come le procedure di assegnazione delle frequenze 5G (700 MHz, 3,6 GHz e 26 GHz) siano state completate o siano ad un buon grado di avanzamento in molti paesi UE, positivi risultano i dati di copertura 5G, soprattutto in termini di accelerazione a partire dal 2020.

Ed infatti, sebbene con la doverosa precisazione che i dati non tengono conto della distinzione tra le coperture realizzate in modalità standalone e non-standalone, la **percentuale di copertura 5G in termini di famiglie raggiunte è passata a livello europeo dal 14% del 2020 all'81,2% nel 2022,** a dimostrazione degli enormi sforzi compiuti dagli operatori. L'Italia, in particolare, è passata dall'8% del 2020 a ben il 99,7% di copertura 5G, risultando quarta in Europa, dopo Cipro, Malta e Paesi Bassi con rispettivamente il 100% ed il 99,9% di copertura 5G. Interessante evidenziare, alla luce delle diverse caratteristiche delle frequenze destinate ai servizi 5G, come la **copertura 5G sulle frequenze 3,4-3,8 Ghz** si attesti al 41% con ben 15 paesi che registrano un dato inferiore alla media, mentre a primeggiare sono Finlandia, Italia e Danimarca con rispettivamente 84, 80 e 75% di copertura. Ciò dimostra quanto sia importante accelerare, per garantire l'effettiva possibilità di offrire e fruire dei servizi abilitati dalle reti 5G.

CAPITOLO 5

Nell'affrontare la sfida della digitalizzazione, l'UE sta cercando di creare un ecosistema normativo quanto più possibile armonizzato e tutelante ed al contempo *innovation oriented*. Si tratta di una sfida ambiziosa che punta a governare il processo di digitalizzazione, nel tentativo di accelerare lo sviluppo delle reti e rendere l'UE leader nello sviluppo e nell'impiego delle nuove tecnologie.

Per quanto attiene le reti, lo scorso 23 febbraio la Commissione ha lanciato il "**Connectivity Package**" che si compone di una proposta di regolamento che fornirà nuove norme per consentire una diffusione più rapida, economica ed efficace delle reti Gigabit in tutta l'UE (**Gigabit Infrastructure Act**), un **progetto di raccomandazione sulla connettività Gigabit** teso a fornire orientamenti alle autorità nazionali di regolamentazione sulle condizioni di accesso alle reti di telecomunicazione degli operatori che detengono un significativo potere di mercato, al fine di incentivare un più rapido abbandono delle tecnologie preesistenti e una diffusione accelerata delle reti Gigabit ed una **consultazione esplorativa sul futuro del settore della connettività e delle relative infrastrutture** per raccogliere opinioni sul modo in cui l'aumento della domanda di connettività e i progressi tecnologici potrebbero incidere sulle esigenze e sugli sviluppi futuri. La proposta di regolamento, in particolare, impatta sulle procedure autorizzative e sulle relative tempistiche, disciplina il coordinamento tra operatori nella realizzazione delle opere civili e detta le regole per le sanzioni e le procedure di risoluzione delle controversie in materia. Il dossier sulla proposta della Commissione è stato attribuito, in Parlamento europeo, alla Commissione per l'Industria, la Ricerca e l'Energia (ITRE) che il 29 settembre scorso ha adottato la propria posizione introducendo una serie di proposte di modifica tra cui si segnalano, per il dibattito che stanno alimentando, l'esplicito riferimento, in una logica di garanzia del principio di neutralità tecnologica, alla necessità di implementare reti ad altissima velocità con performance almeno equivalenti a quelle del 5G ed il riconoscimento della possibilità, per gli Stati membri, di operare scelte più ambiziose rispetto ai requisiti minimi richiesti (ad es. fissando termini più stringenti per il rilascio delle prescritte autorizzazioni). Per quanto attiene la consultazione sopra citata, il 10 ottobre scorso è stata pubblicata dalla Commissione europea la sintesi della consultazione pubblica esplorativa sul futuro della connettività cui hanno preso parte 108 imprese, tra ECN provider e OTT, associazioni di imprese, cittadini sia europei che extraeuropei, organizzazioni non governative, istituti di ricerca, organizzazioni di consumatori e Autorità, di diversi settori e ambiti locali nell'ambito della quale uno dei temi più rilevanti è il cosiddetto **fair share**. In particolare, nella consultazione è emersa la contrapposizione tra quanti si sono mostrati contrati alla luce di considerazioni economiche, tecniche e

di neutralità della rete oltre che dei possibili impatti sul mercato dei contenuti e quanti, al contrario, ritengono che il meccanismo di pagamento ipotizzato avrebbe un impatto positivo sull'intero ecosistema in quanto verrebbero incentivati gli investimenti in tecnologie più efficienti.

Se le reti costituiscono il fattore abilitante la transizione digitale, i dati ne costituiscono la linfa vitale essendo oggetto, a partire dal lancio della strategia nel 2020, di importanti interventi normativi dapprima con il **Data Governance Act** (Reg. n. 2022/868) che ha istituito e disciplinato un meccanismo per il riutilizzo di determinate categorie di dati protetti detenuti da enti pubblici e, successivamente, il 23 febbraio scorso, con il lancio della proposta di **Data Act**, su cui Parlamento e Consiglio hanno raggiunto un accordo politico nel giugno scorso. Il regolamento proposto, in particolare, nella logica di favorire la circolazione dei dati, disciplina la condivisione dei dati da impresa a consumatore e da impresa ad impresa, regola il diritto di condividere i dati con terzi ed istituisce un quadro armonizzato per l'utilizzo, da parte degli enti pubblici e delle istituzioni, agenzie e organismi dell'Unione, dei dati detenuti dalle imprese, in situazioni in cui vi sia una necessità eccezionale dei dati richiesti. Parlamento e Consiglio, dopo non poche difficoltà, nel giugno 2023 hanno trovato un accordo provvisorio (cui seguirà l'approvazione definitiva da parte di entrambe le istituzioni europee) su una serie di punti in merito alla definizione del campo di applicazione del regolamento, la previsione di misure volte ad impedire l'abuso degli squilibri contrattuali nei contratti di condivisione dei dati, l'individuazione di mezzi che consentono agli enti pubblici, alla Commissione, alla Banca centrale europea e agli organismi dell'Unione di accedere ai dati detenuti dal settore privato ed utilizzarli, ove necessario, in circostanze eccezionali come emergenze pubbliche quali inondazioni e incendi boschivi per svolgere un compito di interesse pubblico e la definizione di ulteriori orientamenti in merito al compenso ragionevole per le imprese per la messa a disposizione dei dati, nonché ad adeguati meccanismi di risoluzione delle controversie.

I dati costituiscono il vero carburante di una serie di tecnologie tra cui spicca, per importanza ed opportunità applicative, l'**Intelligenza Artificiale**, rispetto alla quale l'UE è attualmente impegnata ad adottare la prima forma di regolamentazione al mondo, l'**Artificial Intelligence Act** (AI Act). Si tratta di un regolamento che declina obblighi diversificati che seguono un approccio basato sul rischio, che distingue tra usi dell'IA che creano un rischio inaccettabile, un rischio elevato ed un rischio basso o minimo, da cui discendono obblighi di intensità crescente, prescrive l'istituzione, prescrive 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, definisce obblighi anche in capo agli utilizzatori di sistemi di IA ad alto rischio evidenziando la necessità di utilizzare tali sistemi conformemente alle istruzioni per l'uso ed istituisce a livello dell'Unione un Comitato europeo per l'intelligenza artificiale.

Il 6 dicembre 2022 il Consiglio ha adottato il proprio orientamento generale formulando una serie di importanti proposte di modifica tra cui l'esclusione dal campo di applicazione della legge sull'IA degli scopi di sicurezza nazionale, difesa militare e autorità di contrasto, l'estensione ai privati del divieto di utilizzare l'IA per il social scoring, una più puntuale definizione dei requisiti di IA ad alto rischio, l'inserimento di nuove disposizioni tese a considerare le situazioni in cui i sistemi di IA possono essere utilizzati per scopi diversi (IA per scopi generali), l'inserimento di nuove disposizioni per accrescere la trasparenza e accogliere i reclami degli utenti, l'introduzione di importanti modifiche alle disposizioni riguardanti le misure a sostegno dell'innovazione (es. sandbox normative).

Anche il Parlamento ha adottato la propria posizione (nel giugno 2023), introducendo anch'esso modifiche sostanziali al testo proposto dalla Commissione, tra cui la modifica dell'elenco dei sistemi di intelligenza artificiale vietati nell'UE al fine di includervi i sistemi di identificazione biometrica nell'UE sia per l'uso in tempo reale che ex post (tranne in casi di criminalità grave e previa autorizzazione giudiziaria per l'uso ex post) e non solo per l'uso in tempo reale come proposto da parte della Commissione. Il Parlamento, in particolare, ha proposto di vietare tutti i sistemi di categorizzazione biometrica che utilizzano caratteristiche sensibili, sistemi di polizia predittiva, sistemi di riconoscimento delle emozioni e sistemi di intelligenza artificiale che utilizzano lo scraping indiscriminato di dati biometrici dai social media o filmati CCTV per creare database di riconoscimento facciale.
Attualmente sono in corso i triloghi tra i legislatori UE che dovrebbero concludersi prima della fine dell'anno con un accordo.
Molto importante, nella logica di favorire l'accesso ai servizi digitali, la procedura di revisione del quadro eiDAS attraverso la proposta di regolamento lanciata il 3 giugno del 2021 istituendo un quadro normativo per la creazione di uno strumento europeo di identità digitale armonizzato, basato sul concetto di portafoglio europeo di identità digitale "**EUDI wallet**".
Altro ambito particolarmente nutrito di iniziative riguarda la **cybersecurity**, a partire dal 2020, anno in cui la Commissione europea ha lanciato il "Cybersecurity package", costituito dalla "Strategia dell'UE in materia di cibersicurezza per il decennio digitale", una nuova direttiva sulla resilienza delle entità critiche ed una proposta di direttiva relativa alle misure necessarie per conseguire un elevato livello comune di cibersicurezza in tutta l'Unione (direttiva NIS rivista).
All'esito di un ampio ed articolato dibattito, il 27 dicembre 2022 è stata pubblicata sulla G.U. dell'UE la Direttiva n. 2557/2022 sulla resilienza dei soggetti critici (Direttiva CER – Resilience of Critical Entities) che abroga la direttiva 2008/114/CE, il cui termine di recepimento per gli Stati membri è fissato al 17 ottobre 2024. Tale direttiva, in particolare, mira ad aumentare la resilienza di soggetti, negli Stati membri, che sono fondamentali per la fornitura di servizi essenziali per il mantenimento di funzioni vitali della società o di attività economiche nel mercato interno, in una serie di settori che sono alla base del funzionamento di molti altri settori dell'economia dell'Unione. Sono esclusi dal campo di applicazione della direttiva gli enti della pubblica amministrazione operanti nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa o dell'attività di contrasto, compresi l'indagine, l'accertamento e il perseguimento di reati.
Nella medesima data – 27 dicembre 2022 – è stata infine pubblicata la Direttiva n. 2555/2022 (NIS2), entrata in vigore lo scorso 17 gennaio 2023 e da recepire entro il 17 ottobre 2024.
Attraverso la NIS2, l'UE punta ad incrementare e rendere omogeneo il livello di cybersecurity negli Stati membri, creare e ad apprestare misure in grado di fronteggiare in maniera efficace l'incremento dei rischi per la sicurezza conseguenti alla diffusa digitalizzazione dei processi e dei servizi.
Sempre in attuazione di quanto previsto nella Strategia lanciata nel 2020 e partendo dalla constatazione della necessità, per assicurare un ecosistema europeo complessivamente sicuro, di garantire che i dispositivi utilizzati da cittadini, imprese e pubbliche amministrazioni rispondano a standard di sicurezza adeguati, il 15 settembre 2022 la Commissione ha pubblicato una proposta di regolamento sui requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020 (**Cyber Resilience Act – CRA**). Tale proposta, in particolare, mira a salvaguardare i consumatori e le imprese che acquistano o utilizzano prodotti o software con una componente digitale attraverso la fissazione di regole armonizzate per l'immissione sul mercato di prodotti o software con una componente

digitale, l'individuazione di requisiti di cybersecurity che disciplinano la pianificazione, la progettazione, lo sviluppo e la manutenzione di tali prodotti, la fissazione di obblighi per ogni fase della catena del valore e la declinazione di un obbligo generale di diligenza per l'intero ciclo di vita di tali prodotti. La proposta lanciata dalla Commissione in Parlamento europeo è stata assegnata alla commissione ITRE (rapporteur Nicola Danti) che lo scorso 19 luglio ha adottato la relazione sulla proposta presentata il 31 marzo scorso, proponendo una serie di importanti modifiche che, anche in una logica di semplificazione degli adempimenti a carico delle imprese, allineano le procedure a quanto previsto dalla NIS2 ed introducono precisazioni utili in una logica di garanzia della certezza del diritto soprattutto per le PMI che evidentemente si trovano a dover affrontare il tema della sicurezza con un rigore crescente che implica un ripensamento del proprio modello organizzativo ed investimenti decisamente rilevanti.

CAPITOLO 6

L'**I-Com Ultrabroadband Index (IBI) 2023**, l'indice sintetico elaborato da I-Com per fotografare lo sviluppo delle reti e dei servizi digitali nei mercati nazionali europei, conferma nuovamente la **Danimarca**, con un punteggio pari a 78, alla guida della classifica complessiva europea. Le ragioni di questo successo risiedono in un elevatissimo grado di **informatizzazione delle imprese** e in una **copertura 5G e VHCN**, che raggiunge la quasi totalità della popolazione, sia in ambito cittadino che nelle aree rurali. A ciò va ad aggiungersi la rilevante diffusione dell'**e-government**, che vede oltre il 90% dei cittadini interagire con le pubbliche autorità tramite internet.

Sul podio, seguono **Paesi Bassi** e **Spagna**. Quest'ultima recupera ben due posizioni rispetto al 2021, a svantaggio della **Svezia** che retrocede in sesta posizione. L'ottimo risultato della Spagna è motivato da una percentuale elevata di famiglie – il dato più alto nell'UE – che ha sottoscritto un abbonamento in banda larga fissa e da una più alta penetrazione delle reti VHCN e FTTP.

Al di là del podio, i progressi più impressionanti sono quelli della Francia e di Cipro, che guadagnano 11 posizioni, e dell'Italia e dell'Irlanda, che risalgono la classifica di ben 9 gradini dal 2021 al 2023, con l'Italia passata nell'ultimo anno dalla ventesima alla sedicesima posizione.

In particolare, la **performance italiana** è riconducibile a molteplici fattori, tra i quali risulta determinante **l'imponente crescita della copertura 5G**, che dall'8% delle aree popolate e dallo 0% rurale nel 2020 passa al 100% nel 2022.

Un importante passo in avanti si registra anche nel campo dell'e-government, dove il 40% degli italiani ha interagito con la PA via web, anche se il dato resta inferiore alla media UE. Inoltre, un avanzamento considerevole riguarda la diffusione delle reti fisse, indicate dalla copertura VHCN e FTTP a livello rurale, che passa dall'8% al 26% in entrambi i casi, a testimonianza dell'evoluzione dei piani di cablatura dei numeri civici nelle aree grigie e bianche.

La classifica per la componente dell'offerta è ancora una volta dominata da **Danimarca**, **Paesi Bassi** e **Spagna**, così come la classifica generale.

L'**Italia** si trova al dodicesimo posto, con un salto di 12 posizioni rispetto al 2021 e di 2 rispetto al 2022. Il nostro Paese, in termini di penetrazione del 5G tra i paesi europei risulta primo, seguito da Danimarca, Paesi Bassi e Germania. La copertura 5G continua, dunque, ad avere un ruolo preponderante nel determinare il piazzamento finale. Inoltre, in Italia aumenta la copertura delle reti fisse, anche se in questo caso i dati risultano ancora al di sotto del valore medio UE.

Sul versante della domanda, il vertice della classifica continua ad essere appannaggio della **Svezia** sia per l'ampia diffusione dell'e-commerce e soprattutto dell'e-government sia per l'elevato numero di

famiglie che hanno sottoscritto servizi di connettività di banda larga.

L'**Italia**, invece, non tiene il passo degli altri paesi membri, rimanendo relegata al ventitreesimo posto in classifica, davanti solo a Slovacchia, Grecia, Romania e Bulgaria. **Gli indicatori relativi all'e-government, all'e-commerce e alle competenze sono decisamente al di sotto della media europea** anche se, tuttavia, per ognuno di questi si evidenzia un miglioramento rispetto al passato.

In controtendenza rispetto a questo scenario negativo è il dato relativo alla digitalizzazione delle imprese. In questo caso, infatti, **l'Italia è al di sopra della media europea (94%), con una porzione pari al 98% delle imprese aventi una connessione in banda larga**.

In conclusione, l'**Italia** continua a posizionarsi nel cluster dei Paesi ***fast movers***, ossia quelli che, pur partendo da livelli di sviluppo digitale inferiore alla media, presentano una buona dinamica di crescita nel tempo. Indubbiamente, questo risultato è guidato dai progressi ottenuti sul lato dell'offerta, specie per quanto riguarda la copertura della rete 5G. Infatti, nel grafico movers sull'offerta di connettività, l'Italia si posiziona tra i Paesi ***best movers***. Sul fronte della domanda, il nostro Paese si trova, invece, tra i ***fast movers*** e tale posizionamento denota che, seppur partendo nella maggior parte dei casi da valori al di sotto della media europea per quasi la totalità degli indicatori relativi alla domanda di connettività, l'Italia evidenzia una buona dinamica di crescita nel tempo, con una variazione percentuale più marcata rispetto alla media, soprattutto grazie alla crescita dell'e-government, della connessione in banda larga delle famiglie e della digitalizzazione delle imprese. Un segnale incoraggiante che tuttavia andrebbe accelerato qualora l'Italia voglia conseguire nel volgere di pochi anni una posizione di vantaggio rispetto alla media UE, come peraltro ha già fatto da qualche anno un Paese a noi affine come la Spagna.

CAPITOLO 7

Il Piano Nazionale di Ripresa e Resilienza non rappresenta esclusivamente uno slancio per il ripresa dell'economia nazionale a seguito della crisi pandemica ma anche un volano utile a dar vita ad una **crescita più robusta, sostenibile e inclusiva** del nostro Paese. La digitalizzazione ricopre un ruolo cruciale nella pianificazione essendo il tema connotante del primo dei sei pilastri del PNRR. Alla Missione 1 sono destinati complessivamente **€40,29 miliardi, pari al 21% del totale**, il che la rende la seconda per volume di risorse assegnate. Il 70% di tali fondi è destinato ad investimenti specificatamente legati alla transizione digitale del sistema paese.

Pur avendo un ruolo primario nell'ambito della Missione 1, l'elemento digitale (*digital tag*) è trasversale rispetto a tutte le altre missioni del piano. Questo rappresenta infatti un prerequisito necessario e non trascurabile per raggiungere gli obiettivi delineati in tutto il PNRR. **Considerando l'insieme delle missioni, l'ammontare totale delle risorse allocate alla transizione digitale è di €48,09 miliardi**, circa il 25% del totale della dotazione del Piano.

Tra le misure più importanti per la transizione digitale del tessuto produttivo italiano, nell'ambito della Missione 1 – Componente 2 "Digitalizzazione, innovazione e competitività del sistema produttivo", è stato previsto l'Investimento 1 **"Transizione 4.0"** che, con una dotazione finanziaria di €13,381 miliardi (a cui si aggiungono €5,08 miliardi del Fondo complementare), persegue l'obiettivo di sostenere la trasformazione digitale delle imprese. Nonostante la dotazione dei fondi sia andata in pochissimo tempo esaurita, all'inizio dell'anno è stata annunciata dal Governo l'intenzione di inaugurare un nuovo piano che potrebbe essere denominato Transizione 5.0, la cui fonte di finanziamento, per €4,04 mld di euro, è stata individuata nel piano RePower EU. Nel mese di agosto è stata dunque inviata dall'Italia alla Commissione Europea – di cui si attende la pronuncia – una

proposta che assegna per l'appunto la cifra sopraindicata al finanziamento di un **"Piano Transizione 5.0".** Sebbene sia la presentazione della legge di bilancio la sede deputata alla definizione della cornice normativa del nuovo piano, secondo le prime indiscrezioni, il Piano Transizione 5.0 dovrebbe confermare le aliquote attualmente previste fino al 2025 per gli investimenti in beni strumentali 4.0 sopra descritte, con la speranza che vada in qualche modo ad **includere anche le infrastrutture di rete,** ma dovrebbe al contempo disporre un'importante novità, ossia la previsione di premialità – che potrebbero addirittura raddoppiare le aliquote – nel caso in cui gli investimenti, oltre a rispondere ai requisiti previsti dalla normativa per i beni 4.0, offrano benefici tangibili in ottica green.
Altro ambito in cui la digitalizzazione gioca un ruolo di assoluto primo piano in ottica PNRR è **la Sanità**. I servizi sanitari digitali costituiscono un prezioso strumento per affrontare le sfide principali del SSN. Questi danno la possibilità di **ridurre le disparità geografiche e territoriali nell'accesso alle cure**, garantendo un livello uniforme di assistenza grazie all'adozione di tecnologie innovative. Parallelamente possono **migliorare l'esperienza di cura per i pazienti**, rendendo l'assistenza medica più accessibile. Infine, contribuiscono a **potenziare l'efficienza** dei sistemi sanitari regionali promuovendo la possibilità **di fornire assistenza a domicilio e di monitorare i pazienti da remoto**.

CAPITOLO 8

Alla luce degli obiettivi di connettività fissati a livello UE, nel marzo 2015 è stata lanciata la **Strategia per la Banda Ultralarga**, con la quale i decisori politici avevano assunto l'impegno, coerentemente con gli obiettivi dell'Agenda digitale UE 2020, di coprire almeno l'85% della popolazione con connettività ≥100 Mbit/s e il 100% con copertura ad almeno 30 Megabit/s. Tale strategia, in particolare, puntava alla copertura delle aree bianche, ossia le aree a fallimento di mercato e prevedeva misure a sostegno della domanda (voucher).

Al fine di dare attuazione a quanto previsto rispettivamente con la Comunicazione sulla Connettività per un mercato unico digitale europeo (cd. 'Gigabit Society') e la Comunicazione sul decennio digitale (cd. "Digital compass") con cui sono stati presentati la visione, gli obiettivi e le modalità per conseguire la trasformazione digitale dell'Europa entro il 2030, il 27 maggio 2021 è stata lanciata la **Strategia italiana per la Banda Ultralarga "Verso la Gigabit Society"** con l'obiettivo di portare la connettività a 1 Gbps su tutto il territorio nazionale entro il 2026, con un anticipo di 4 anni rispetto agli obiettivi europei fissati per il 2030. La nuova strategia, in particolare, in attuazione del Piano Nazionale di Ripresa e Resilienza che destina il 27% delle risorse alla transizione digitale, di cui 6,7 miliardi di euro per progetti relativi alla connettività, ha individuato altre 5 azioni da aggiungere alle due già in atto e da completare (il Piano aree bianche appena descritto e il Piano voucher) e, nello specifico, il Piano "Italia a 1 Giga", il Piano "Italia 5G", il Piano "Scuole connesse", il Piano "Sanità connessa" e il Piano "Isole Minori".
Partendo dalla constatazione delle criticità registrate nella fase di implementazione dei Piani sopra descritti, nel mese di agosto è stata lanciata la **Strategia italiana per la Banda Ultra Larga 2023-2026** che, sulla base dell'analisi dei gap attualmente presenti lungo la "catena del valore" della BUL, ovvero degli interventi attualmente in essere per la creazione e diffusione delle reti ad altissima capacità in Italia, declina un insieme di azioni tese a traguardare gli obiettivi fissati al 2026. Nello specifico, la strategia si articola in una serie di iniziative sussumibili in 5 macro-finalità: 1) incremento competenze della PA e potenziamento R&S del settore; 2) rafforzamento delle attività di monitoraggio, programmazione e pianificazione degli interventi; 3) realizzazione e potenziamento delle infrastrutture di rete; 4) aumento di efficienza e resilienza delle reti; 5) supporto alla domanda e all'aumento del take up.

Per quanto riguarda gli interventi per lo sviluppo della **connettività fissa**, la nuova strategia individua una fase 3 del Piano Scuola Connessa, con estensione della gratuità del servizio di connettività e della relativa manutenzione fino al 2035 per tutte le scuole pubbliche nazionali, prevede l'offerta di servizi di connettività ad almeno 1 Gigabit/s, oltre ad assistenza tecnica e servizi di manutenzione per 5 anni a 3.000 Comuni per favorire la transizione digitale delle sedi comunali più piccole, annuncia una consultazione pubblica tesa a valutare l'estensione del piano Isole Minori ad ulteriori 10 isole circa, propone l'adeguamento della connettività delle strutture sanitarie pubbliche territoriali, anche aderenti al piano "Sanità connessa", prevedendo prestazioni minime di 10 Gigabit/s gratuite, sostiene l'adeguamento connettività progetto "Polis" per l'accesso ai servizi digitali e connettività ultraveloce in ambito sicurezza e gestione delle emergenze a 10 Gigabit/s Stima costi.

In relazione alla **connettività mobile,** la strategia riprende il tema dei limiti elettromagnetici, proponendo l'avvio di un dialogo istituzionale a vari livelli teso a verificare la congruenza delle attuali modalità di rilevazione dei dati nazionali rispetto a quelle europee, l'adozione di interventi che favoriscano un utilizzo più efficiente dello spettro radio e supportare soprattutto i territori e le amministrazioni locali, la realizzazione, in collaborazione con Ferrovie dello Stato, di un'infrastruttura radio mobile multi operatore 5G di proprietà pubblica con priorità lungo le tratte ad alta velocità e di garantire copertura e connettività mobili (4G e/o 5G) lungo la rete stradale, incluse le tratte in galleria, per tutte le linee di comunicazione principali verso le sedi di svolgimento degli eventi olimpici relativi a "Milano – Cortina 2026" ed infine di finanziare progetti per la realizzazione da parte di Enti pubblici e distretti industriali, aree portuali, poli di alta specializzazione e aree agricole, di servizi innovativi basati sul 5G anche mediante sistemi DAS ("Distributed Antenna System") indoor e outdoor e su accesso fisso ultra broadband e VHCN, dove alle infrastrutture si affianchi lo sviluppo e la sperimentazione di servizi innovativi basati sull'uso di Edge Cloud Computing destinato a reti fisse e mobili che consentano la sperimentazione di tali servizi innovativi.

Per quanto riguarda, infine, le **iniziative a sostegno della domanda**, da un lato si prevede una revisione del piano Voucher Famiglie mediante la previsione di un voucher dedicato alle nuove attivazioni per collegamenti in Banda Ultra Larga; dall'altro, è annunciata l'individuazione, di concerto con la Commissione europea, di forme di incentivazione alle imprese per l'attivazione di servizi dedicati (es. cloud computing, cyber security, ecc.).

Relativamente allo stato di copertura, gli ultimi dati ufficiali relativi allo stato della copertura del territorio italiano in rete fissa risalgono alle mappature condotte da Infratel Italia nel 2021 Il primo dato interessante emerso dal monitoraggio consisteva nel grado di copertura dei numeri civici in rete fissa con una velocità di download di almeno 30 Mbit/s al 2021. Tale dato si attestava **al 64,1% dei numeri civici presenti a livello nazionale**. Analizzando la scomposizione territoriale della copertura, **i risultati registrati a livello locale evidenziano notevoli differenze tra regioni**. Per quanto concerne il tasso di civici coperti ad una velocità di connessione di almeno 30 Mbit/s, i dati mostrano come a primeggiare fossero quattro regioni meridionali, ovvero Puglia (88,5%), Sicilia (75,5%), Calabria (75,2%) e Sardegna (69,1%). Questi risultati sono dovuti principalmente ai precedenti interventi di infrastrutturazione a banda larga, storicamente concentrati prevalentemente nel Sud Italia. Lo scenario cambia notevolmente analizzando i soli civici coperti con tecnologie che forniscono una velocità di connessione tra i 300 Mbit/s e 1 Giga (2021). In questo caso la classifica delle regioni maggiormente coperte si ribalta, mostrando una netta prevalenza di regioni centro-settentrionali.

Le pianificazioni attivate negli ultimi anni per coprire

il territorio il con reti fisse di ultima generazione sono due: **il Piano Piano Banda Ultralarga (Piano BUL) e il Piano Italia a 1 giga**. Relativamente al Piano BUL, al 31 agosto 2023, dal punto di vista progettuale **risultavano 10.033 progetti approvati su 11.346 previsti in *Fiber to the home* e 6.826 approvati su 7.116 previsti in Fixed Wireless Access.** A livello realizzativo, per le infrastrutturazioni in fibra sono stati emessi **9.991 ordini di esecuzione, di cui 7.444 risultano chiusi,** ovvero con CUIR (Comunicazione Ultimazione Impianto di Rete), a fronte di **5.576 collaudi positivi**. Per i cantieri FWA si osservano **3.182 ordini emessi, di cui 3.074 con CUIR e 1.336 siti già collaudati positivamente**.

Se questo è lo stato di attuazione del Piano BUL, grazie al Piano "**Italia a 1 Giga**", secondo gli ultimi dati pubblicati sul portale *connetti.italia.it*[1] (aggiornati ad agosto 2023)*,* **sono stati connessi oltre 234 mila civici, ovvero il 3,4% di quelli previsti dall'intervento**.

Tra le tecnologie utilizzate per la copertura in rete fissa del territorio italiano di notevole importanza è il ruolo del **Fixed Wireless Access (FWA).** La tecnologia FWA nel corso degli anni ha avuto un ruolo chiave nel contribuire a colmare il problema del *digital divide* e rappresenta oggi **una realtà in forte crescita**. Inoltre, la natura del FWA rende questa tecnologia **complementare all'FTTH nel fornire connettività alle aree a bassa densità abitativa** del Paese che rientrano nel Piano Italia 1 Giga e nella nuova Strategia BUL 2023-2026.

A livello di copertura, in base ai dati forniti ad I-Com da Infratel Italia, al 2021 **i civici raggiunti in FWA passed sul territorio nazionale risultano essere il 5,7% a velocità compresa tra i 30 e i 100 Mbit/s e il 14,8% con velocità di connessione compresa tra i 100 e i 300 Mbit/s.**

Oltre ai dati di copertura, per analizzare la diffusione della tecnologia FWA in Italia appare interessante osservare i dati relativi agli accessi, ovvero gli abbonamenti sottoscritti dagli utenti. Secondo i dati pubblicati nell'ultima versione dell'Osservatorio Trimestrale Agcom (giugno 2023), **il numero di abbonamenti complessivi in tecnologia FWA a marzo 2023 ammonta a circa 1,88 milioni di unità**, che equivalgono al **10% delle linee broadband totali**.

Relativamente alla copertura mobile, l'argomento principale è certamente lo stato della 5G. Gli ultimi dati pubblicati dal 5G Observatory indicano come, nel primo trimestre del 2023, gli operatori italiani abbiano dichiarato **una copertura della popolazione pari al 99,7%, il quarto valore più alto tra quelli pubblicati a livello europeo**. Nonostante l'ottima performance registrata dal nostro Paese, ad un'analisi più attenta emerge chiaramente come **tale livello sia stato ad oggi raggiunto almeno in parte grazie all'eredità storica della buona copertura 4G e dell'utilizzo della tecnologia DSS.** Se consideriamo esclusivamente **il 5G standalone** risultava coperto solo il **7,3% del territorio nazionale**.

Relativamente allo stato di avanzamento del **Piano Italia 5G** (aggiornamento ad agosto 2023), dal punto di vista del ***backhauling*** – ovvero della rilegatura in fibra delle Stazioni Radio Base (SRB) che, secondo quanto emerso dalla mappatura, non verranno coperte dai soli operatori entro il 2026 – risultano completati oltre il 10% dei siti oggetto di intervento, mentre un ulteriore 15% è in lavorazione. Sul versante della **densificazione,** la situazione sembrerebbe **procedere un po' più a rilento con solo il 3,26% degli interventi completati e il 13,95% in lavorazione**.

Oltre che analizzare il lato dell'offerta, per comprendere lo stato delle telecomunicazioni in Italia è interessante andare ad osservare la domanda di connettività nel Paese. Dai dati contenuti nell'ultima relazione dell'Osservatorio Trimestrale sulle Telecomunicazioni realizzata da Agcom (N.2/2023), emerge come **il numero di accessi diretti alla rete**, ovvero il numero di

1 Estratti il 13-10-2023

linee attive, nell'ultimo triennio **abbia sperimentato un andamento oscillante.** Un notevole passo avanti si è fatto però sul versante della tecnologia. Analizzando infatti il mix tecnologico, si evidenzia **il calo delle connessioni completamente in rame (-29%),** che restano comunque il 20,7% del totale, **a fronte di una netta crescita di tutte le altre, in particolare di FTTH (passato dal 5,7% al 18,8%), FTTC (dal 38,1% al 51,1%) e FWA (dal 6,5% al 9,4%).**
Uno degli strumenti su cui le istituzioni hanno puntato per garantire una maggiore diffusione di servizi di connettività a banda ultralarga nel Paese consiste nel **Piano voucher connettività**. Sul versante delle business, s **il 55,3% (€326 milioni) dei fondi destinati alle imprese risulta essere stato attivato, mentre un ulteriore 6,7% (€39,5 milioni) è stato prenotato**. Per quel che riguarda i risultati ottenuti dalla **fase I del Voucher Famiglie**, attivata a novembre 2020 e conclusa nel 2021, si osserva come **sui €200 milioni disponibili a livello nazionale, circa il 51% risulta essere stato erogato, mentre il 49% non è stato utilizzato.**

CAPITOLO 9

Per realizzare la transizione digitale si pongono come fondamentali le competenze digitali e dunque la loro diffusione si presenta come un passaggio obbligato. La loro mancanza può ostacolare significativamente la partecipazione attiva nella società e nell'economia digitale. In questo contesto **i dati provenienti dall'Italia si dimostrano pessimi**: infatti il nostro Paese si posiziona **in fondo alle classifiche europee per diffusione di competenze digitali**, con enormi divari rispetto ai *best performer*.
La diffusione nelle competenze nella popolazione è anche fortemente influenzata da fenomeni socioculturali passati: queste sono più diffuse tra gli uomini nelle fasce d'età più avanzate rispetto a quelle più giovani (unica eccezione nella fascia 20-24), dimostrando la **presenza di un "gender gap"**. Bisogna fare dei distinguo fra le singole competenze digitali, l'Italia è poco distante dalla media UE in dei casi, come per l'utilizzo dei social network, ma il divario si amplia per altri, come nel caso delle competenze in sicurezza informatica. Per poter sfruttare nel miglior modo il potenziale della rivoluzione digitale è fondamentale il ruolo svolto dalla Pubblica Amministrazione. In questo contesto vi sono delle differenze significative fra tipologie di pubbliche amministrazioni (**i comuni** ad esempio **sono quelli che fronteggiano maggiore difficoltà nell'processo di digitalizzazione**), ma anche rispetto alle diverse aree geografiche (l'Emilia-Romagna è la regione in cui nel 2020 le PA hanno fornito maggiormente corsi di formazione, la Calabria è quella che ne ha forniti di meno). Anche per le imprese il dato che emerge è negativo, sebbene rispetto ai corsi di formazione erogati la media italiana sia poco al di sotto alla media UE. La stessa percentuale negli anni è aumentata e si è avvicinata alla media comunitaria, tuttavia lo stesso divario è rimasto grossomodo costante dopo il 2019. Inoltre sempre le imprese ritengono che **le skill che necessitano maggiormente di potenziamento sono quelle legate alla sicurezza informatica**. Nell'ambito la formazione l'Italia raggiunge anche questa volta un record negativo, conquistando l'ultimo posto in Europa per la quota di laureati ICT sul totale. Dal 2018 il numero di laureati in materie STEM ha segnato di anno in anno un lieve aumento, ad eccezione solamente del 2022; al contrario i diplomati degli istituti tecnici sono diminuiti nello stesso quinquennio. Nonostante ciò, nel periodo 2023-2027 si prevede comunque **un importante divario fra la domanda e l'offerta di laureati STEM e economico-statistici**.
I rischi derivanti dalla rete e l'esigenza di ampliare la sicurezza della stessa irradiano un tema fondamentale, quello delle **competenze in cybersecurity**. L'analisi dei dati forniti da Eurostat con riferimento all'anno 2022 evidenzia che **solo il 59,8% dei cittadini ha competenze almeno basilari in materia di sicurezza informatica** e, puntando il focus sulla

scomposizione per età, la quota di persone impreparate cresce in maniera direttamente proporzionale all'età anagrafica. Per comprendere al meglio il quadro nazionale sulle iniziative finalizzate ad aumentare le competenze in cybersecurity, va preso in considerazione il monitoraggio delle attività di **formazione dedicate al tema in ambito universitario**, avviato a partire da gennaio 2022 dall'Istituto per la Competitività (I-Com). Nello specifico, con riferimento all'**anno accademico 2022/2023**, si registra la presenza di **271 corsi di formazione universitaria**, precisamente 112 insegnamenti singoli all'interno di corsi di laurea magistrale, 56 insegnamenti singoli all'interno delle lauree triennali, 44 dottorati, 22 lauree magistrali, a fronte di 13 corsi all'interno di dottorati di ricerca, 18 master e 4 lauree triennali interamente concernenti la cybersecurity. È importante osservare come la formazione specializzata abbia raggiunto quota **88 corsi di studio interamente dedicati**, oltre all'elevato numero di master specifici sui temi della cybersicurezza, per cui su tutto il territorio nazionale ne sono stati rilevati 18, 9 di I Livello e ulteriori 9 di II Livello. Una maggiore attenzione sul punto si è evinta anche nell'ambito degli **Istituti Tecnici Superiori (ITS)** tra cui, secondo l'aggiornamento risalente a giugno 2023 del monitoraggio INDIRE e un'analisi svolta da I-Com, quelli **interessati alla cybersicurezza sono il 14%** rispetto al numero complessivo degli ITS attivi. Infine, il Piano Nazionale di Ripresa e Resilienza mira a produrre un notevole effetto positivo nel settore delle competenze digitali, con un cospicuo stanziamento di risorse a tale scopo. Queste rappresentano un argomento trasversale fra le 6 missioni e sono particolarmente attenzionate sia dal PNRR che dalla Commissione europea.

icom
istituto per la competitività

CAPITOLO 1

USI E COSTUMI DIGITALI DELLE IMPRESE E DEI CITTADINI EUROPEI

1.1. L'EVOLUZIONE DELLE ABITUDINI DI UTILIZZO DI INTERNET DEI CITTADINI ITALIANI ED EUROPEI

Dopo la spinta dell'emergenza pandemica alla transizione digitale, nel **2022 il processo di digitalizzazione ha continuato a mostrare una tendenza positiva**, confermata dai tassi di crescita nell'adozione delle tecnologie digitali, sia da parte dei cittadini che delle imprese a livello dell'Unione Europea. Nel contesto di questa rapida evoluzione, il capitolo si propone di esaminare le **attuali tendenze nell'utilizzo di internet, degli strumenti e dei servizi digitali tra cittadini, imprese e amministrazioni pubbliche, con uno sguardo sulle prospettive future**. La prima parte del capitolo comprende un'analisi dello stato dell'arte in materia di utilizzo di internet dei cittadini italiani ed europei. La seconda parte è dedicata alla transizione digitale delle imprese e approfondisce, in particolare, il tema degli **investimenti in cybersecurity**. La terza parte è rivolta alla digitalizzazione della Pubblica Amministrazione.

Conoscere la **quantità di utenti di internet in Europa** può rappresentare un buon punto di partenza per avere informazioni circa il contesto in cui si sviluppa la transizione digitale. Secondo i dati Eurostat, in media, **più del 90% dei cittadini europei ha utilizzato internet almeno una volta nel corso dei 12 mesi precedenti alla rilevazione statistica**, con Lussemburgo, Danimarca, Finlandia e Svezia ben oltre la quota del 95% (Fig. 1.1) **In Italia, questa percentuale scende all'85%, un valore al di sotto della media europea** e che colloca il nostro paese in fondo alla classifica.
La percentuale di individui che ha utilizzato internet almeno una volta nei 12 mesi precedenti alla rilevazione statistica dell'Eurostat è **più alta nelle zone urbane rispetto alle zone rurali** (Fig. 1.2). Questo vale sia per l'Europa, sia nello specifico per l'Italia, dove la quota nelle zone urbane è pari all'87%, mentre nelle zone rurali è dell'82%.
È interessante notare come, nell'arco di poco più di un decennio, sia significativamente cresciuta la quota di individui che utilizzano internet tutti i giorni (Fig. 1.3). Se in Europa, nel 2009, tale percentuale era del 46% appena, **nel 2022 ha raggiunto l'85%.** Un

Fig. 1.1: Individui che hanno utilizzato internet almeno una volta negli ultimi 12 mesi, per paese (%, 2022)

Fonte: Eurostat

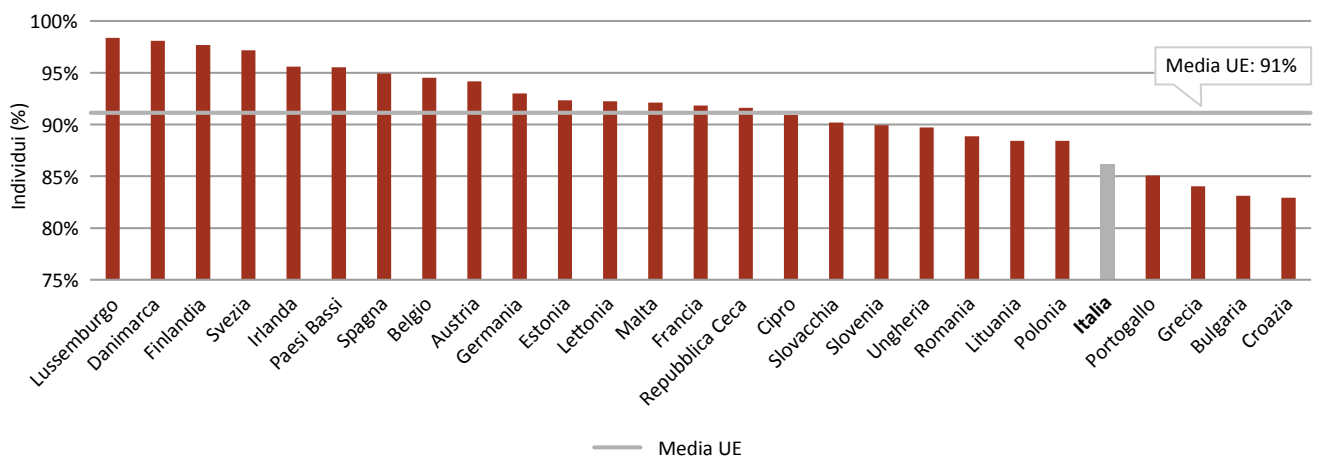
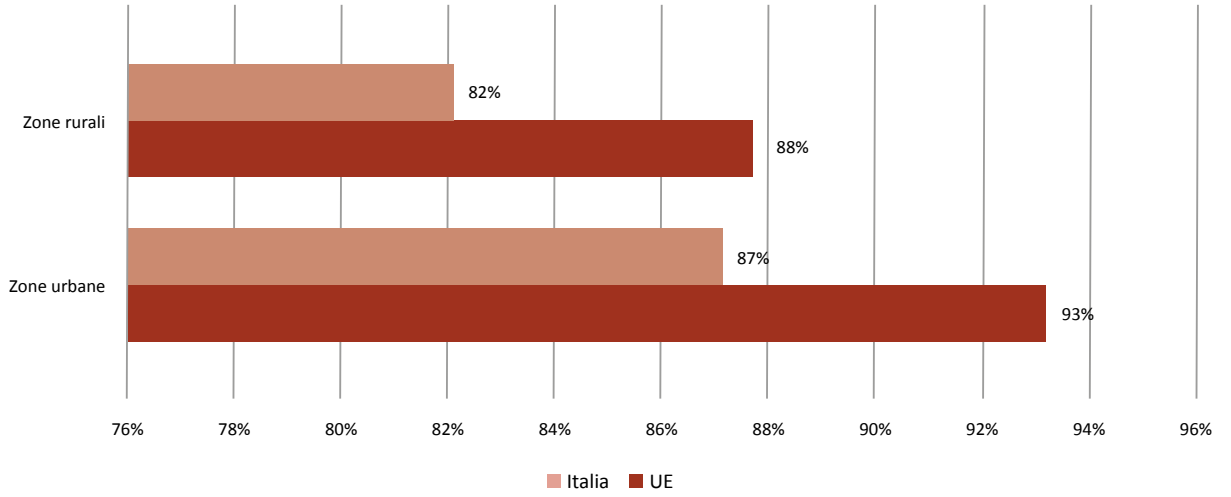


Fig. 1.2: Individui che hanno utilizzato internet almeno una volta negli ultimi 12 mesi, per tipologia di zona (%, 2022)

Fonte: Eurostat



simile andamento si è registrato anche in Italia, che è passata dal 40% nel 2009 all'**82% nel 2022**, vedendo diminuire gradualmente il divario rispetto alla media dei paesi UE.

Approfondendo ulteriormente l'argomento, possiamo osservare un **netto aumento nell'utilizzo di internet per svolgere una serie di attività specifiche** (Fig. 1.4). Nel 2016, circa il 15% dei cittadini europei (il 10% tra i cittadini italiani) utilizzava la rete per fruire di **contenuti video on demand** tramite piattaforme di streaming. Nel corso di soli sei anni, questa percentuale è quasi triplicata, raggiungendo il 42,3% in Europa nel 2022, mentre l'Italia ha seguito una tendenza simile con un aumento dal 10% al 41%. Sempre nell'ambito dell'intrattenimento, in Italia è cresciuta anche la quota di individui che utilizza internet per **giocare o scaricare videogiochi**, passando dal 21% al 28%. La connettività digitale ha aperto nuove opportunità anche per l'apprendimento: sempre più persone sfruttano internet per **seguire corsi online, accedere a materiale didattico e partecipare a programmi di formazione**. Quest'ultima tendenza, forse ancora più di altre, è stata accelerata dalla pandemia, che ha portato a una maggiore domanda di educazione fruibile attraverso la rete.

Fig. 1.3: Individui che utilizzano internet tutti i giorni (%)

Fonte: Eurostat

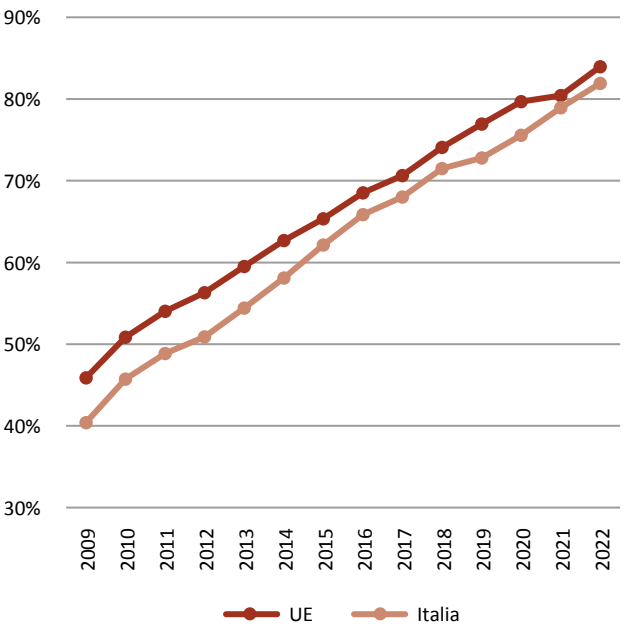
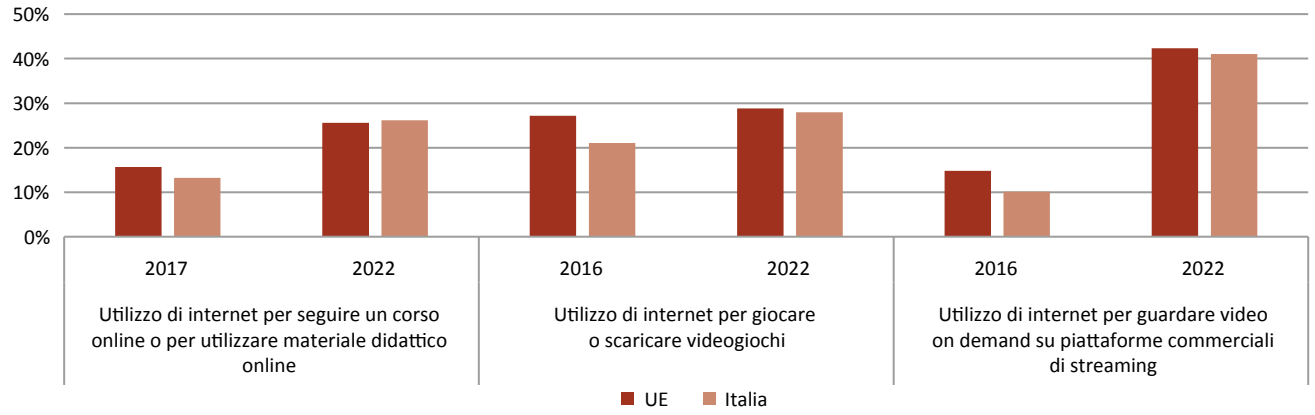


Fig. 1.4 Individui che utilizzano internet, per tipologia di attività (%)

Fonte: Eurostat



Inoltre, l'aumento nell'utilizzo di internet ha innescato una **crescente adozione di dispositivi connessi**, contribuendo così a ridefinire il nostro modo di interagire con la tecnologia nella quotidianità. Questi dispositivi includono **smart TV**, **assistenti virtuali**, e una **vasta gamma di dispositivi IoT**, che rendono le nostre case sempre più intelligenti e interconnesse. Coerentemente a quanto detto sopra circa l'utilizzo di internet per guardare contenuti video su piattaforme di streaming, **è particolarmente alta la quota di individui che utilizzano smart tv: in Europa supera il 50% mentre in Italia si attesta al 49%** (Fig. 1.5).

È interessante anche considerare il tempo che viene dedicato quotidianamente a diverse attività "digitali". Secondo i dati presenti nel rapporto annuale "Digital 2023" di We Are Social, **nel corso del 2022, gli italiani**

Fig. 1.5: Utilizzo di dispositivi connessi da parte dei cittadini (%, 2022)

Fonte: Digital Economy and Society Index (DESI)

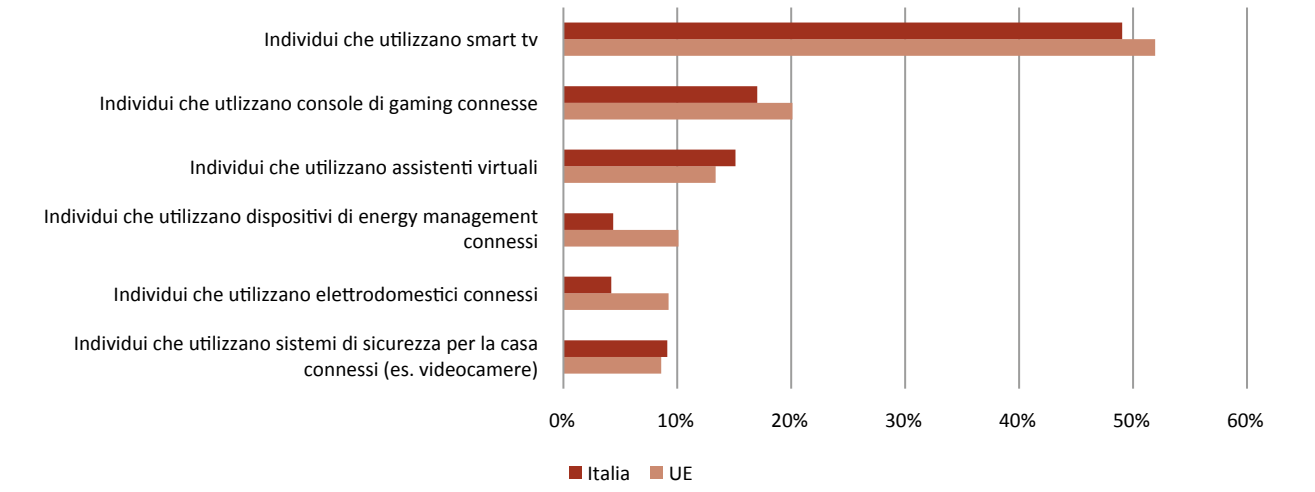
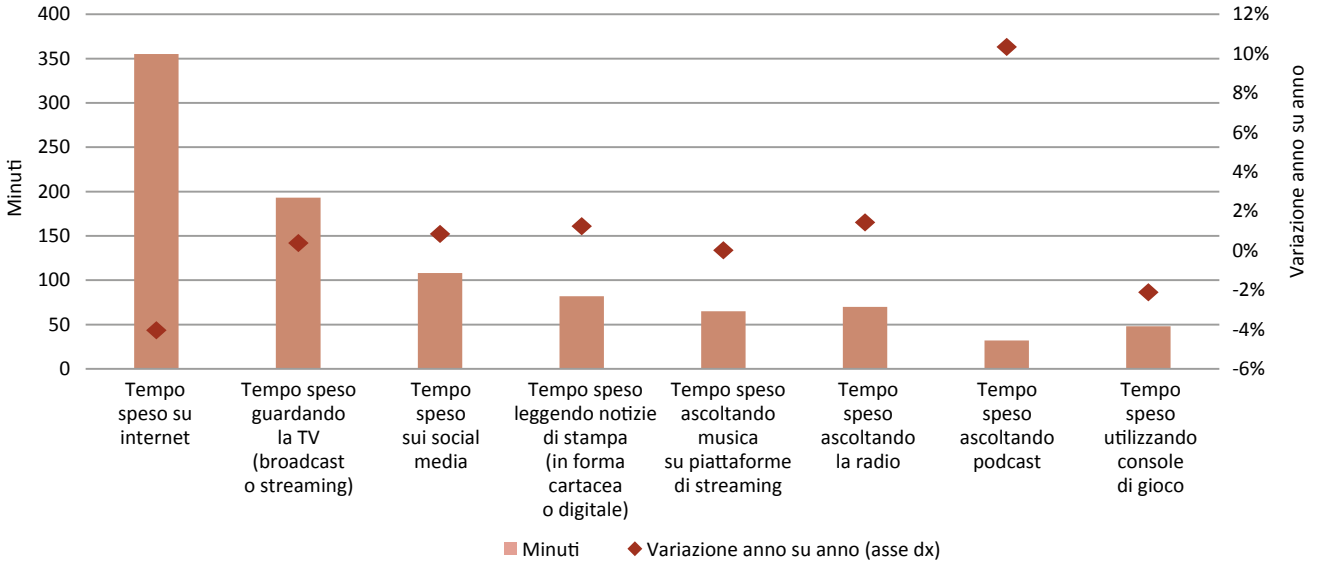


Fig. 1.6: Minuti spesi ogni giorno svolgendo diverse attività, in Italia (individui tra i 16 e i 64 anni, 2022)

Fonte: We Are Social, Digital, 2023

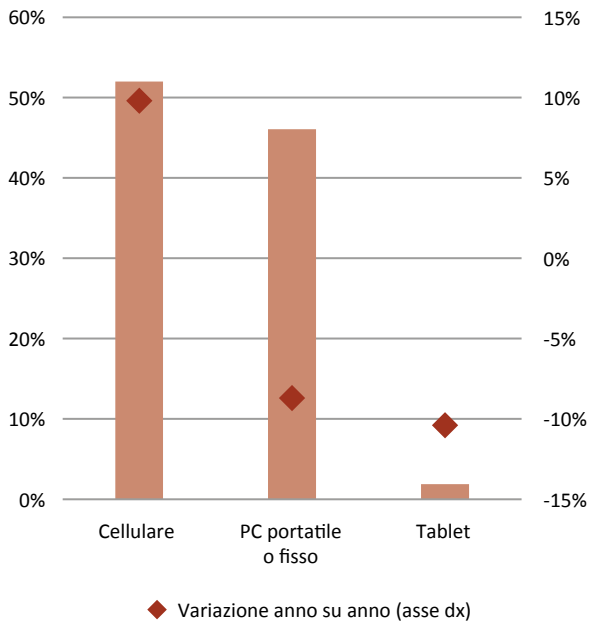


hanno trascorso in media 335 minuti al giorno online, segnando una leggera diminuzione del 4% rispetto all'anno precedente (Fig. 1.6). Tra le altre attività digitali a cui gli italiani hanno dedicato parte del loro tempo, si trovano la **fruizione televisiva, con una media di 193 minuti al giorno, e l'uso dei social media, a cui sono stati dedicati circa 108 minuti al giorno.** Inoltre, è interessante notare che il tempo trascorso ad ascoltare **podcast** è aumentato del 10% rispetto al 2021, indicando una crescente diffusione di questa forma di intrattenimento.

Negli ultimi anni, si è anche assistito a una significativa evoluzione nelle preferenze degli utenti riguardo ai **dispositivi digitali**. I dati recenti indicano un **drastico calo nell'uso di PC e tablet, a favore di un crescente utilizzo degli smartphone**, che hanno guadagnato un ruolo predominante nell'accesso a internet e nell'esecuzione di varie attività online**. Nel 2022, circa il 52% del totale delle pagine web è stato visualizzato tramite cellulare, il 46% tramite computer portatile o fisso e solo il 2% tramite tablet** (Fig. 1.7)

Fig. 1.7: Percentuale del totale delle pagine web visualizzate in Italia, per tipo di dispositivo (2022)

Fonte: We Are Social, Digital, 2023



L'emergenza pandemica ha avuto un impatto anche sul settore finanziario e in particolare sul rapporto banca-cliente, che negli ultimi anni si è adeguato in modo tale da garantire la disponibilità dei servizi tramite il canale digitale. Nel 2022, utilizzano l'internet banking quasi il 60% dei cittadini europei e il 48,8% dei cittadini italiani (Fig. 1.8). Si tratta, soprattutto per l'Italia, di una crescita significativa, considerando che nel 2018 la percentuale di utenti che utilizzava questo servizio nel nostro paese era pari al 33,8%.

1.2. LA TRANSIZIONE DIGITALE DELLE IMPRESE

L'accelerazione nel processo di digitalizzazione ha riguardato anche le imprese. Per queste ultime, la transizione digitale rappresenta una sfida impegnativa, ma allo stesso tempo anche un'importante opportunità da cui poter trarre un vantaggio competitivo. In quanto fenomeno trasversale, la digitalizzazione coinvolge l'intero tessuto imprenditoriale europeo ed esercita un impatto diretto su tutte le funzioni aziendali, esigendo che le aziende rivedano e ristrutturino il loro modello di business in modo da adattarsi prontamente ai mutamenti del mercato.

A tal proposito, i dati Eurostat forniscono interessanti indicazioni relative alla transizione digitale delle imprese europee. Nell'ambito dell'indagine sull'uso delle tecnologie dell'informazione e delle comunicazioni (ICT) e sull'e-commerce nelle imprese, l'Eurostat calcola **l'indice di intensità digitale (DII),** un indicatore composito che si basa su 12 variabili, con ciascuna delle variabili che attribuisce un punto. **In base al DII è possibile distinguere quattro livelli di intensità digitale delle imprese**: per punteggi compresi tra 0 e 3: intensità digitale "**molto bassa**"; per punteggi compresi tra 4 e 6: intensità digitale "**bassa**"; per punteggi compresi tra 7 e 9: intensità digitale "**alta**"; per punteggi compresi tra 10 e 12: intensità digitale "**molto alta**". Il DII rappresenta uno dei principali indicatori di performance utilizzato per il monitoraggio nell'ambito del Decennio Digitale europeo. Quest'ultimo delinea gli obiettivi di digitalizzazione dell'Europa e stabilisce i target concreti da raggiungere entro il 2030 in termini di competenze, infrastrutture, trasformazione digitale delle imprese e dei servizi pubblici. Considerando la situazione europea al 2022, notiamo che **la percentuale di imprese con 10 o più addetti che presentano un livello di intensità digitale "molto alto" è ancora piuttosto bassa in tutti i paesi europei.** La percentuale di imprese con un livello almeno "alto" è più alta

Fig. 1.8: Utilizzo dell'internet banking (%)

Fonte: Digital Economy and Society Index (DESI), 2022

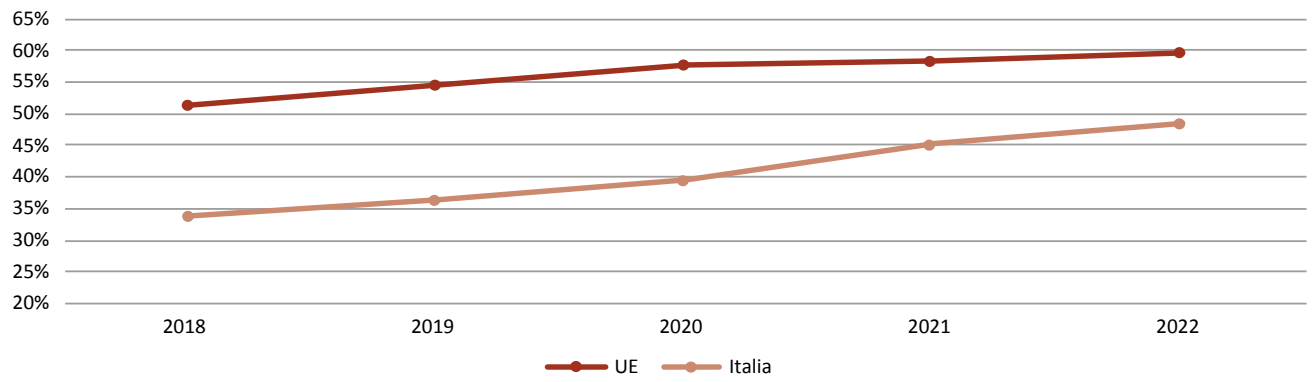
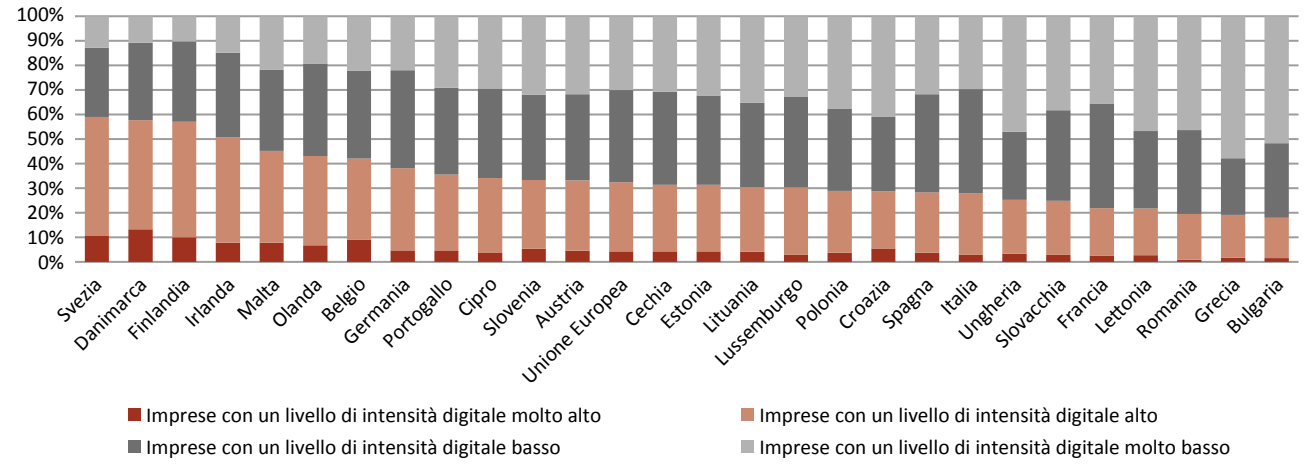


Fig. 1.9: Intensità digitale delle imprese con 10 o più addetti (%, 2022)

Fonte: Eurostat



nei paesi del nord Europa, e in particolare in Svezia Danimarca e Finlandia ed è in media pari al 32,4% in Europa**. L'Italia si colloca, invece, sotto la media europea con un valore del 27,8%** (Fig. 1.9).

Considerando la percentuale di imprese con un livello di intensità digitale almeno "alto" per **dimensione di impresa**, è interessante notare che, sebbene come abbiamo visto l'Italia si collochi complessivamente al di sotto della media europea, **il divario risulta essere particolarmente ridotto per le imprese con più di 250 addetti** (82% in Italia e 84% in Europa) e addirittura invertito di segno per le imprese con un numero di addetti compreso tra 50 e 249 addetti (57% in Italia vs 56% in Europa) (Fig. 1.10). Tuttavia, in questo contesto, è opportuno ricordare che la maggior parte del tessuto imprenditoriale italiano è costituito da microimprese (imprese con meno di dieci addetti) il cui livello di digitalizzazione non viene rilevato nell'ambito dell'indagine Eurostat. In Italia le microimprese sono circa 4 milioni, rappresentano quasi il 95% delle imprese attive sul territorio e più del 26% del valore aggiunto realizzato.

Scendendo più nel dettaglio e considerando alcune delle diverse tecnologie digitali adottate dalle imprese, notiamo che i risultati in termini di integrazione variano a seconda della tecnologia che viene presa in considerazione. Oltre che nell'utilizzo della

Fig. 1.10: Imprese con intensità digitale alta o molto alta, per dimensione di impresa (%, 2022)

Fonte: Eurostat

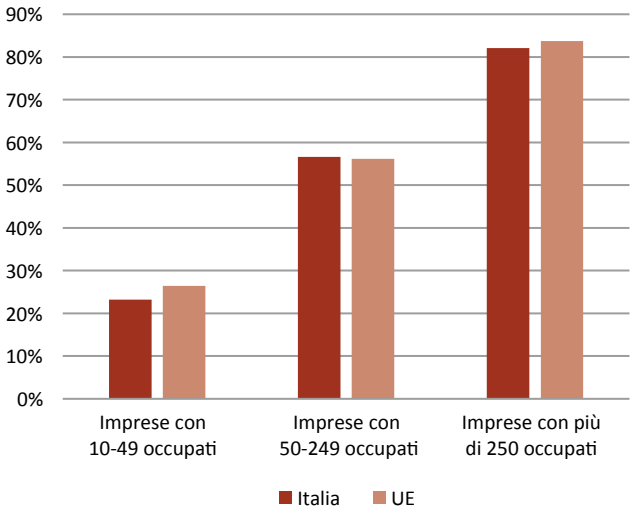


Fig. 1.11: Imprese con 10 o più addetti che utilizzano il cloud (%, 2021)

Fonte: Eurostat

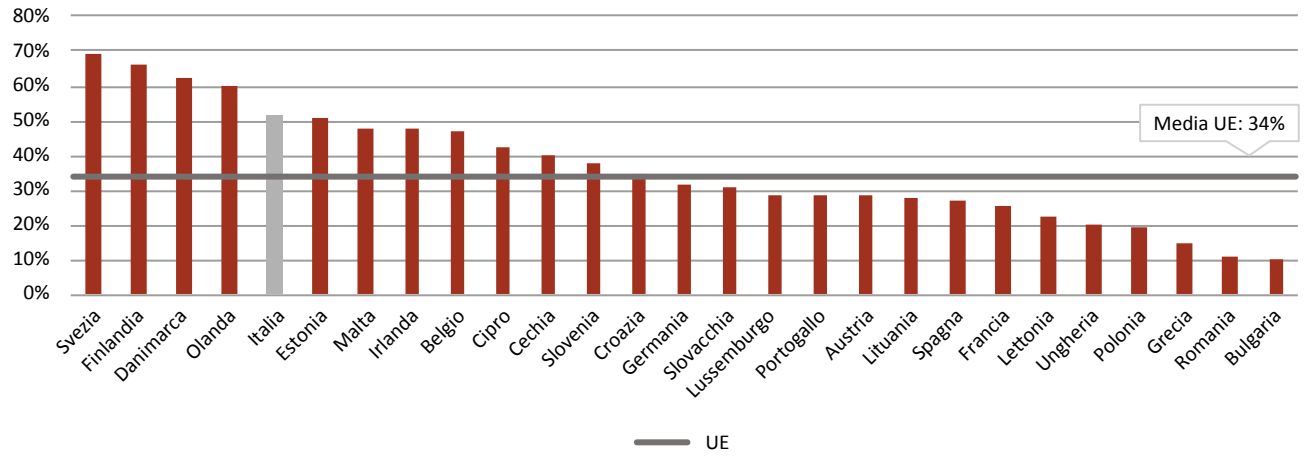
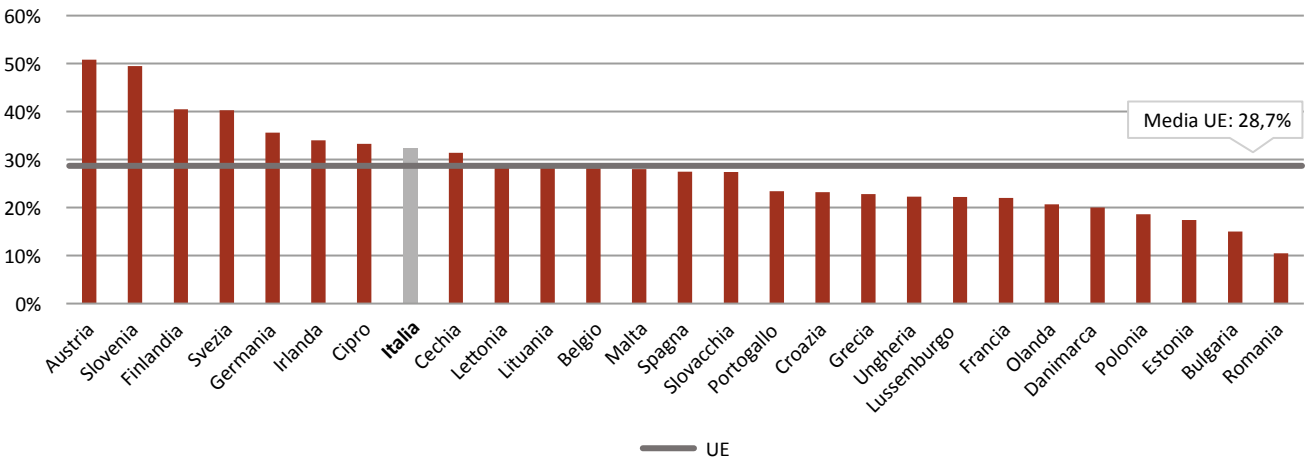


Fig. 1.12: Imprese con 10 o più addetti che utilizzano l'IoT (%, 2021)

Fonte: Eurostat



fatturazione elettronica, che grazie agli interventi governativi ha raggiunto una quota di adozione del 95%, **l'Italia registra buoni risultati anche per quanto riguarda la diffusione del cloud e dell'internet of Things (IoT)**. Nell'ambito dei servizi cloud, sono circa il **52%** delle imprese ad utilizzare tale tecnologia, ben al di sopra della media europea del **34%** (Fig. 1.11). Si tratta di una percentuale che permette al nostro paese di posizionarsi quinto nella classifica dei paesi europei, preceduto solo dalla Svezia, Finlandia, Danimarca e Olanda. Anche l'uso dell'IoT è piuttosto diffuso tra le imprese italiane, sono circa il **32%** delle imprese a farne uso, contro una media europea del **28,7%** (Fig. 1.12).

1.2.1. *Gli investimenti delle imprese in cybersecurity*

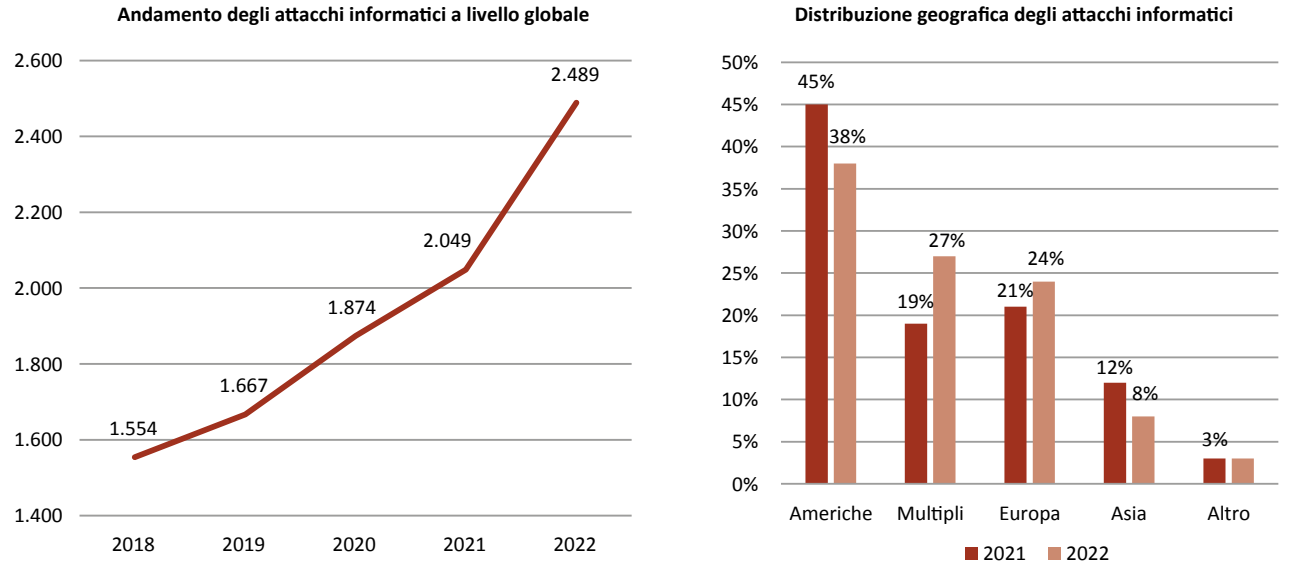
La transizione digitale porta inevitabilmente con sé un aumento della superficie di attacco e nuove forme di minacce cibernetiche, che possono essere sfruttate da diverse tipologie di attori malevoli, tra cui i cybercriminali, come punto di accesso per raggiungere il proprio obiettivo (es. ritorno economico) grazie all'utilizzo di software malevoli, ivi inclusi gli ormai noti ransomware. In tale contesto, dato che le imprese ricorrono a una moltitudine di dispositivi e sistemi per le relative attività di business, possono diventare vittime di attacchi informatici, con ripercussioni potenzialmente gravi non solo per il soggetto colpito, bensì per l'intera supply chain.

L'ultimo rapporto dell'Associazione Italiana per la Sicurezza Informatica (Clusit), pubblicato a marzo 2023, fornisce una chiara panoramica di come le minacce cibernetiche a livello globale siano cresciute costantemente nel corso degli ultimi anni. Lo studio è basato sull'analisi di oltre 16.000 attacchi informatici noti andati a buon fine e di particolare gravità, a partire dal 2011, che hanno avuto impatti significativi in termini economici, tecnologici, legali, reputazionali o che comunque prefigurano scenari particolarmente allarmanti. Osservando i dati relativi all'ultimo quinquennio, è possibile notare come il numero di azioni malevole annuali sia cresciuto di oltre il 60%, passando dalle 1.554 del 2018 alle 2.489 del 2022 (Fig. 1.13). Altro dato particolarmente preoccupante è quello della crescita tra il 2021 e il 2022 delle azioni malevole (+21,5%), oltre il doppio dell'aumento riscontrato nell'anno precedente. Dall'analisi di queste risultanze, si può affermare che **il 2022 è stato l'anno peggiore di sempre per la cibersicurezza a livello globale**.

La stessa figura mostra anche la distribuzione geografica delle vittime nel 2022, per cui – seppur prevalga ancora il continente americano – **l'Europa si posiziona al terzo posto, attraendo il 24% delle azioni degli attori malevoli, in crescita del 3% rispetto all'anno precedente**.

Fig. 1.13: Andamento e distribuzione geografica degli attacchi informatici

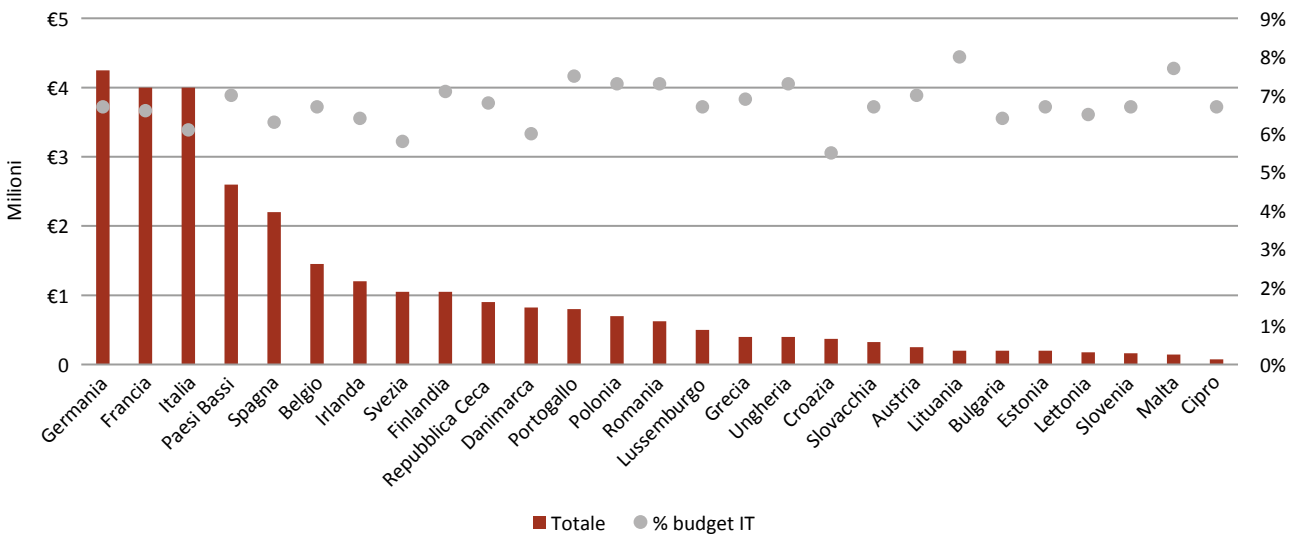
Fonte: Clusit – Rapporto sulla sicurezza ICT in Italia, 2023



Dai dati sin qui analizzati emerge chiaramente quanto le minacce cibernetiche siano in costante crescita. Pertanto, è quantomai fondamentale che le organizzazioni si dotino di adeguati strumenti di sicurezza, intesi non solo come contromisure tecnologiche, ma anche processi e regole chiare per prevenire, gestire e reagire in maniera consona a un attacco informatico che coinvolga, direttamente o indirettamente, le reti, i sistemi e i servizi di propria pertinenza. Ciò detto, l'ultima versione del report *"NIS Investments"*[2], pubblicato dall'ENISA a novembre 2022, vengono analizzati gli investimenti effettuati per la sicurezza informatica da parte degli OSE/DSP europei nel corso del 2021. L'indagine è stata condotta intervistando esponenti di 1080 organizzazioni residenti in tutti e 27 gli Stati Membri (40 per paese), appartenenti ai settori economici sottoposti alla direttiva NIS[3] e suddivisi in due macrocategorie, ovvero gli "Operatori di servizi essenziali" (OSE)[4] e i "*Digital Service Providers*"[5] (DSP). Ebbene, la spesa media per la sicurezza informatica effettuata da tali soggetti nel corso del 2021 si è attestata a €4 milioni, in forte crescita rispetto all'anno precedente (€2,15 milioni). Tuttavia, **gli OSE/DSP hanno destinato mediamente il 7,82% del proprio budget IT alla cybersicurezza nel 2021, evidenziandosi una netta diminuzione rispetto al 2020 (8,8%)**.
Analizzando nel dettaglio i singoli Paesi, si osserva come le organizzazioni tedesche siano quelle che spendono di più in sicurezza informatica in valore assoluto (€4,25 milioni), seguite da quelle italiane e francesi che riportano una spesa pari a €4 milioni (Fig. 1.14).

Fig. 1.14: Spesa per la sicurezza informatica degli OSE/DSP, per Stato membro (2021)

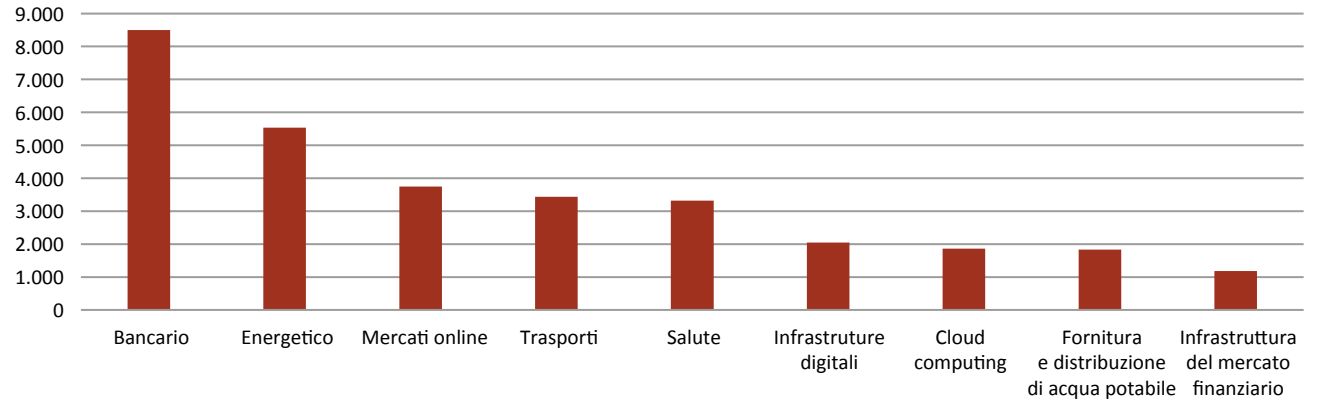
Fonte: ENISA, NIS Investments Report, 2022



2 https://www.enisa.europa.eu/publications/nis-investments-2022
3 Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
4 OSE – energia; trasporti; bancario; finanziario; salute; servizi idrici; infrastrutture digitali.
5 DSP (Fornitori di servizi digitali) – marketplace online; cloud computing provider; motori di ricerca online.

Fig. 1.15: Spesa per la sicurezza informatica degli OSE/DSP, per settore (€ migliaia, 2021)

Fonte: ENISA, NIS Investments Report, 2022

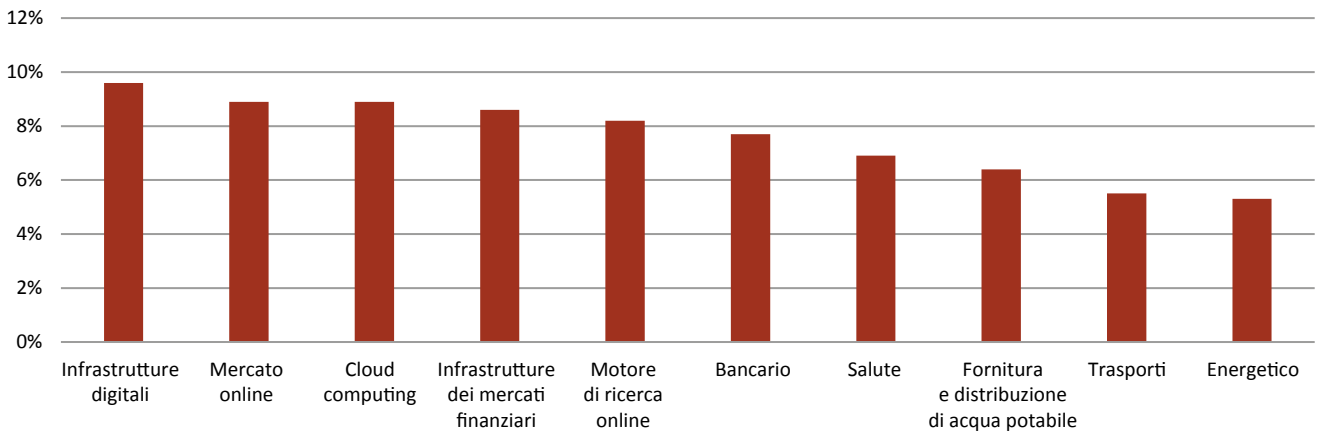


Spostando il focus sull'analisi settoriale, **le organizzazioni del settore bancario sono quelle che hanno investito di più in cibersicurezza in valori assoluti, con una media di €8,5 milioni nel 2021** (Fig. 1.15), seguite dalle imprese del settore energetico (€5,5 milioni) e i marketplace online (€3,8 milioni). I settori che hanno investito di meno a livello europeo nel 2021 sono i cloud computing providers, con una media di €1,9 milioni, i servizi idrici (€1,8 milioni) e, infine, le infrastrutture del mercato finanziario (€1,2 milioni).

Volgendo uno sguardo alla spesa per la sicurezza informatica come quota della spesa totale IT (Fig. 1.16), **le infrastrutture digitali risultano le più attente, con una media del 9,6% di budget IT dedicato alla cibersicurezza, seguite dai marketplace online e cloud computing providers, entrambi col 8,9%**. Diversamente, i servizi idrici (6,4%), i trasporti (5,5%) e il settore energetico (5,3%) chiudono la classifica in esame.

Fig. 1.16: Spesa per la sicurezza informatica come quota della spesa totale IT, per settore (2021)

Fonte: ENISA, NIS Investments Report, 2022



La figura successiva (Fig. 1.17) illustra i fattori esterni che influenzano gli investimenti in cybersicurezza degli OSE/DSP, distinguendoli in tre livelli d'importanza, con il primo che rappresenta quello principale. Lo scenario sopra citato circa l'aumento costante delle minacce cibernetiche ha rappresentato il motivo più impattante per un incremento degli investimenti dedicati alla cybersicurezza, con €752 mila corrispondenti al 23,2% del totale delle risorse allocate, risultando, altresì, il maggior volume di esborso afferente al livello 1, ossia quello considerato più importante per le organizzazioni in esame. La necessità di adeguarsi alla direttiva NIS occupa la seconda posizione con il 22,2% delle risorse mobilitate, seguita dal contesto normativo (17,3%). **Appare particolarmente interessante che l'aver subito una violazione dei dati sia la penultima motivazione, con un mero 7,7% delle risorse investite**.

Un altro importante indicatore circa l'andamento degli investimenti in cibersicurezza può essere rappresentato dal volume di ricavi che ha generato questo mercato globalmente. Difatti, le ultime stime effettuate da Statista attestano **i ricavi globali in cybersicurezza a circa €139,5 miliardi, mostrando un trend in forte crescita, che dovrebbe far registrare un importante raddoppio entro il 2026**.

Focalizzandosi sull'analisi delle principali economie globali (Fig. 1.18), è possibile osservare una netta prevalenza del mercato della cybersecurity statunitense, il quale ha raggiunto €59,3 miliardi nel 2022, più di Europa e Cina considerate congiuntamente. La figura riportata di seguito consente di evidenziare il considerevole distacco degli USA, che si è costantemente ampliato nel corso degli anni.

Quanto al mercato europeo, esso occupa stabilmente il secondo posto dal 2016, avendo varcato i €20,9 miliardi di ricavi nel 2022, quasi il doppio della Cina, la quale ha totalizzato €11,9 miliardi nello stesso periodo. Altro dato meritevole di essere menzionato concerne le previsioni al 2026 che, sebbene pongano comunque in evidenza l'ampio distacco tra gli USA e le altre due aree considerate, mostrano come il mercato europeo e quello cinese dovrebbero avere una crescita in termini percentuali più marcata rispetto a quella statunitense (pari al 42%), rispettivamente del 45% e del 66%.

Fig. 1.17: motivazione e classe di importanza degli investimenti nella cybersecurity nella UE (€ migliaia, 2021)

Fonte: ENISA, NIS Investments Report, 2022

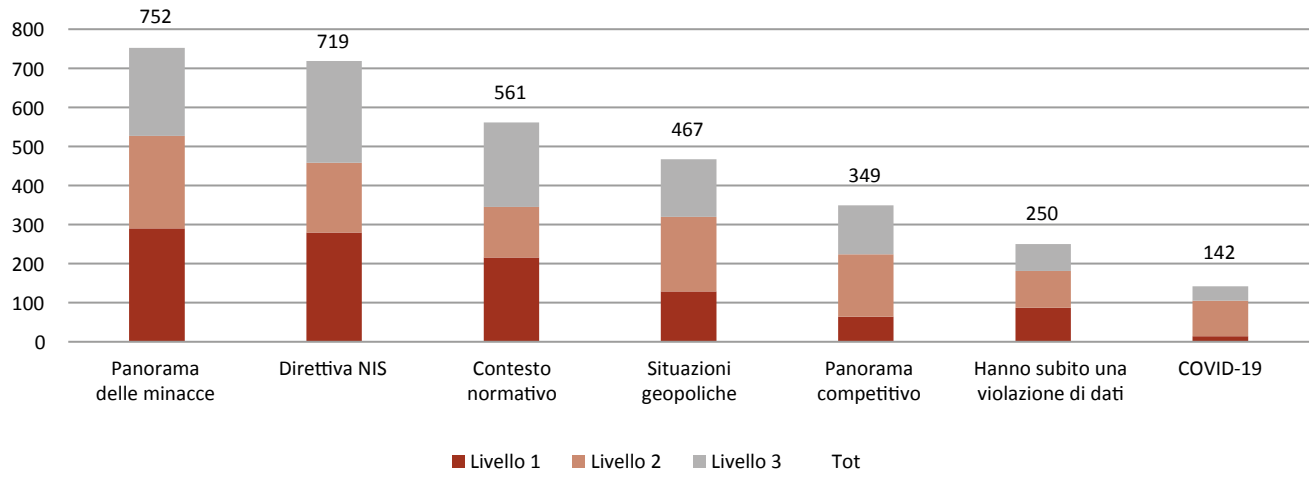
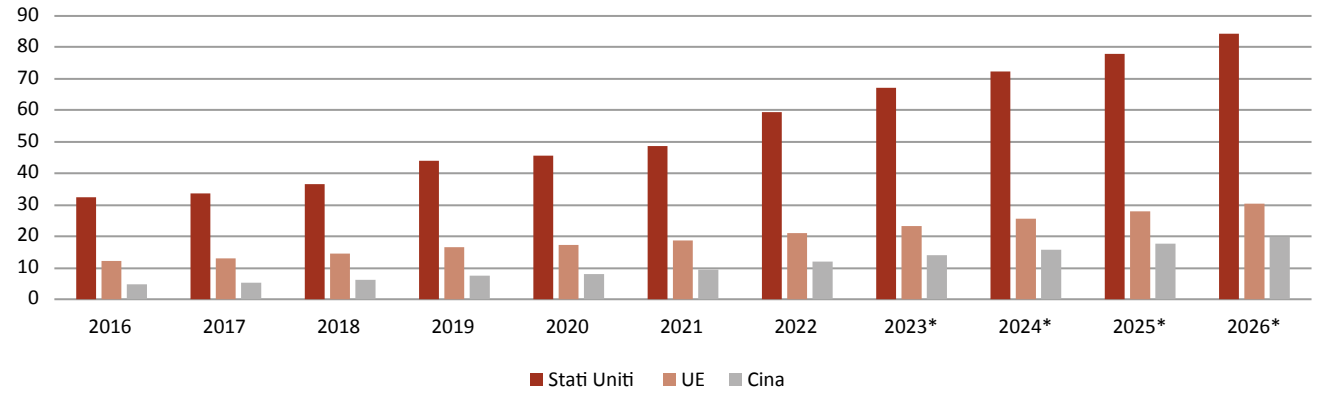


Fig. 1.18: Ricavi mercato cybersecurity negli Stati Uniti, Cina e UE (€ miliardi)

Fonte: Statista
*Dati previsionali

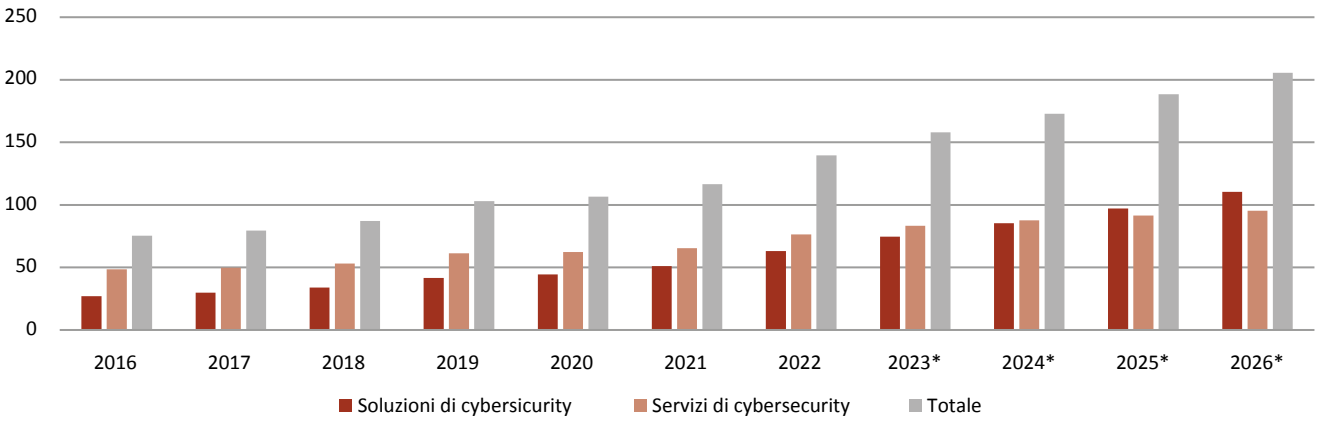


Peraltro, Statista ha condotto un'analisi in cui distingue le tipologie di prodotti di cibersicurezza acquistati in due categorie principali (Fig. 1.19), ovverosia:

- **le soluzioni di cybersecurity**, cioè quelle tecnologie automatizzate che supportano le attività di monitoraggio, rilevazione, segnalazione, contrasto e protezione delle organizzazioni dal rischio di attacchi informatici, incluso l'ormai tristemente noto phishing, che possono comportare, fra l'altro, estorsione di informazioni e violazioni di dati (tali soluzioni comprendono, ad esempio, strumenti per garantire la sicurezza di applicazioni, del cloud, dei dati e della rete);
- **i servizi di cybersecurity**, che si riferiscono a un processo globale o a un'ampia gamma di servizi che consentono di migliorare la protezione

Fig. 1.19: Ricavi globali per segmento (€ miliardi)

Fonte: Statista
*Dati previsionali



e la strategia di sicurezza di un'organizzazione contro le tipologie di attacchi informatici più comuni, tra cui il phishing, il malware o il ransomware (questi servizi ricomprendono la progettazione, l'integrazione, la consulenza, l'implementazione, la valutazione dei rischi e delle minacce, nonché la formazione e l'addestramento professionale).

I servizi di cybersecurity hanno rappresentato il 55% del mercato globale della cybersicurezza nel 2022, avendo prodotto un ricavo complessivo di circa €76 miliardi, mentre le soluzioni di cybersecurity si sono posizionate poco dietro con €63 miliardi (45%). **L'analisi previsionale al 2026 mostra che il mercato inerente entrambi i segmenti succitati potrebbe crescere sino a superare i servizi di cybersecurity, raggiungendo una quota di mercato del 53,7%**.

1.3. LA DIGITALIZZAZIONE DELLA PA

La **digitalizzazione dei servizi pubblici** è un elemento cruciale per garantire servizi più efficienti e accessibili ai cittadini e alle imprese. Nel contesto sempre più digitale del mondo moderno, la transizione verso servizi pubblici digitali è diventata una priorità europea. In questo paragrafo, ci concentreremo sul grado di digitalizzazione della pubblica amministrazione sia in Italia che in Europa.

Partendo dall'**offerta di servizi digitali per i cittadini** UE, i dati della Digital Agenda Scoreboard del 2022 mostrano una **situazione nel complesso moderatamente positiva** (Fig. 1.20), anche se rimangono larghi margini di miglioramento. Su una scala da 0 a 100 – dove un punteggio alto indica una maggiore percentuale di procedure amministrative che possono essere svolte online dai cittadini – il punteggio medio dell'UE è pari a 77. Il divario tra la media europea e l'Italia è di quasi 10 punti, con la PA italiana che si attesta a 67,9 punti. I Paesi in testa alla classifica sono Malta, che raggiunge il punteggio massimo di 100 punti, seguita da Lussemburgo, Estonia e Finlandia. In coda, invece, si trovano Polonia, Bulgaria e Romania.

Per quanto riguarda l'**offerta di servizi pubblici digitali per le imprese**, la situazione complessiva rimane positiva (Fig. 1.21). La media europea raggiunge un punteggio di 83,7, mentre l'Italia si attesta a 74,7. Nonostante il divario con la media dell'Unione Europea sia leggermente inferiore rispetto alla situazione relativa ai servizi per i cittadini, **l'Italia si posiziona nella parte inferiore della classifica**, seguita a breve distanza da Grecia, Polonia, Croazia e, infine, dalla Romania, il cui punteggio di 44,6 è notevolmente più basso rispetto a quello degli altri paesi europei.

Fig. 1.20: Servizi pubblici digitali per i cittadini (intervallo di valori tra 0 e 100, 2022)

Fonte: DESI 2023 indicators

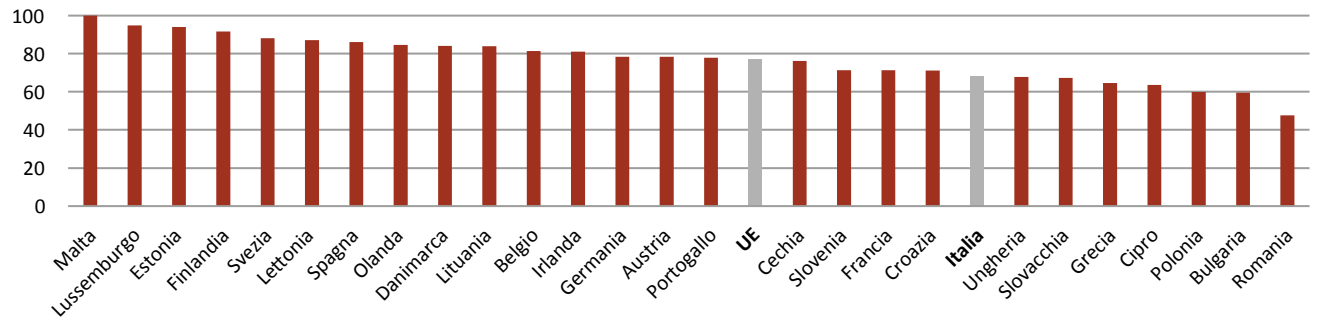
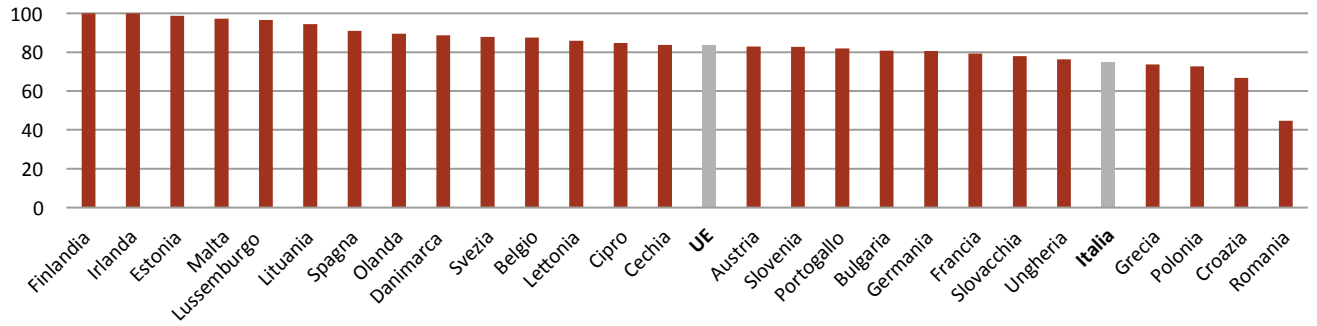


Fig. 1.21 Servizi pubblici digitali per le imprese (intervallo di valori tra 0 e 100, 2022)

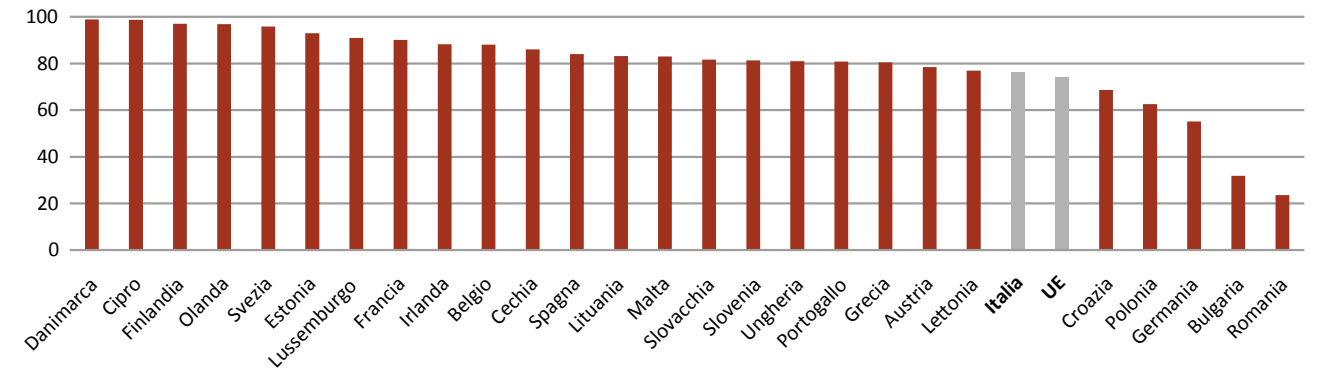
Fonte: DESI 2023 indicators



L'offerta di servizi pubblici digitali è fondamentale per garantire a imprese e cittadini un'efficiente interazione con la Pubblica Amministrazione, ma da sola non è sufficiente. Per sfruttare appieno le opportunità offerte dalla trasformazione digitale del settore pubblico, **è fondamentale che l'offerta si evolva parallelamente alla domanda.** In questa prospettiva, diventa essenziale che cittadini e imprese siano in grado di interagire in modo efficace con l'apparato amministrativo e, di conseguenza, possiedano le competenze digitali necessarie per farlo. Mentre il tema delle competenze verrà approfondito più avanti (vedi cap.9), la figura 1.22 mostra la percentuale di individui che nei 12 mesi precedenti alla rilevazione statistica dell'Eurostat, ha utilizzato **internet per interagire con le pubbliche autorità**. **In Italia, tale percentuale è pari al 76,3%, leggermente superiore alla media europea del 74,2%.** È tuttavia opportuno sottolineare che tale media è fortemente influenzata dalla situazione particolarmente negativa di alcuni paesi, nello specifico Bulgaria e Romania, la cui percentuale di utenti che interagiscono online con la PA è ancora ferma rispettivamente al 31,7% e 23,5%. La maggioranza dei restanti paesi, ad eccezione di

Fig. 1.22: Individui che hanno utilizzato internet, negli ultimi 12 mesi, per interagire con le pubbliche autorità su siti web o su applicazioni mobili (%, 2022)

Fonte: DESI 2023 indicators



Croazia, Polonia e Germina, si colloca invece al di sopra della media europea e presenta quindi un grado di interazione con le pubbliche autorità che può essere giudicato nel complesso positivo.

Per quanto riguarda il **grado di trasparenza dei processi, il coinvolgimento degli utenti nella progettazione dei servizi e la gestione da parte di questi ultimi dei propri dati personali**, la situazione in Europa è più eterogenea (Fig. 1.23). Su una scala che va da 0 a 100, la media UE è di 64,7. Malta è il paese più performante, raggiungendo un punteggio di 98, seguita da Lussemburgo (89) e dall'Estonia (86). L'Italia si posiziona in fondo alla classifica, con un punteggio di 49,2, seguono Slovacchia, Romania e Cipro.

Infine, considerando i **problemi riscontrati durante l'utilizzo dei siti web di e-Government**, nel 2022 circa il 15% dei cittadini europei ha dichiarato di aver riscontrato **problemi tecnici**, mentre il 12% ha avuto problemi dovuti alla **difficoltà di utilizzo** del sito Web o dell'applicazione mobile (Fig. 1.24). Simili percentuali emergono anche per l'Italia e sono rispettivamente pari al 13,5% e al 10,1%.

Fig. 1.23: Misura in cui i processi sono trasparenti, i servizi sono progettati coinvolgendo gli utenti e gli utenti possono gestire i propri dati personali (intervallo di valori tra 0 e 100, 2022)

Fonte: DESI 2023 indicators

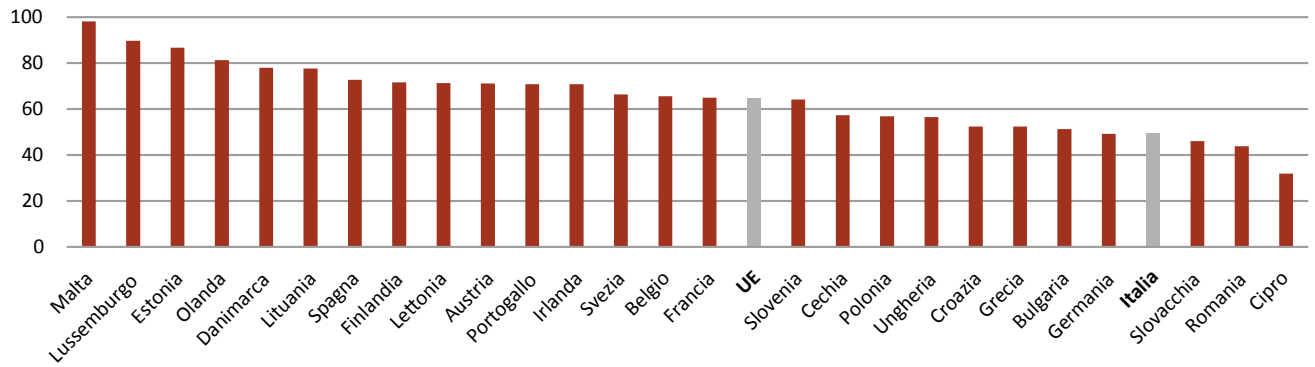
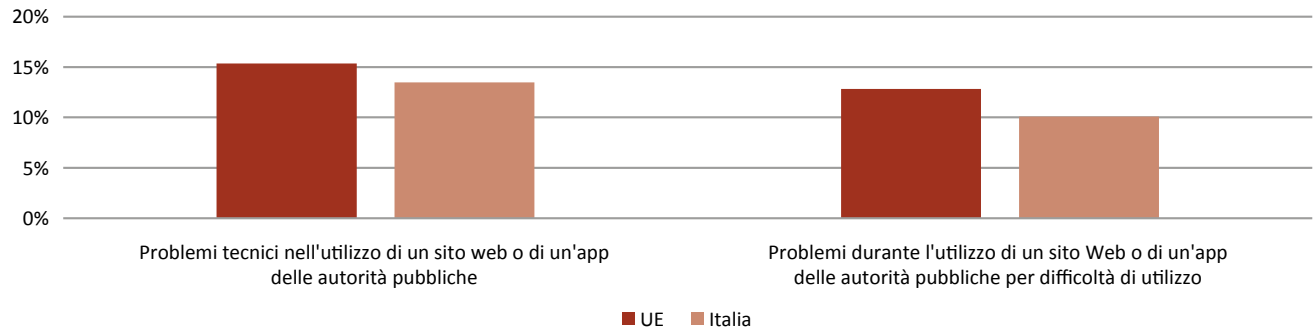


Fig. 1.24: Individui che hanno riscontrato problemi durante l'utilizzo dei siti web di e-government, per tipologia di problema (%, 2022)

Fonte: Eurostat



icom
istituto per la competitività

CAPITOLO 2

LE NUOVE FRONTIERE DELLA TECNOLOGIA: L'INTELLIGENZA ARTIFICIALE

2.1. I SISTEMI DI INTELLIGENZA ARTIFICIALE TRA SFIDE E OPPORTUNITÀ

L'**intelligenza artificiale** è sicuramente oggi considerata una delle più strabilianti frontiere tecnologiche per le grandi opportunità che offre sia al settore privato sia a quello pubblico.

Le applicazioni di intelligenza artificiale sono davvero molteplici e non è semplice fornire un quadro esaustivo e completo delle soluzioni adottate (o adottabili) dalle imprese e dai cittadini. Di seguito vengono indicate sei classi di soluzioni principalmente in uso[6]:

1. Il **chatbot o virtual assistant** è una delle soluzioni più diffuse tra le aziende italiane e internazionali. È uno strumento capace di offrire assistenza 24/7 sia ai clienti che ai dipendenti e si presta, inoltre, a diversi impieghi in ambito **marketing**, **HR management**, e **ricerca & sviluppo.**
2. Le **tecniche di NLP (Natural Language Processing)** si pongono l'obiettivo di creare sistemi in grado di favorire **l'interazione e la comprensione uomo/macchina**. L'NLP è alla base di programmi informatici che traducono il testo da una lingua all'altra, rispondono a comandi vocali e riassumono grandi volumi di testo rapidamente, anche in tempo reale, come applicazioni diventate molto famose con l'avvento di ChatGPT. Si può interagire con l'NLP sotto forma di sistemi GPS a comando vocale, assistenti digitali, software di dettatura speech-to-text, chatbot per il servizio clienti e altre funzionalità destinate ai consumatori. Ma l'NLP gioca anche un ruolo centrale nelle soluzioni aziendali che aiutano a snellire le operazioni di business, aumentare la produttività dei dipendenti e semplificare i processi di business mission-critical[7].
3. La **computer vision** studia algoritmi e tecniche per permettere ai computer di raggiungere una comprensione di alto livello del contenuto di immagini o video.
4. La classe di **soluzioni degli Intelligent Data Processing** è quella più ampia dal punto di vista delle applicazioni. Vi rientrano tutte quelle soluzioni che utilizzano algoritmi di intelligenza artificiale – su dati strutturati e non – per finalità collegate all'estrazione delle informazioni presenti nei dati stessi. Le principali finalità che spingono le imprese nell'utilizzo di queste soluzioni sono: **forecasting** e **classification & clustering**.
5. Gli **algoritmi di raccomandazione** per l'IA sono il pilastro del modello di business di tutte le **piattaforme social** ed **eCommerce** (Amazon, Netflix, Spotify, ma non solo). Alla base di tanti servizi digitali, ci sono algoritmi che tengono traccia delle azioni dell'utente e, comparandole con quelle degli altri, apprendono le sue preferenze e sono in grado, a mano a mano che l'utente utilizza la piattaforma, di produrre raccomandazioni più precise.
6. Le **soluzioni fisiche** di IA sono ancora poco diffuse tra le organizzazioni italiane. Sono tre le categorie da prendere in esame: i **veicoli autonomi**, gli **autonomous robot** (robot in grado di muoversi senza l'intervento umano) e gli **intelligent object** (oggetti in grado di compiere azioni senza l'intervento umano e di prendere decisioni in base alle condizioni dell'ambiente circostante).

Dunque, gli **ambiti applicativi** di questa tecnologia sono davvero innumerevoli e spaziano dal campo della **sanità** a quello dell'**internet of Things**, al campo del **fintech** e dell'**insurtech**, fino a quello della **privacy** e della **sicurezza Informatica,** con **impatti importanti sulle attività di imprese e pubbliche amministrazioni**, oltre che sulla vita delle persone.

6 https://blog.osservatori.net/it_it/intelligenza-artificiale-funzionamento-applicazioni#applicazioni-intelligenza-artificiale
7 https://www.ibm.com/it-it/topics/natural-language-processing

Le **applicazioni IA in ambito sanitario** possono portare a numerosi **benefici**, in termini di diagnosi più precise grazie all'analisi dei dati clinici dei pazienti, supportando così i medici nel prendere le decisioni e andando sempre più verso **una medicina personalizzata**. L'IA in ambito **fintech** e **insurtech** (ovvero nei settori finanziario e assicurativo abilitati dalle tecnologie digitali) è sempre più diffusa per via della possibilità di **conoscere in maniera più approfondita i propri clienti** e della finalità di **garantire un servizio mirato e coerente** con il rispettivo profilo di rischio
Nell' **eCommerce e retail**, i **recommendation system** sono tra le applicazioni più utilizzate, in grado di suggerire acquisti basandosi su quelli fatti in precedenza, influenzando l'utente nel suo processo decisionale. Nel caso di negozi fisici, invece, le applicazioni di IA sono presenti per esempio nei **camerini dotati di display trasparenti e touch**, che forniscono in tempo reale le informazioni richieste da cliente e, una volta comprese le preferenze, mostrano i prodotti in linea con i propri interessi.
In **cybersecurity** le soluzioni IA possono svolgere diverse funzioni: vengono impiegate per rilevare e prevenire le anomalie nel traffico di rete e per analizzare e correlare grandi quantità di dati provenienti da diverse fonti, con l'obiettivo di **identificare le minacce** (come gli attacchi informatici) e accelerare il tempo di risposta. Inoltre, l'IA può essere impiegata per automatizzare e orchestrare le azioni di risposta a eventuali incidenti, riducendo così il carico di lavoro e gli errori umani. Infine, sistemi di *detect* and *response* vengono integrati a sistemi evoluti di IA e machine learning per monitorare le attività dei dispositivi e bloccare **malware** e **ransomware**[8].
Tante sono le **opportunità** legate a questa nuova frontiera tecnologica. Tuttavia, essa solleva non poche **sfide**, di ordine etico e legale. Ad esempio, i contenuti generati dall'intelligenza artificiale potrebbero essere utilizzati per scopi dannosi, come la diffusione di disinformazione o la creazione di deepfake. Risulta perciò fondamentale che gli sviluppatori e le piattaforme implementino linee guida e regolamenti etici per evitare che l'IA venga utilizzata per scopi malevoli. Altri rischi riguardano la sicurezza e la privacy in termini di mancanza di tutela dei dati degli utenti e di furto di identità. A questi si aggiunge la mancanza di trasparenza dei processi decisionali che caratterizzano i sistemi di IA e la disuguaglianza in termini di accessibilità alle tecnologie. Infine, l'IA può avere implicazioni sull'evoluzione del mercato del lavoro in ragione della crescente automazione di alcuni task lavorativi.

2.2. IL MERCATO DELL'INTELLIGENZA ARTIFICIALE E L'UNIONE EUROPEA NELLA COMPETIZIONE GLOBALE

Il crescente interesse nei confronti delle numerose applicazioni IA è confermato anche dai dati. Stando ad alcune stime, si prevede che il **mercato mondiale** dell'intelligenza artificiale toccherà i **$241,8 miliardi entro la fine del 2023**. Le dimensioni del mercato IA[9] mostreranno un tasso di crescita annuale (CAGR 2023-2030) del 17,3%, raggiungendo un volume di mercato di $738,8 miliardi di dollari entro il 2030 (Fig. 2.1). E a trainare principalmente tale crescita saranno le applicazioni basate sulle tecniche di machine learning.
Nel confronto globale, gli Stati Uniti coprono il 36% del mercato IA, seguiti da Cina (12%), Germania (4%) e Regno Unito (4%). L'Italia non va oltre il 2%, posizionandosi comunque all'ottavo posto a pari merito con l'Australia (Fig. 2.2).

8 Ibidem
9 Le dimensioni del mercato sono generate dall'importo dei finanziamenti delle società di intelligenza artificiale (IA) in progetti ed iniziative IA.

Fig. 2.1: Il mercato mondiale dell'intelligenza artificiale ($ miliardi, 2023)

Fonte: stime Statista

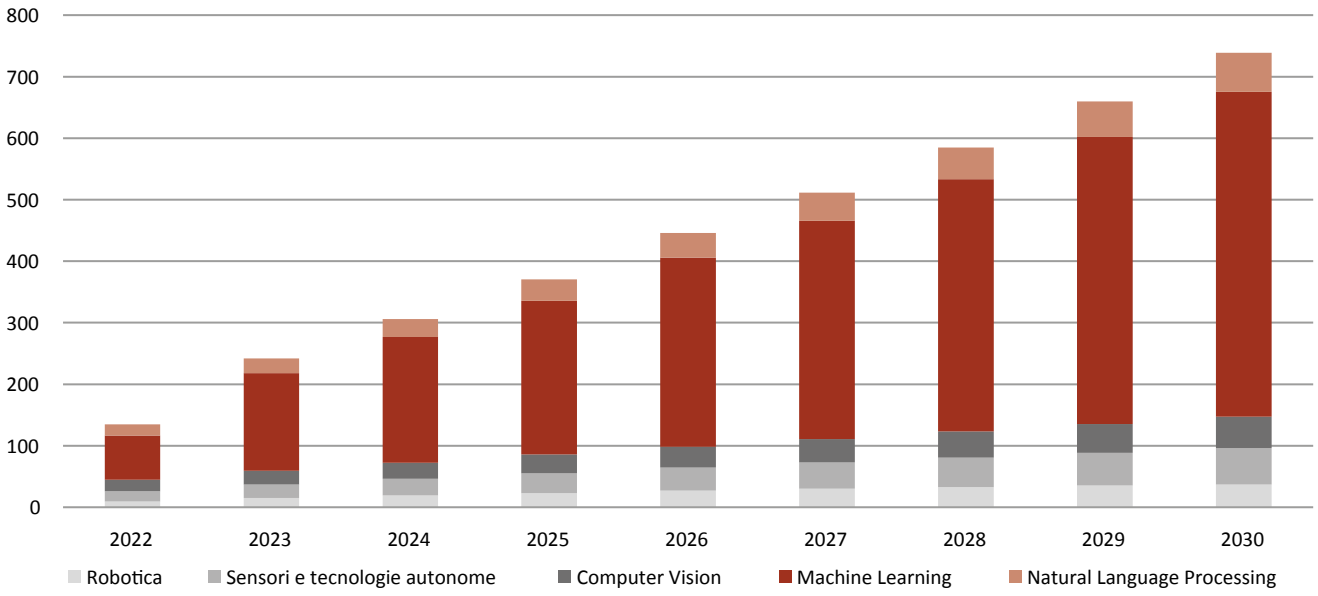
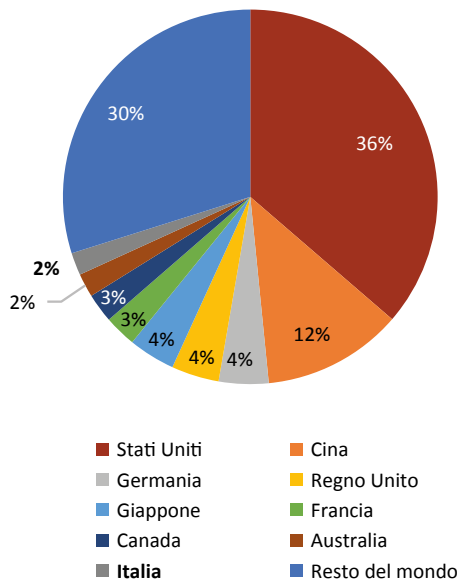


Fig. 2.2: Il mercato mondiale dell'intelligenza artificiale, per Paese (% del valore totale, 2023)

Fonte: elaborazioni I-Com su stime Statista

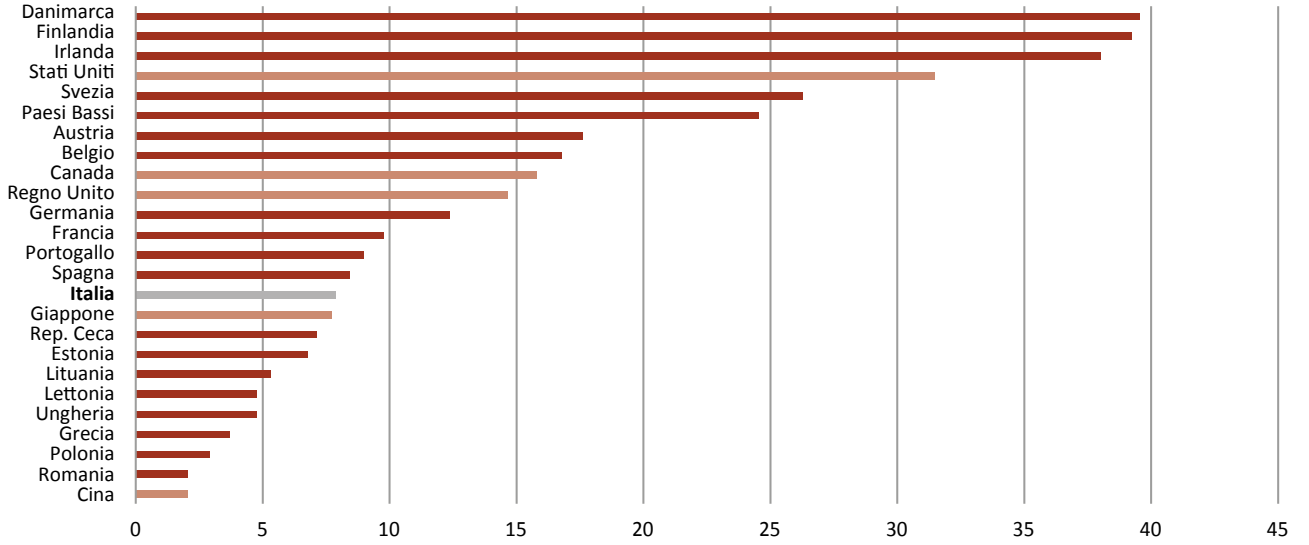


Tenendo conto delle dimensioni della popolazione di ciascun paese, la **Danimarca** risulta il più grande mercato dell'IA a livello globale, con un valore di mercato per 100.000 abitanti di circa $39 milioni, seguita da **Finlandia** e **Irlanda**. Gli **Stati Uniti** si collocano, invece, in quinta posizione anche se in termini assoluti mostrano il valore di mercato più alto ($87,18 miliardi nel 2023). La **Germania** è il più grande mercato dell'IA in Europa in termini assoluti ($10,30 miliardi nel 2023). Tuttavia, in termini relativi si colloca in undicesima posizione nella classifica globale (e ottava tra i 20 Stati membri UE considerati, con $12 milioni per 100.000 abitanti). L'Italia addirittura quindicesima (e dodicesima UE, dunque oltre la metà della classifica) con circa $8 milioni per 100.000 abitanti, un valore pari a 1/5 di quello danese e meno di 1/3 di quello statunitense (Fig. 2.3).

Negli ultimi anni, con una evidente accelerazione nell'ultimo, il mercato dell'IA è sempre più trainato dall'**IA generativa** ovvero un nuovo campo di ricerca

Fig. 2.3: Valore di mercato IA/100.000 abitanti (in milioni di $) – Confronto tra gli Stati Membri e Stati Uniti, Canada, Regno Unito, Cina e Giappone

Fonte: elaborazioni I-Com su dati Statista, Eurostat e OCSE



che utilizza tecniche di Machine Learning e Deep Learning per generare nuovi dati, tra cui immagini, musica e testo, che non esistevano in precedenza.

L'IA generativa rappresenta già oggi una fetta rilevante del mercato IA, destinata ad aumentare nei prossimi anni. Nel 2023 copre il 19% del mercato totale e secondo le stime arriverà ad un'incidenza del 28% entro il 2030 (Fig. 2.4).

Il segmento dell'IA generativa è destinato, dunque, ad esplodere, partendo da una dimensione di mercato di "soli" $40 miliardi di ricavi nel 2022 e arrivando fino a $1,3 trilioni nei prossimi 10 anni. Si prevede

Fig. 2.4: Il mercato mondiale dell'IA generativa (in % del totale del mercato IA)

Fonte: elaborazioni I-Com su stime Statista

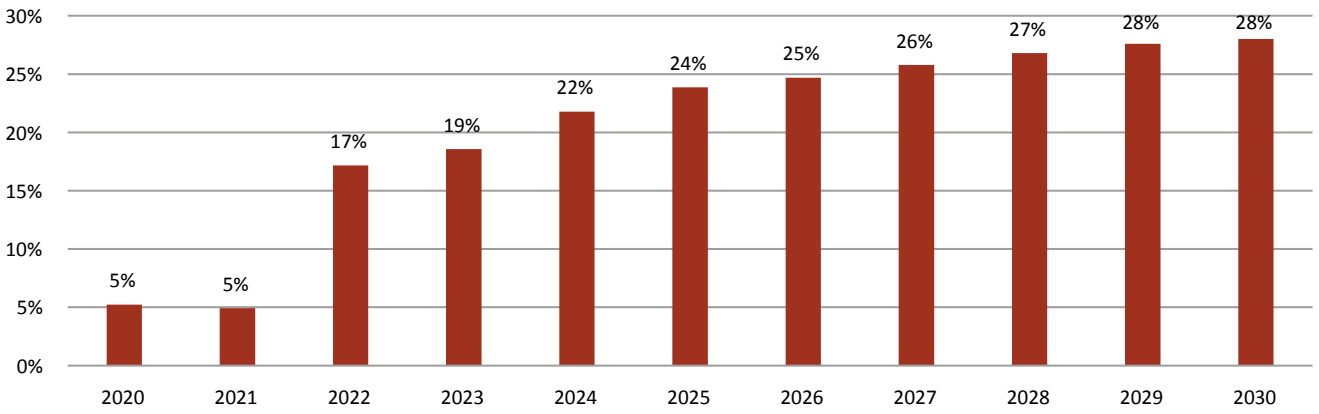


Fig. 2.5: Il mercato dell'IA generativa negli Stati membri (%, 2023)

Fonte: elaborazioni I-Com su stime Statista

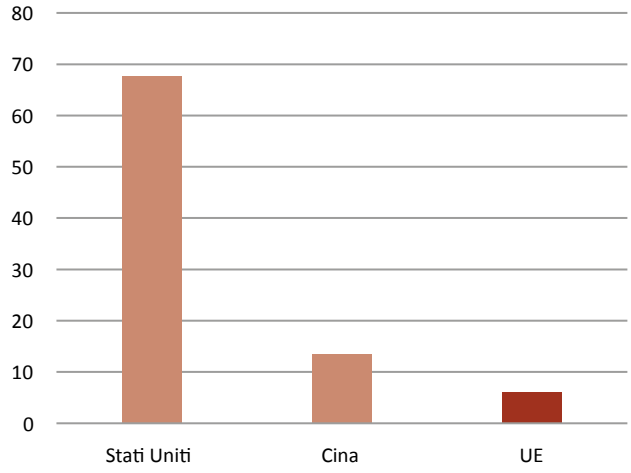
che il valore mostrerà un tasso di crescita annuo (CAGR 2022-2032) del 42%[10].

Tra i principali Stati membri, la **Germania** è il più grande mercato dell'IA generativa, coprendo il 22% del mercato totale europeo, seguita da **Francia** (14%) e **Italia** (10%).

Dunque, la corsa all'intelligenza artificiale appare in pieno svolgimento e un'ulteriore conferma è data dal volume degli **investimenti privati in IA**, che aumentano costantemente.

Fig. 2.6: Investimenti venture capital in IA ($ miliardi, 2023*)

Fonte: OCSE, 2023
Nota: *stime



Gli **Stati Uniti** continuano ad essere il paese leader in termini di investimenti venture capital nell'IA. Nel 2023, i $67,7 miliardi investiti negli Stati Uniti rappresentano circa cinque volte l'importo investito in **Cina** (€13,5 miliardi) e undici volte l'importo investito nell'**UE** (€6,1 miliardi) (Figura 2.6).

Tra i Paesi UE, la **Francia**, la **Germania** e la **Svezia** si collocano sul podio con un volume di investimenti venture capital che complessivamente copre circa il 65% degli investimenti VC totali in UE. L'**Italia** si classifica in ottava posizione (204 milioni di dollari) dietro a paesi come **Romania**, **Spagna** e **Irlanda** (Figura 2.7).

Anche in termini di **startup IA**, gli **Stati Uniti** continuano a guidare la classifica mondiale con
542 realtà finanziate per la prima volta nel 2022. Seguono **Cina** e **Regno Unito**, rispettivamente con 160 e 99 startup IA. I principali Paesi UE per numero di startup seguono a distanza con un numero di nuove imprese finanziate nel 2022 che non rappresentano nemmeno 1/4 di quelle statunitensi (Figura 2.8).

L'**UE** continua pertanto a far fatica a stare al passo con Stati Uniti e Cina, nonostante una maggiore specializzazione nell'IA acquisita negli ultimi anni.

10 https://www.bloomberg.com/company/press/generative-ai-to-become-a-1-3-trillion-market-by-2032-research-finds/

Fig. 2.7: Investimenti venture capital in IA, per Paese UE ($ milioni, 2023*)

Fonte: OCSE, 2023
Nota:*stime

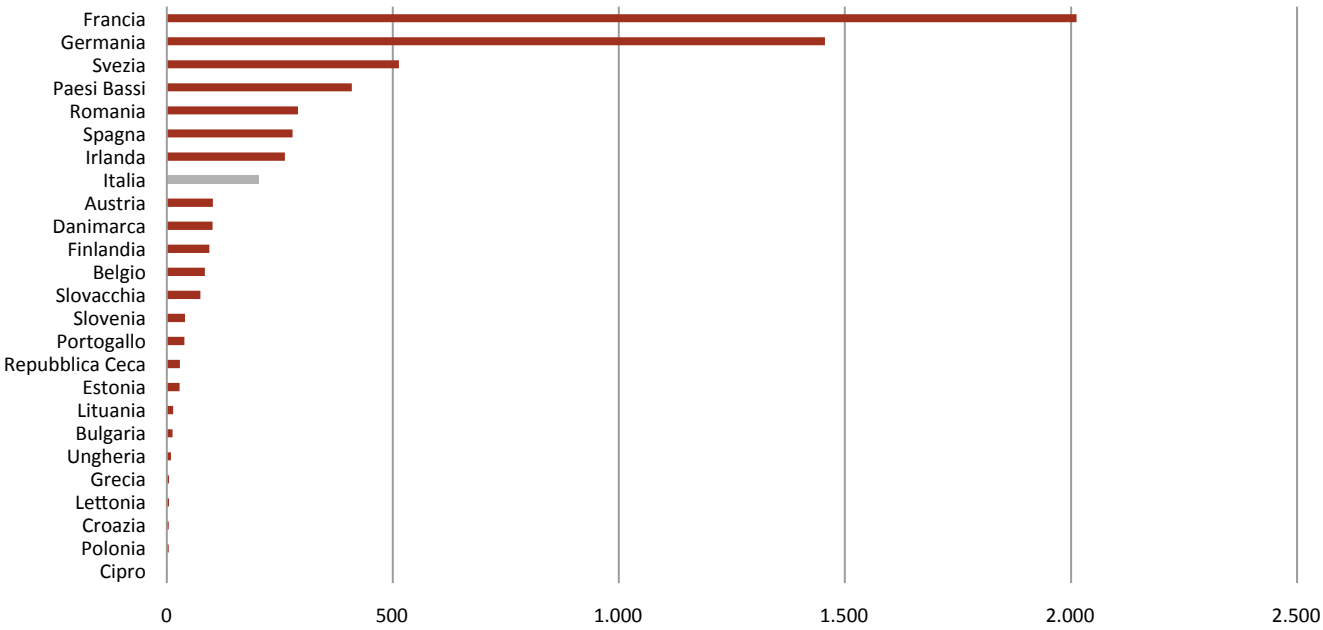
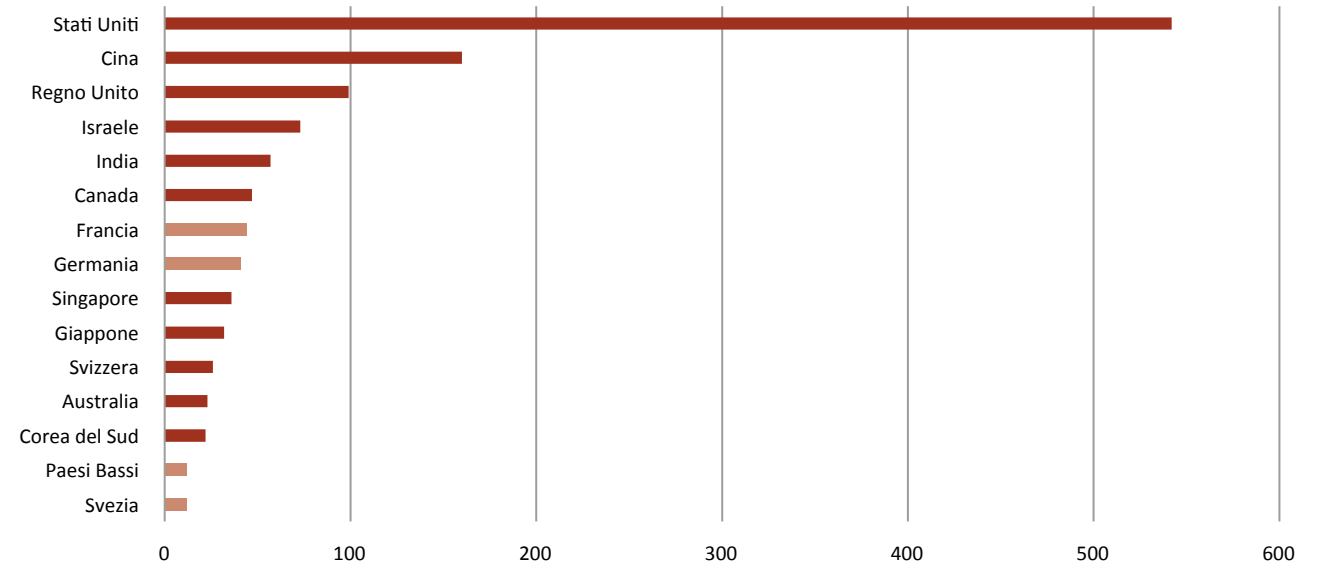


Fig. 2.8: Numero di startup IA finanziate per la prima volta, per Paese (2022)

Fonte: Stanford University, 2023



2.3. LA DIFFUSIONE DELL'INTELLIGENZA ARTIFICIALE NELLE IMPRESE

Secondo una survey di McKinsey contenuta nello studio "The state of AI in 2022—and a half decade in review"[11], l'**adozione dell'IA da parte delle imprese** di tutto il mondo è più che raddoppiata in soli 6 anni. Nel 2017, il 20% delle organizzazioni aveva riferito di adottare applicazioni IA in almeno un'area di business. Nel 2022, la percentuale è salita al 50%, con il picco più alto registrato però nel 2019 (58%) (Fig. 2.9).

Alcune applicazioni, quali ad esempio la generazione del linguaggio naturale, il riconoscimento delle immagini, i sistemi di supporto alle decisioni, il machine learning e la robotica hanno raggiunto livelli di maturità tali da poter essere già adesso applicate a gran parte dei prodotti e dei servizi di largo consumo.
In particolare, sempre secondo lo studio di McKinsey, **il numero medio di funzionalità di intelligenza artificiale utilizzate dalle organizzazioni**, come la generazione del linguaggio naturale e la visione artificiale, **è raddoppiato**, passando da 1,9 nel 2018 a 3,8 nel 2022 (Fig. 2.10).

Fig. 2.9: Percentuale di intervistati che affermano che la loro organizzazione ha adottato l'IA in almeno una funzione aziendale o area di business

Fonte: McKinsey & Company, 2022

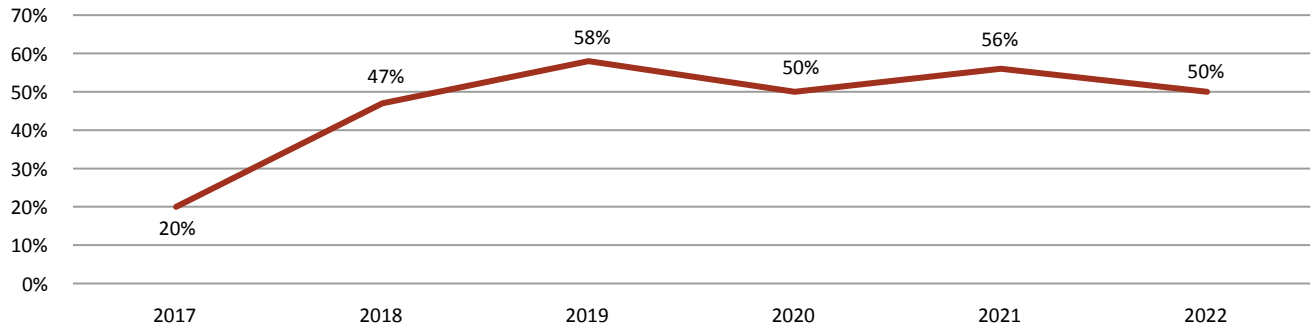
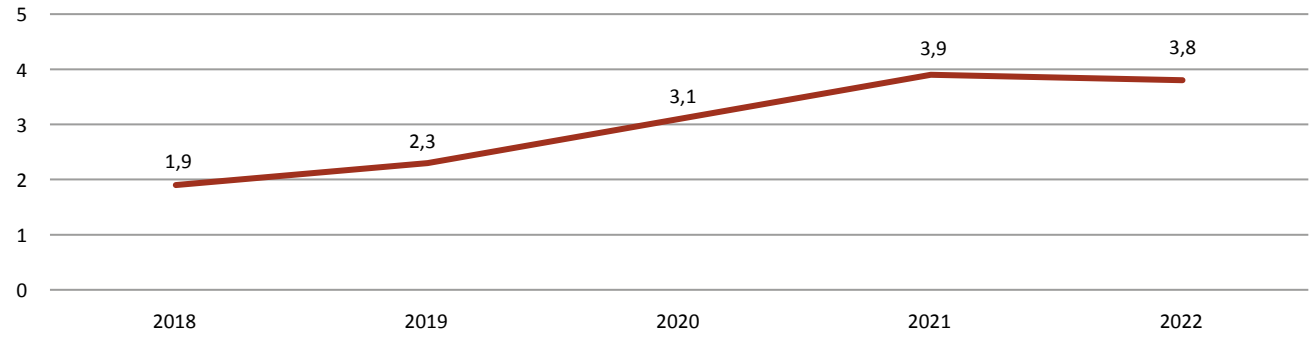


Fig. 2.10: Numero medio di funzionalità IA impiegate all'interno di almeno una funzione aziendale o area di business

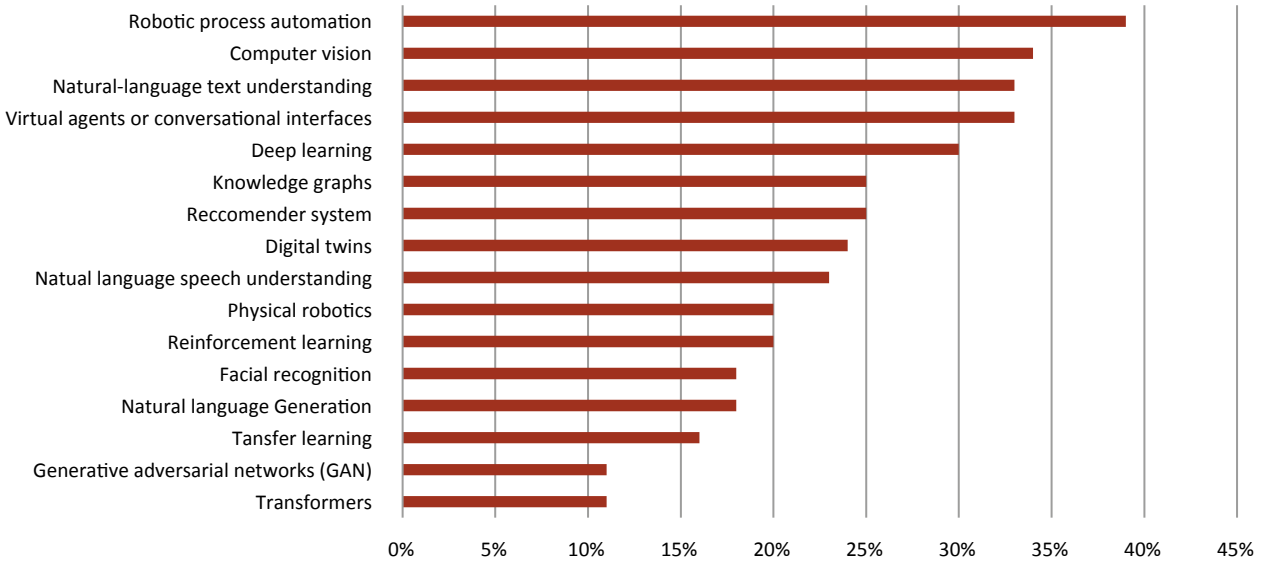
Fonte: McKinsey & Company, 2022



11 https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2022-and-a-half-decade-in-review#/

Fig. 2.11: Percentuale di intervistati che affermano che una determinata funzionalità di intelligenza artificiale è incorporata in prodotti o processi aziendali in almeno una funzione o area di business (2022)

Fonte: McKinsey & Company, 2022

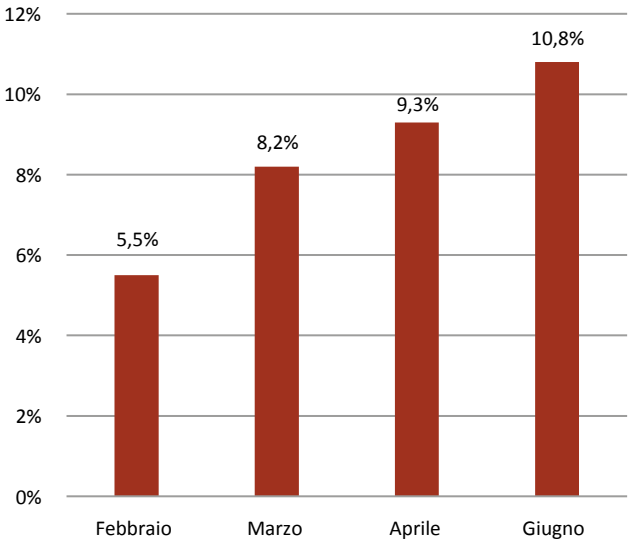


L'automazione robotica dei processi e la visione artificiale sono le funzionalità IA maggiormente implementate. Ben il 39% degli intervistati ha dichiarato che nella propria organizzazione si fa ricorso a sistemi di automazione dei processi, e il 34% alla visione artificiale. Tra le altre funzionalità IA di uso comune tra le imprese rientrano la comprensione del linguaggio naturale, gli agenti virtuali e il deep learning (Fig. 2.11).

Anche l'IA generativa sta riscuotendo molto interesse tra le imprese di tutto il mondo. L'ultimo aggiornamento di dati di Statista conferma un aumento del numero di dipendenti aziendali a livello mondiale che utilizzano **ChatGPT** – a tutt'oggi l'applicazione simbolo (ma non certo l'unica) dell'IA generativa – in ambito lavorativo. Nello specifico, a partire da giugno 2023, il 10,8% dei dipendenti delle aziende di tutto il mondo ha utilizzato ChatGPT sul posto di lavoro almeno una volta: un dato in aumento di oltre 5 punti percentuali rispetto a tre mesi prima (Fig. 2.12).

Fig. 2.12: Numero di dipendenti a livello globale che ha utilizzato ChatGPT almeno una volta in ambito lavorativo (%, 2023)

Fonte: Statista, 2023



In generale, l'**uso di applicazioni di IA generativa sta crescendo in modo esplosivo in tutti i settori economici**. Un recentissimo sondaggio di McKinsey a livello globale[12] evidenzia che il 33% degli intervistati del settore tecnologico, dei media e delle telecomunicazioni utilizza regolarmente l'IA generativa per lavoro o al di fuori del lavoro, mentre il 37% degli intervistati dello stesso settore ha dichiarato di aver utilizzato questa tecnologia almeno una volta. Altri due settori che usano questi nuovi strumenti sono i servizi finanziari e i servizi aziendali, legali e professionali in cui quasi un quarto degli intervistati utilizza regolarmente l'IA generativa (Fig. 2.13).

Soffermando l'attenzione sull'**adozione dell'intelligenza artificiale nell'UE**, si può osservare che solo l'**8% delle imprese UE ha adottato almeno**

Fig. 2.13: L'uso delle applicazioni di IA generativa nei principali settori economici (%, 2023)

Fonte: McKinsey & Company, 2023

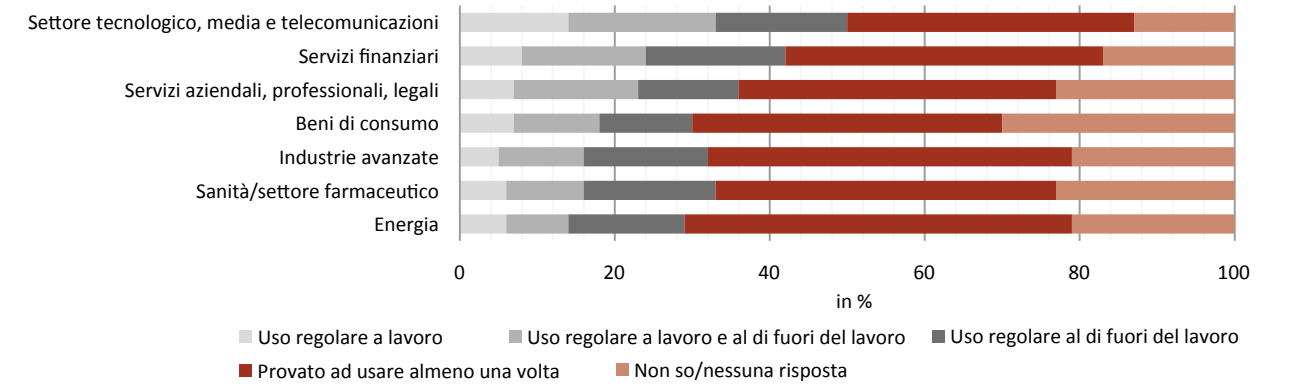
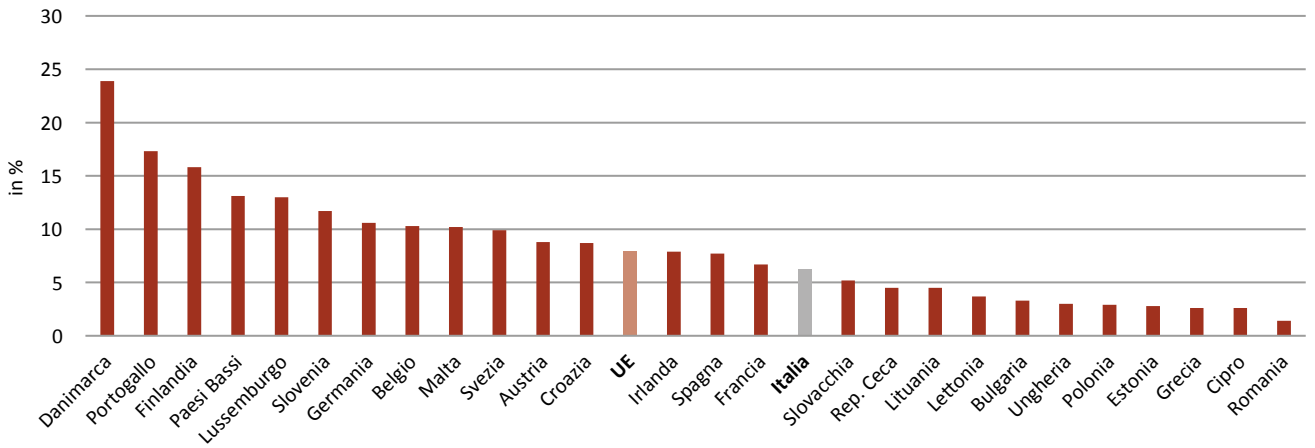


Fig. 2.14: Imprese UE che hanno adottato almeno una tecnologia IA (%, 2021)

Fonte: Eurostat



12 https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-AIs-breakout-year

una tecnologia IA. Il tasso di adozione più elevato si registra in **Danimarca**, dove circa un'impresa su quattro ha fatto uso di almeno una tra le tecnologie intelligenti più comuni. In fondo alla classifica si trova la **Romania**, che presenta il livello più basso di adozione IA con solo l'1,5% di imprese che ha utilizzato almeno una tecnologia. L'**Italia** si colloca al di sotto della media UE, con circa il 6% delle imprese che ha adottato almeno una tra le tecnologie IA a disposizione (Fig. 2.14).

Tra le diverse tecnologie IA, l'Italia presenta la performance migliore nella **robotica di servizio**, unico campo dove si colloca nettamente al di sopra della media UE, con oltre il 4% delle imprese che ha adottato robot

Fig. 2.15: L'adozione delle tecnologie IA più comuni (%, 2021)

Fonte: Eurostat

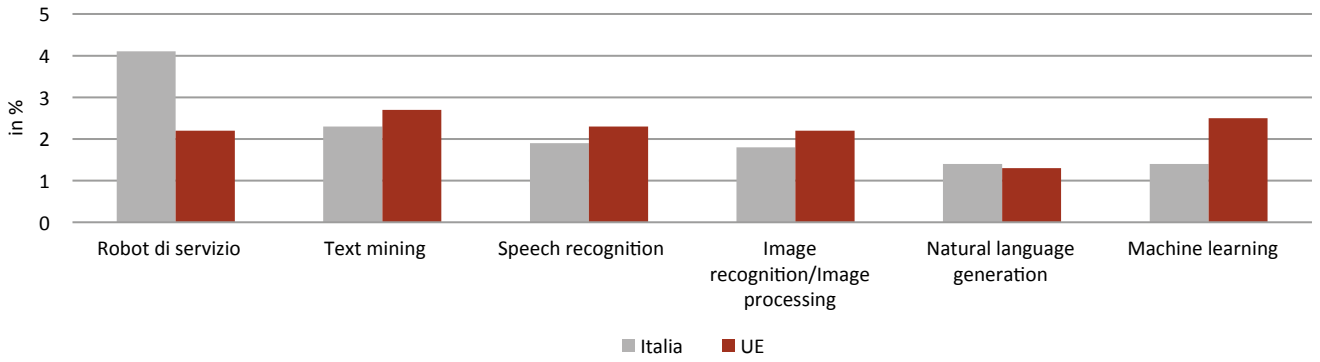
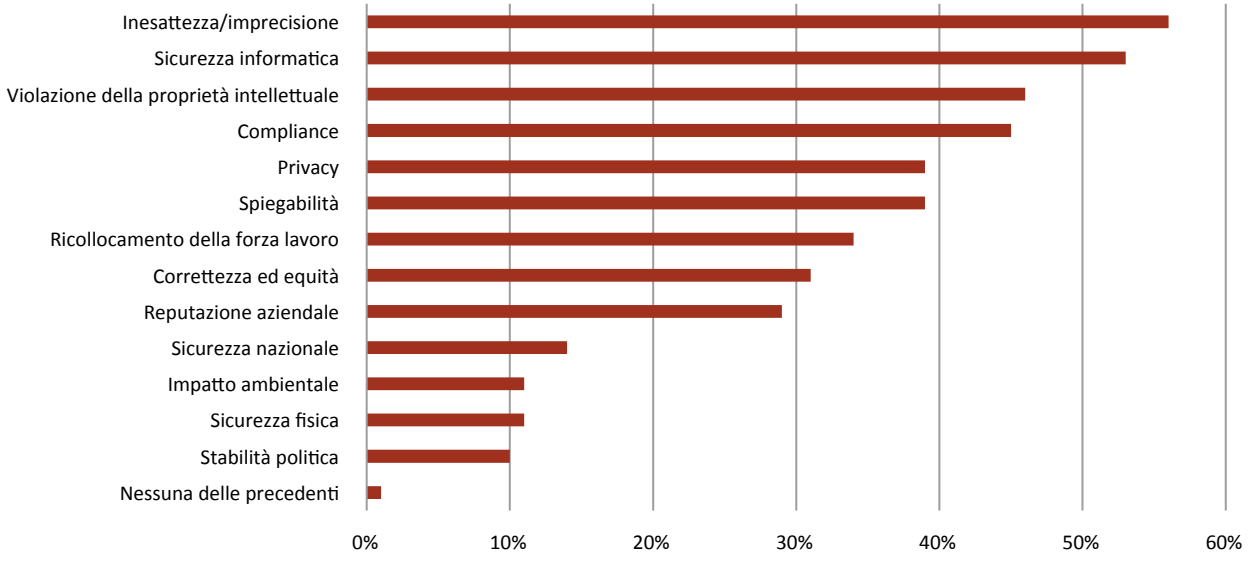


Fig. 2.16: I principali rischi relativi all'IA generativa secondo le imprese (%, 2023)

Fonte: McKinsey & Company, 2023



di servizio (Fig. 2.15). Anche gli ultimi dati dell'IFR (la Federazione Internazionale di Robotica) confermano il boom delle installazioni di robot di servizio nel nostro Paese, dove soprattutto il settore dell'hospitality (ristoranti, hotel e l'industria del turismo in generale) mette a segno un aumento del 125% nell'utilizzo dei robot destinati ai servizi professionali, con circa 24.500 unità vendute nel 2022[13].

Nonostante il largo impiego delle tecnologie IA nelle imprese di tutto il mondo, permangono i timori e aumenta la percezione di determinati rischi legati a questa tecnologia. Sempre secondo i dati rilevati da McKinsey in una recente survey del 2023[14], tra i **principali rischi relativi nello specifico all'IA generativa ma che sostanzialmente riguardano l'IA nel complesso**, considerati rilevanti dalle organizzazioni rientrano quelli legati all'inesattezza/imprecisione delle tecnologie (56% degli intervistati), alla sicurezza informatica (53%) e alla violazione dei diritti di proprietà intellettuale (46%). A questi poi si aggiungono i timori relativi alla privacy e alla sicurezza dei dati personali, al ricollocamento della forza lavoro nonché rischi reputazionali (Fig. 2.16).

2.4.* SURVEY SULLE RICERCHE ONLINE RELATIVE ALL'INTELLIGENZA ARTIFICIALE

Il presente paragrafo analizza l'**interesse nei confronti dell'IA** in termini di uso, rischi e opportunità percepiti, attraverso l'osservazione di determinate keyword utilizzate nelle ricerche effettuate in rete dagli utenti nel periodo compreso tra **settembre 2020 e agosto 2023**. **L'intento dell'indagine realizzata da Bytek e I-Com** e che prende in considerazione cinque Paesi (**Italia**, **Stati Uniti**, **Francia**, **Germania** e **Spagna**) **consiste nel comprendere quanto sia attuale il tema dell'intelligenza artificiale** e cerca di mettere in evidenza analogie e differenze tra i vari paesi analizzati, in un momento storico di profonda trasformazione, in cui il lancio di ChatGPT di Open AI e quello di Google Bard certamente hanno acceso, ora più che mai, i riflettori su questa nuova frontiera tecnologica e influenzato la percezione degli individui e, dunque, questa è la nostra ipotesi di partenza, la qualità e la quantità delle ricerche effettuate.

L'analisi per il presente studio è basata su **dati raccolti in rete** da Bytek, società specializzata in soluzioni software proprietarie IA che annoverano tra le altre finalità la possibilità di misurare i trend online, valutando la dinamica del volume delle ricerche effettuate sul motore di ricerca di Google in termini di argomenti relativi all'IA.

Ci si è avvalsi, dunque, di una **metodologia** generalmente impiegata per la realizzazione di indagini di mercato online che presenta, tra gli altri, il vantaggio di riuscire a bypassare le tradizionali reticenze a rispondere da parte degli intervistati o fenomeni quali il "response set"[15].

Dal punto di vista pratico, l'analisi riportata nel presente paragrafo è stata svolta seguendo diversi step.

In primo luogo, a partire dall'argomento oggetto di indagine "intelligenza artificiale" sono state individuate una serie di **"keyword"** o **"query di ricerca"** che generalmente gli individui inseriscono su Google per cercare informazioni di loro interesse. Per ognuna di queste query è stato individuato il volume di ricerca mensile.

Una volta individuate tutte le query di interesse queste sono state raggruppate in subcluster specifici (es.

* Realizzato in collaborazione con ByTek

13 https://www.innovationpost.it/tecnologie/robotica/robotica-di-servizio-boom-di-istallazioni-48-nel-2022/

14 https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-AIs-breakout-year

15 La tendenza degli intervistati a rispondere in maniera piuttosto simile a tutte le domande, spesso in accordo con l'idea di ciò che il rispondente si è fatto rispetto a ciò che l'intervistatore sta cercando di misurare.

ricerche su cos'è l'IA, ricerche su come funziona l'IA, ricerche relative ai rischi dell'IA, ricerche relative ai corsi universitari e non su IA, ecc.). I subcluster omogenei sono stati a loro volta raggruppati in Cluster più ampi (es. ricerche generiche, ricerche sulla paura correlata all'IA, ricerche sulla formazione).

Il primo dato interessante che emerge dall'analisi è relativo al **numero totale di ricerche** effettuate in rete sull'intelligenza artificiale, che ha una vera e propria impennata in tutti i Paesi oggetto dell'analisi (eccetto la Germania) tra il terzo e il quarto trimestre 2022, periodo coincidente con il lancio di ChatGPT (Fig. 2.17). Gli Stati Uniti guidano la classifica con il maggior numero di ricerche in termini assoluti. Andando a parametrare le ricerche totali sull'IA rispetto alla popolazione nel primo semestre 2023, gli Stati Uniti continuano a rappresentare il paese in cui si è registrato il maggior interesse generale verso l'argomento, con oltre 60 mila ricerche ogni 100.000 abitanti (Fig. 2.18). Seguono la **Francia** e l'**Italia** con rispettivamente 51.506 e 33.950 ricerche pro-capite effettuate nel corso del primo semestre dell'anno in corso.

L'interesse nei confronti dell'intelligenza artificiale sta sicuramente aumentando grazie all'avvento dell'**intelligenza artificiale generativa** che sta influenzando il settore sotto tanti punti di vista. Interesse davvero sorprendente negli **Stati Uniti**, dove le ricerche online del termine "generative AI" sono cresciute in modo esponenziale a partire da ottobre 2022 e pongono la prima superpotenza mondiale in vetta anche in termini relativi. Una palese conferma, lato domanda, della leadership tecnologica statunitense. Laddove, invece, in **Italia**, **Spagna** e **Francia** l'interesse è molto meno diffuso anche se negli ultimi mesi la tendenza a ricercare informazioni online sull'IA generativa è in aumento, specie nel nostro Paese (Fig. 2.19 e 2.20).

Passando all'analisi del numero di ricerche online relative ad informazioni circa l'**utilizzo dell'intelligenza artificiale**, emerge come in tutti i Paesi analizzati l'interesse maggiore si concentri su ricerca di **app IA per foto/immagini, che nel caso dell'Italia è pari al 55%**. Altri utilizzi che suscitano interesse, specie **in Italia**, tanto da essere oggetto di specifiche ricerche online sono chat IA oppure

Fig. 2.17: Ricerche totali su IA, per trimestre

Fonte: elaborazioni I-Com su dati Bytek

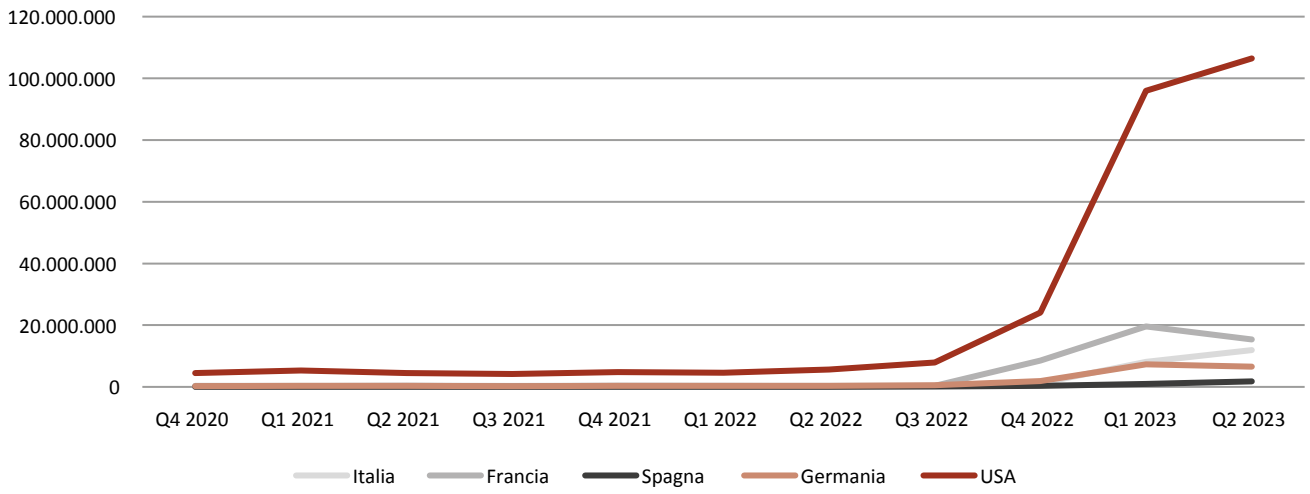


Fig. 2.18: Ricerche totali su IA effettuate nel primo semestre 2023 per 100.000 abitanti

Fonte: elaborazioni I-Com su dati Bytek

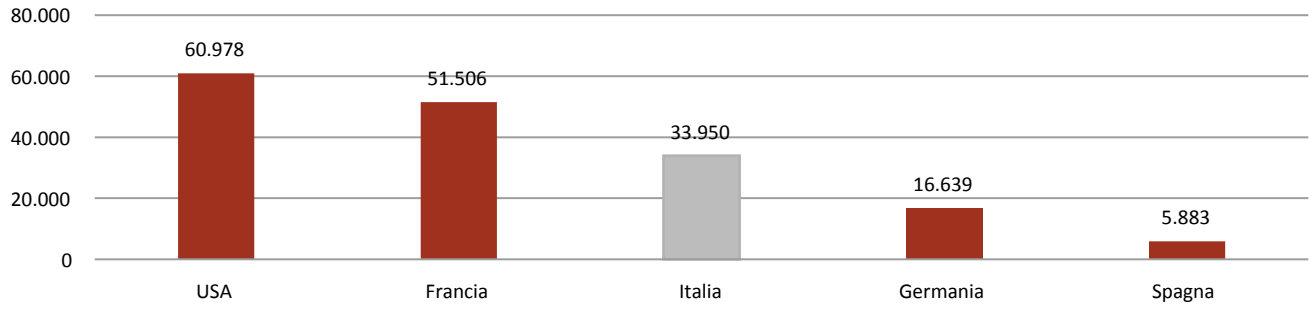


Fig. 2.19: Ricerche mensili su "IA generativa", per Paese

Fonte: elaborazioni I-Com su dati Bytek

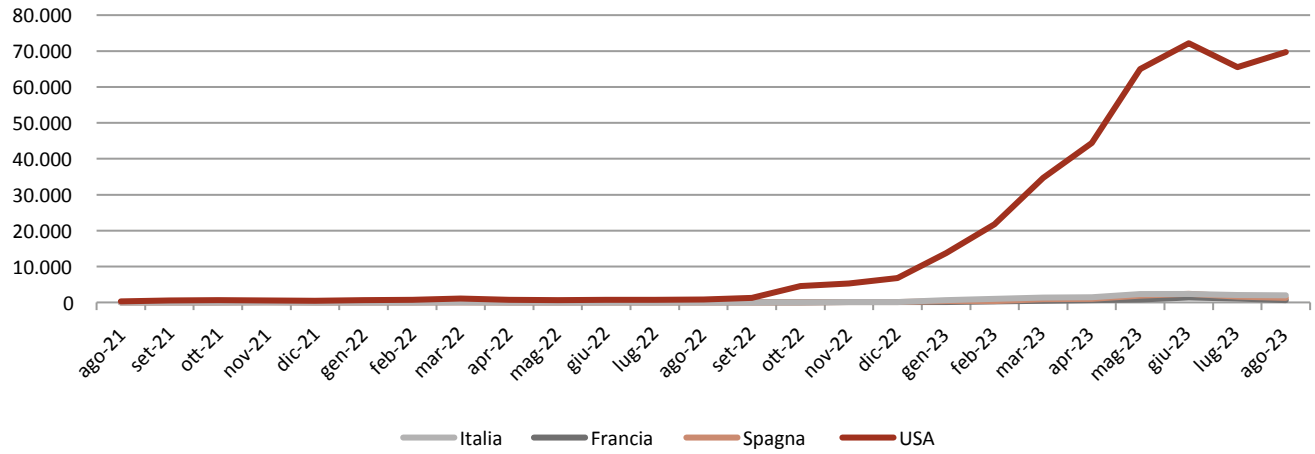
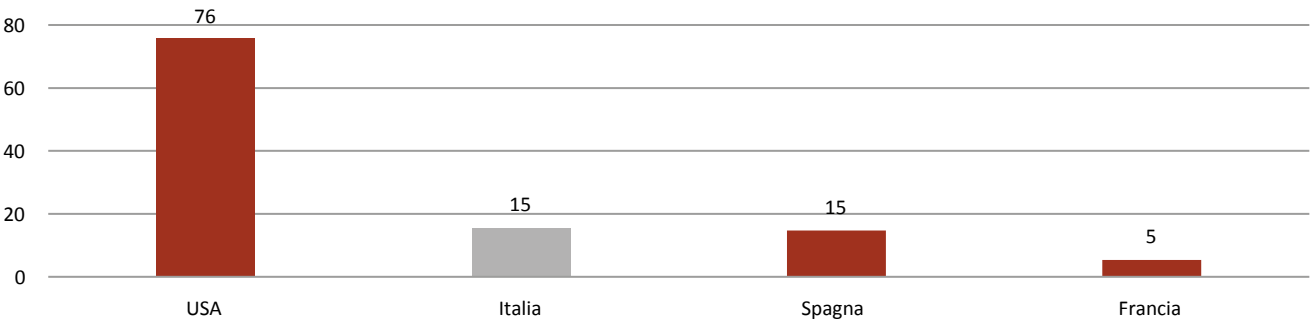


Fig. 2.20: Ricerche totali su "IA generativa" effettuate nel primo semestre 2023 per 100.000 abitanti

Fonte: elaborazioni I-Com su dati Bytek



applicazioni per modificare/creare contenuti di tipo testuale (Fig. 2.21).

Altro aspetto interessante che emerge dall'analisi delle ricerche effettuate sul web riguarda la **formazione**. In tutti i Paesi analizzati si nota a partire dal secondo trimestre 2022 un aumento delle ricerche online relative a corsi di formazione di vario tipo (inclusi quelli universitari) sull'IA (Fig. 2.22). Anche in questo caso, gli **Stati Uniti** guidano la classifica. Tuttavia, in termini relativi, anche la **Francia** mostra particolare interesse nei confronti della formazione in IA con 7 ricerche online ogni 100.000 abitanti collocati nella fascia d'età lavorativa (Fig. 2.23).

L'interesse nei confronti della formazione in IA è

Fig. 2.21: Ricerche sui principali utilizzi dell'IA, per Paese (%, primo semestre 2023)

Fonte: elaborazioni I-Com su dati Bytek

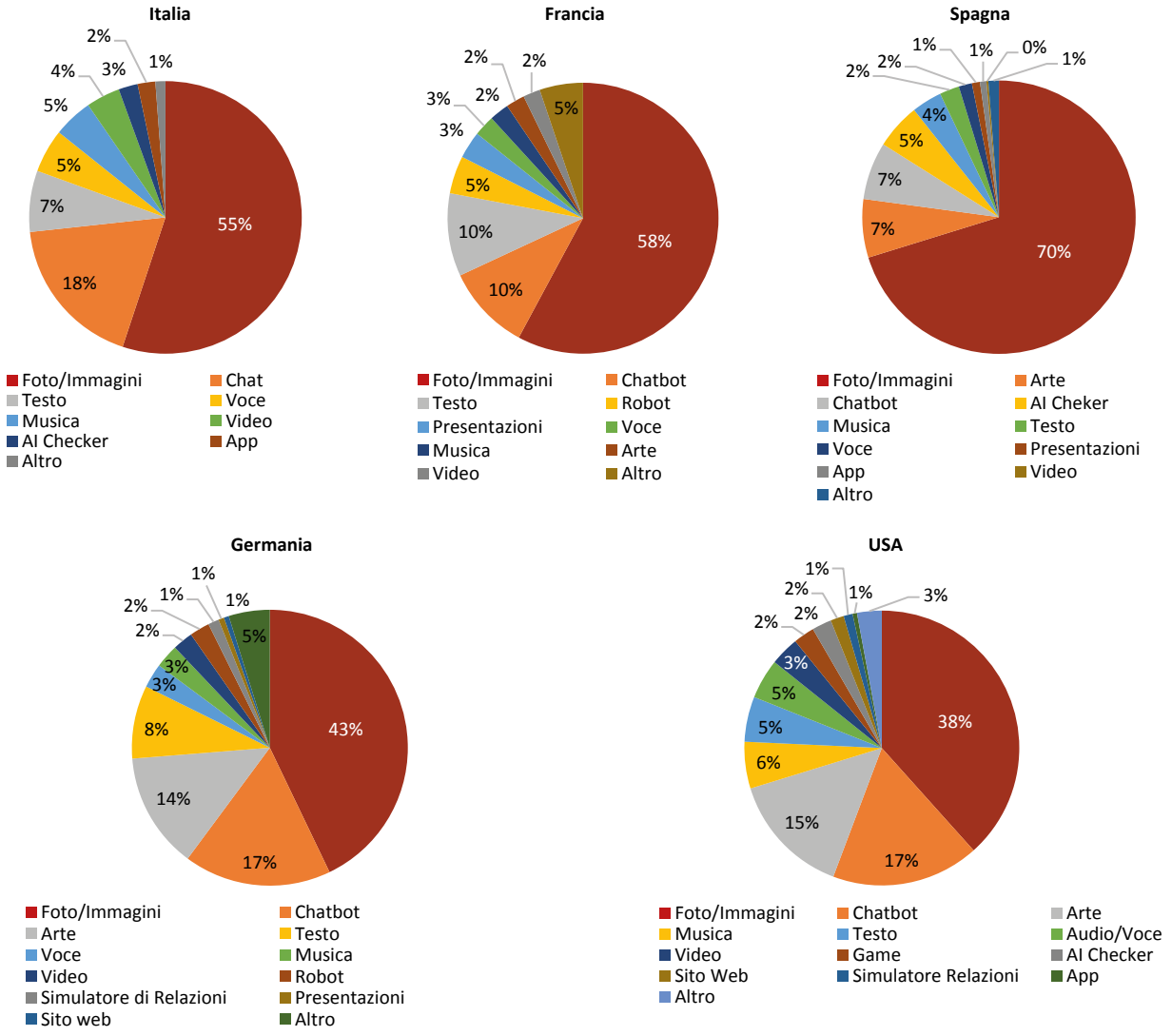


Fig. 2.22: Ricerche su corsi di formazione (universitari e non) su IA, per trimestre

Fonte: elaborazioni I-Com su dati Bytek

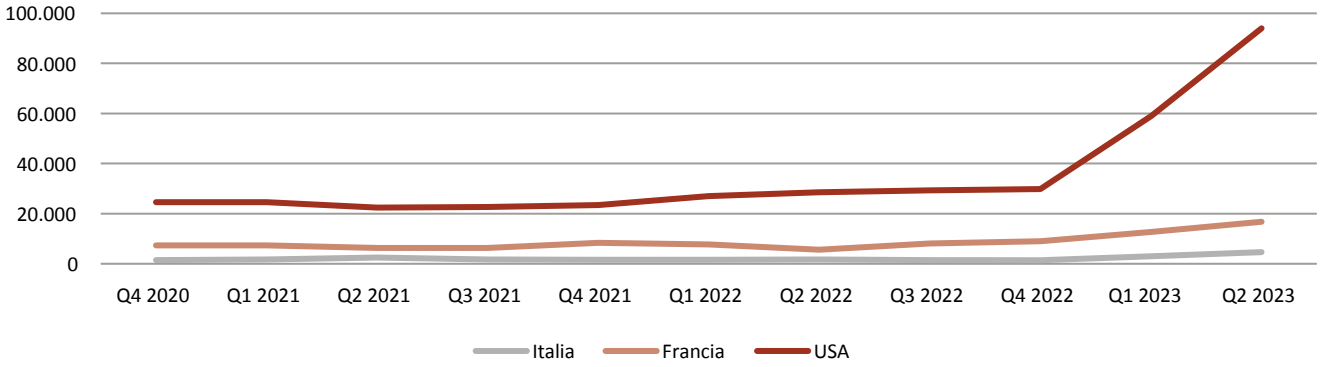
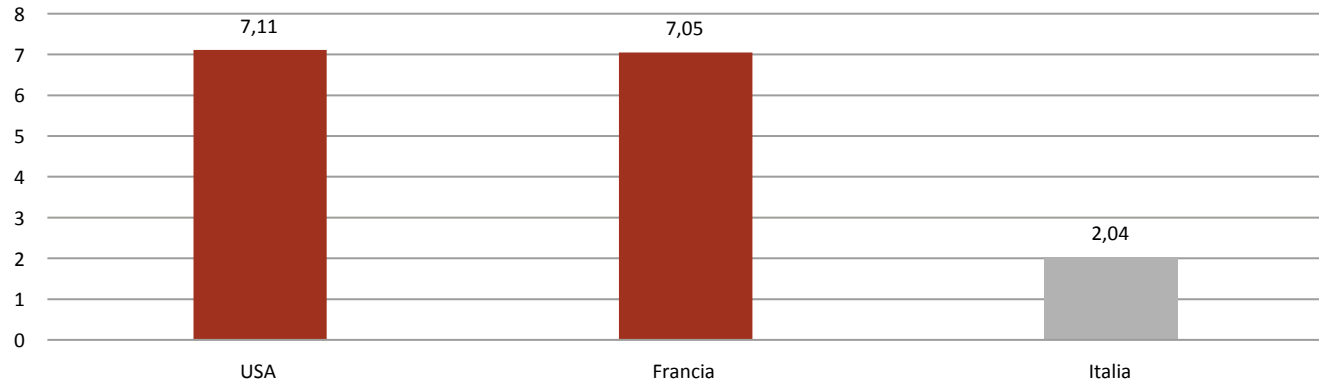


Fig. 2.23: Ricerche su corsi di formazione (universitari e non) su IA ogni 10.000 abitanti nella fascia d'età lavorativa (15-64 anni) – (primo semestre 2023)

Fonte: elaborazioni I-Com su dati Bytek

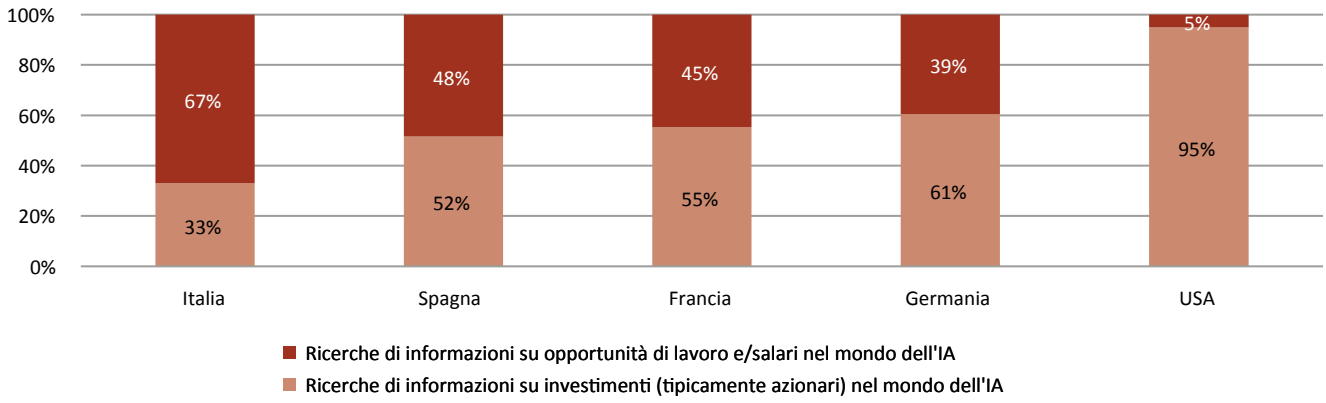


sicuramente correlato alle **opportunità** specie lavorative che questa nuova frontiera tecnologica può offrire (oltre alla necessità di dover adeguare le proprie competenze per non rimanere indietro). Il numero di ricerche online circa informazioni riguardanti le opportunità legate all'intelligenza artificiale è crescente in quasi tutti i Paesi analizzati. In particolare, in Italia, Spagna, Francia e Germania, la stragrande maggioranza delle ricerche relative alle opportunità IA riguarda appunto il mondo del lavoro, quindi **possibilità di impiego nel settore dell'IA**. Solo negli Stati Uniti, le ricerche si concentrano prevalentemente su informazioni relative ad **opportunità di investimento** nel settore dell'IA (Fig. 2.24). Il dibattito sull'intelligenza artificiale non si ferma però solo alle opportunità, ma analizza a fondo anche i **rischi** ad essa associati, che potrebbero essere alla base di un **sentimento di paura nei confronti delle tecnologie IA**.

Dall'analisi delle ricerche online in tema di intelligenza artificiale emerge che le ricerche correlate alla paura sono in aumento in tutti i Paesi analizzati, pur mantenendosi a un livello ancora piuttosto basso (Fig. 2.25). Ecco dunque che negli **Stati Uniti**,

Fig. 2.24: Ricerche relative alle opportunità correlate all'IA (%, primo semestre 2023)

Fonte: elaborazioni I-Com su dati Bytek



27 ricerche su 100.000 abitanti riguardano un sentimento di paura legato al fenomeno IA. Seguono la **Francia** e la **Spagna** con rispettivamente 20 ricerche correlate alla paura dell'IA ogni 100.000 abitanti. Mentre in **Italia** il numero di ricerche correlate alla paura si ferma a 17 ogni 100.000 abitanti (Fig. 2.26). Tuttavia, nel nostro Paese il 34% delle ricerche relative alla paura dell'IA riguarda il **rischio di perdere il posto di lavoro** a causa delle tecnologie intelligenti, una percentuale seconda solo a quella tedesca. Laddove in Francia e soprattutto negli Stati Uniti i timori riguardano nella stragrande maggioranza (rispettivamente, il 94% e il 96%) altri tipi di rischio, da quelli futuribili di estinzione a quelli legati a disinformazione, privacy e cybersecurity (Fig. 2.27).

Fig. 2.25: Ricerche relative ad un sentimento di paura verso l'IA, per trimestre

Fonte: elaborazioni I-Com su dati Bytek

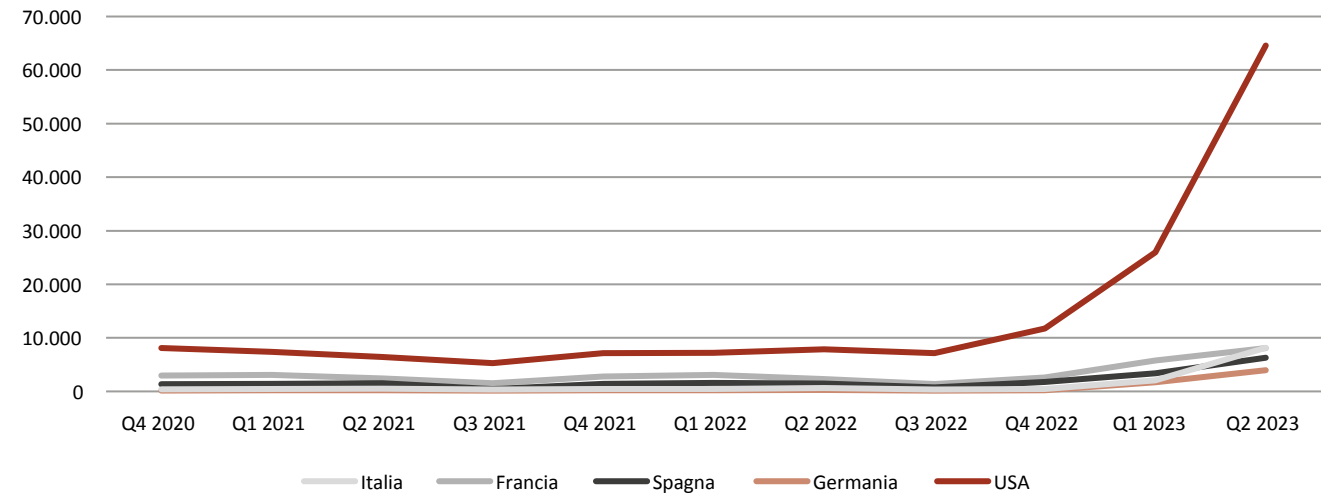


Fig. 2.26: Ricerche relative ad un sentimento di paura verso l'IA per 100.000 abitanti (primo semestre 2023)

Fonte: elaborazioni I-Com su dati Bytek

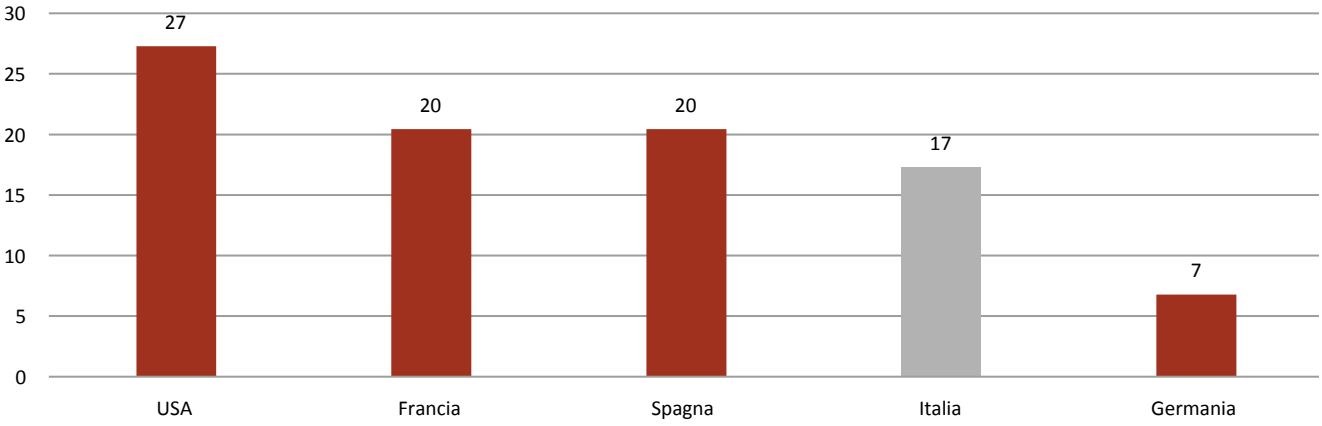
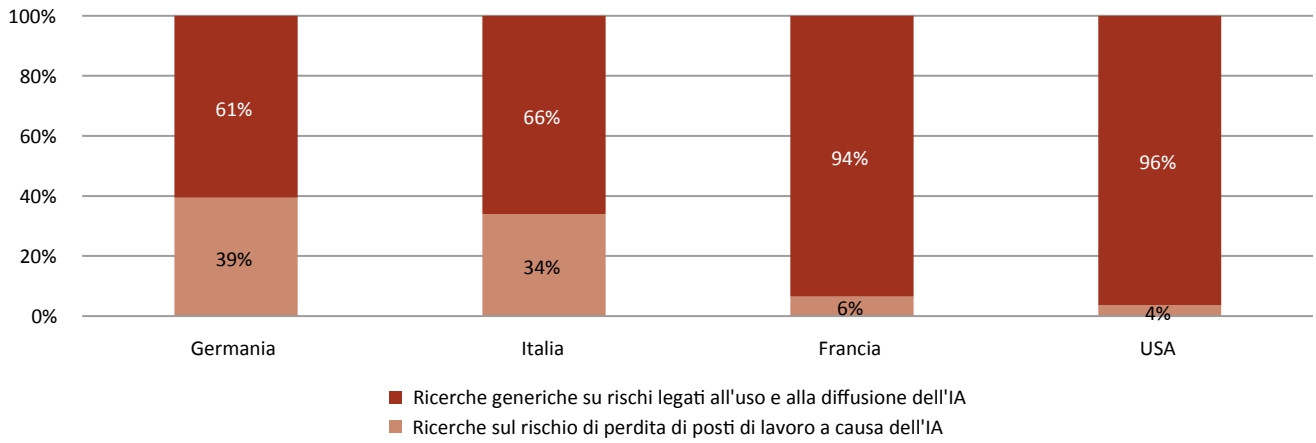


Fig. 2.27: Ricerche su rischi legati all'IA (%, primo semestre 2023)

Fonte: elaborazioni I-Com su dati Bytek



icom
istituto per la competitività

CAPITOLO 3

GLI SCENARI DEL FUTURO: IL METAVERSO

3.1. IL METAVERSO NELL'IMMAGINARIO DEGLI UENTI DEL WEB

Nel corso degli ultimi decenni, moltissime opere letterarie e cinematografiche hanno provato ad immaginare **come si integrerà l'innovazione digitale con la vita umana** in un futuro più o meno remoto, spesso ipotizzando un mondo virtuale in cui gli individui si troveranno a vivere **un'esistenza parallela e completamente immersiva**. Proprio in una di queste opere è stato coniato il termine metaverso, utilizzato per la prima volta nel 1992 dallo scrittore Neal Stephenson. Nonostante siano passati ormai più di trent'anni da quando tale parola ha fatto la sua prima apparizione, è interessante osservare come **non esista ad oggi non solo una definizione univoca**, ma neanche un'idea concettuale condivisa su cosa si indichi con tale accezione. L'attenzione su questo argomento è cresciuta sensibilmente da quando Facebook, nel 2021, ha cambiato la propria denominazione in Meta. Nonostante tale accelerazione, sebbene il metaverso sia generalmente ritenuto **una possibile evoluzione dell'attuale World Wide Web**, i suoi confini non appaiono bene definiti né agli occhi della maggioranza dei consumatori, né tantomeno agli stessi addetti ai lavori.

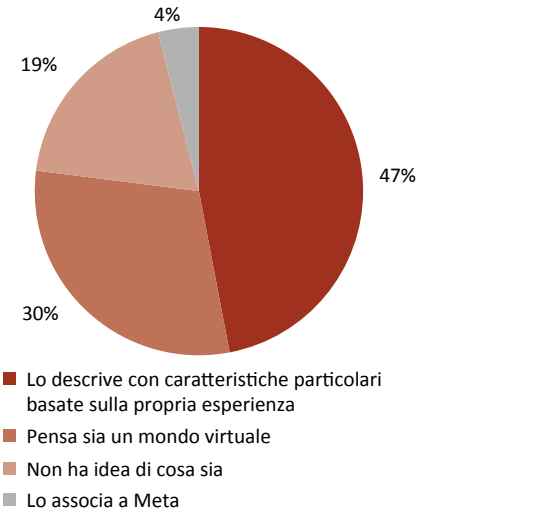
Per quanto concerne i primi, a febbraio 2022 McKinsey & Company ha intervistato oltre mille cittadini statunitensi (di età compresa tra i 13 e i 70 anni), realizzando una survey per comprendere quanto sia conosciuto e chiaro il concetto di metaverso (Fig. 3.1). Da questa analisi risulta come circa la metà dei rispondenti (47%) lo descriva con caratteristiche particolari basate sulla propria esperienza personale, fornendo inoltre molteplici definizioni. Tra tutte le descrizioni emerse, i principali punti in comune risultano le parole **"immersivo" e "interattivo"**. Un ulteriore 30%, probabilmente condizionato dalle già citate esperienze letterarie e cinematografiche, associa la parola metaverso ad un mondo virtuale, mentre circa il 19%, quindi appena uno su 5, non ha idea di cosa sia. Infine, il 4% degli intervistati associa il metaverso all'azienda Meta.

Come dimostrato da tale ricerca, l'incertezza su una definizione precisa di metaverso nasce anche dalle **esperienze personali degli utenti**, che spesso lo associano a piattaforme di social gaming (come Fortnite), a mondi digitali che si basano sulle criptovalute (come Decentraland) o ad un ecosistema di mondi virtuali tridimensionali che sfruttano la realtà virtuale (come Horizon di Meta).

A tal proposito, secondo un'analisi del portale Vincos, esistono oltre 40 ecosistemi che, ad oggi, vengono assimilati alla parola metaverso, peraltro con caratteristiche tecniche molto diverse tra loro (Fig. 3.2). Altrettanto spesso, il metaverso viene assimilato alla realtà virtuale e/o alla realtà aumentata. Tuttavia, è importante osservare come l'essere dotati di device AR o VR non costituisca un prerequisito fondamentale per accedere al metaverso, il quale è fruibile tramite un'ampia gamma di altri dispositivi, come PC, smartphone e console per videogiochi.

Fig. 3.1: Come descrivono il metaverso i consumatori americani (%, 2022)

Fonte: McKinsey & Company, 2022



In generale, è possibile identificare una serie di caratteristiche fondamentali comuni a tutti gli ecosistemi digitali che vengono accomunati al metaverso:

- l'essere immersivi;
- fornire interattività in tempo reale;
- consentire l'interazione con altri utenti;
- garantire un certo grado di interoperabilità tra piattaforme e dispositivi.

D'altro canto, se il concetto di metaverso appare ancora piuttosto astratto, i consumatori sembrano avere già un'idea chiara di quali potrebbero essere **i principali benefici** della prossima evoluzione del web. Da una survey effettuata da Tidio intervistando 1.050 utenti di internet a livello globale, è emerso come **il 39% dei rispondenti ritiene che nel metaverso potranno fare esperienze altrimenti irrealizzabili nel mondo reale**, mentre il 37% crede che si potrà girare il mondo senza muoversi, nonché migliorare la creatività e immaginazione (Fig. 3.3). Oltre il 30% degli intervistati ritiene inoltre che il metaverso possa migliorare l'alfabetizzazione tecnologica (34%) e creare nuove opportunità lavorative (30%). In generale, tutte le risposte citate dagli utenti lasciano intravedere l'aspettativa di un'esperienza di utilizzo, probabilmente anche collegata alla realtà virtuale, estremamente più immersiva rispetto a quella offerta dal web attuale.

Nel complesso, tuttavia, le principali ragioni per entrare nel metaverso da parte dei consumatori fanno pensare che **questo non venga percepito semplicemente come uno spazio destinato a fini ludici**, bensì anche come **un'opportunità professionale e di investimento**. Lo studio di Tidio citato in precedenza indica come la motivazione prioritaria per entrare nel metaverso (Fig. 3.4) sia costituita dalle **opportunità di lavoro** che potrebbero scaturire da questo nuovo ecosistema (52%), seguite al terzo posto da investimenti in NFT e criptovalute (44%) e al quarto dalla "Formazione Scolastica", selezionata da ben il 40% dei rispondenti.

Fig. 3.2: La mappa dei "metaversi" (2022)

Fonte: Vincos, 2022

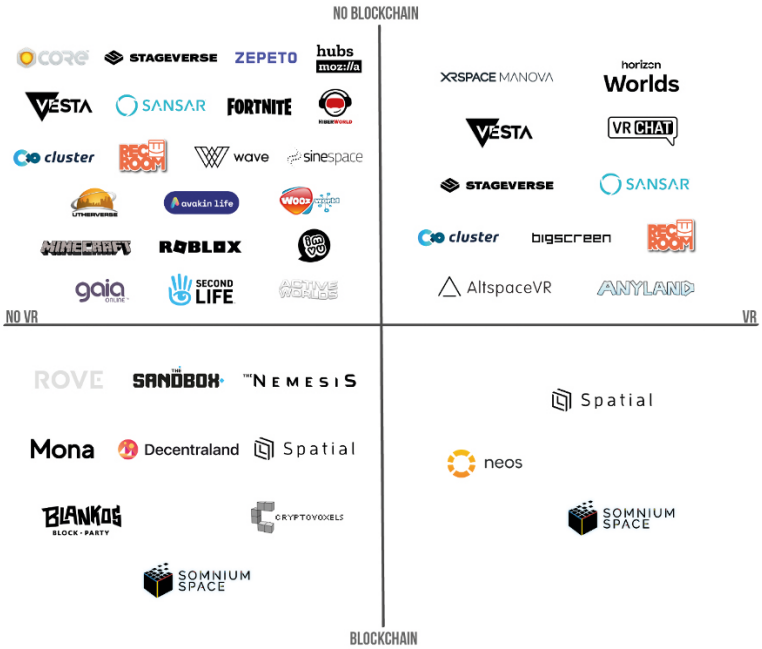


Fig. 3.3: Principali benefici del metaverso secondo i consumatori (%, 2021)

Fonte: Tidio, 2021

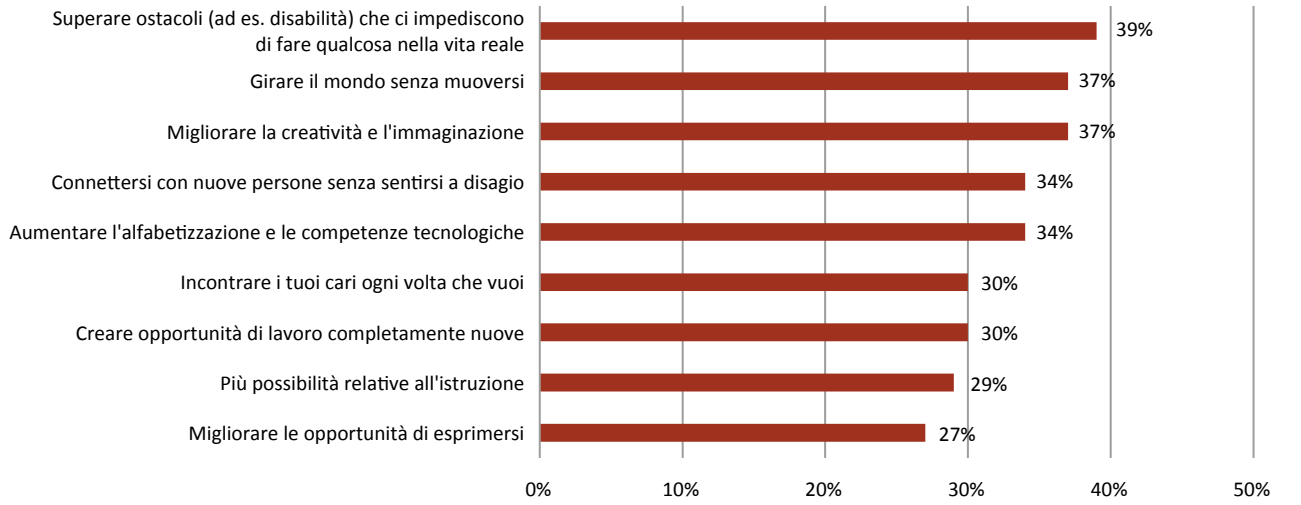
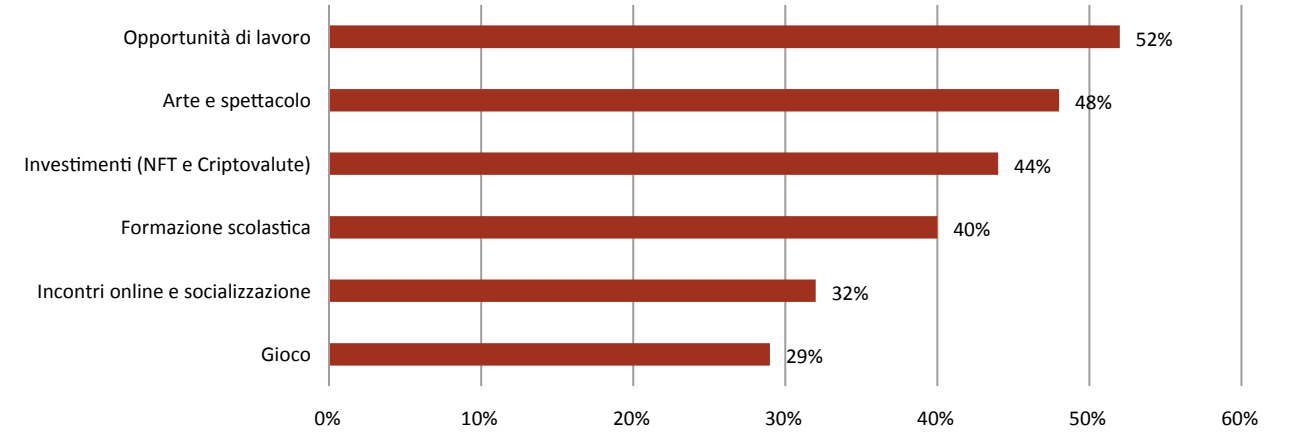


Fig. 3.4: Principali ragioni per entrare nel metaverso secondo gli utilizzatori di internet (%, 2021)

Fonte: Tidio, 2021



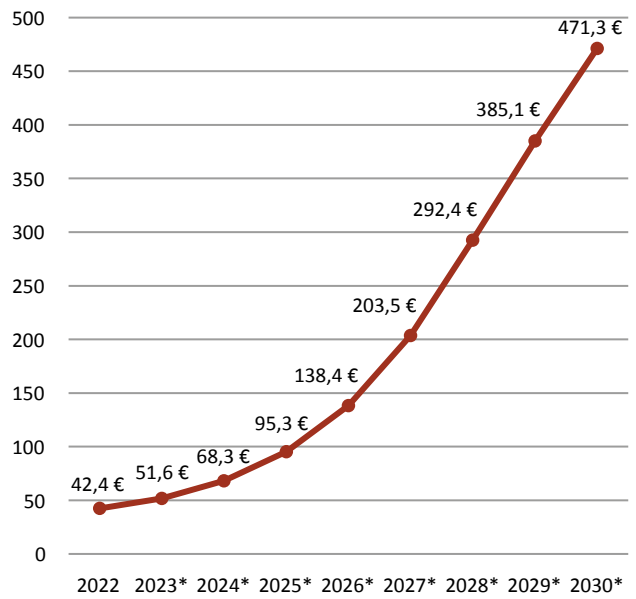
Infine, appare opportuno sottolineare **la differenza tra il metaverso e il c.d. Web3**, con cui spesso viene (più o meno sensatamente) accomunato. In concreto, più che ad un cambiamento dell'esperienza di utilizzo del web così come lo conosciamo, **il Web3 si riferisce ad un cambio di paradigma verso un ecosistema sempre più decentrato** e gestito prevalentemente (o esclusivamente) dagli utenti e non più dalle grandi piattaforme. Nato dalla cultura legata alle criptovalute e alla blockchain che si è largamente diffusa negli ultimi anni, il Web3 sta trovando una sua collocazione anche nel metaverso (es. Decentraland), costituendone uno dei (molteplici) rami di sviluppo.

3.2. IL MERCATO DEL METAVERSO: L'UE NEL CONTESTO GLOBALE

Nonostante rappresenti ancora un concetto piuttosto astratto sia per i consumatori che per le imprese, il metaverso (pur nei differenti perimetri che gli vengono attribuiti) sembra avere già una dimensione economica di rilievo: secondo le previsioni di mercato diffuse ad agosto 2023 da Statista, **il metaverso presenta ad oggi ricavi a livello globale pari a €42,4 miliardi**, che potrebbero diventare €471,3 entro la fine del decennio (Fig. 3.5). È importante osservare come l'analisi condotta da Statista tenga in considerazione i ricavi generati dagli acquisti in-app, dalla spesa pubblicitaria e dalla spesa dei consumatori per app, giochi, oggetti, prodotti e hardware (come cuffie o visori).

Fig. 3.5: Ricavi del metaverso a livello globale (€ miliardi)

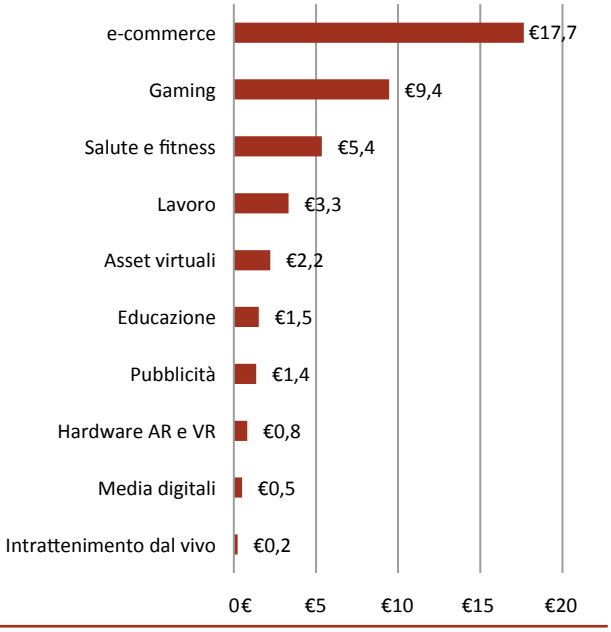
Fonte: Statista Market Insights
*Dati previsionali



Entrando nel dettaglio della composizione dei ricavi vediamo come nel 2022 il segmento che ha fatto registrare la quota maggioritaria a livello globale sia **l'e-Commerce, con €17,7 miliardi** (Fig. 3.6). Nella sezione commercio digitale ricadono tutti i beni e servizi che sono stati venduti sulle piattaforme assimilate al metaverso. Al secondo posto per volume di ricavi generati in ambito metaverso si trova il **gaming** (€9,44 miliardi), comparto che sta assumendo sempre più importanza negli ultimi anni all'interno del mercato digitale e che potrebbe vivere una vera e propria rivoluzione grazie al metaverso. Secondo lo stesso Statista[16], **nel 2022 il numero globale di videogiocatori ha raggiunto la considerevole cifra di €2,7 miliardi, che dovrebbero diventare €3,1 miliardi entro il 2030**.
A conferma di quanto detto in precedenza rispetto all'interesse non esclusivamente ludico dei

Fig. 3.6: Ricavi del metaverso a livello globale per segmento di mercato (€ miliardi, 2022)

Fonte: Statista Market Insights



16 Statista Advertising & Media Insights, Agosto 2023

consumatori verso il metaverso, **i comparti lavoro e educazione lo scorso anno hanno fatto registrare ricavi rispettivamente per €3,3 e €2,5 miliardi a livello globale**.

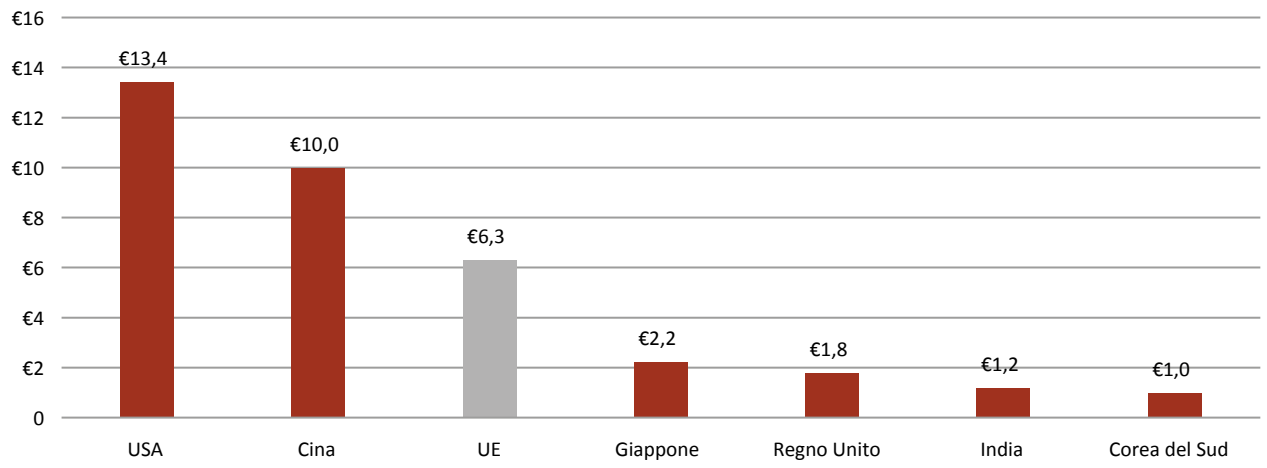
Altro tema interessante che vale la pena di approfondire è quello della scomposizione geografica dei ricavi generati dal metaverso. Sotto questo aspetto, come facilmente presumibile, a primeggiare sono gli USA che hanno sperimentato nel 2022 un giro d'affari pari a €13,4 miliardi, il 32% del totale globale, seguiti a stretto giro dalla Cina con €10miliardi. Sebbene si posizioni al terzo posto a livello globale, l'Unione Europea appare notevolmente indietro rispetto alle due economie che la precedono con soli €6,3 miliardi di ricavi (Fig. 3.7).

Come già anticipato, tra le tecnologie che permetteranno ai consumatori di vivere a pieno l'esperienza immersiva del metaverso ci sono certamente la **realtà virtuale e la realtà aumentata**.

La correlazione tra questi mondi appare chiarissima soprattutto guardando le previsioni di mercato collegate alla diffusione di questi device. Secondo Statista, nei prossimi anni **i ricavi dell'AR e della VR a livello globale potrebbero vedere una netta impennata, passando dai €23,9 miliardi del 2022 a quota €49,9 miliardi nel 2026** (Fig. 3.8). Tra le due tecnologie, quella che allo stato attuale sta riscuotendo il maggior successo è la realtà aumentata, che nel 2022 ha generato ricavi per €14,3 miliardi, previsti in crescita fino a superare i €30 miliardi entro il 2027. Questo è probabilmente dovuto al fatto che, ad oggi, gli use case della realtà virtuale nelle aziende sono ancora relativamente pochi, mentre **la AR sta sperimentando già da alcuni anni uno sviluppo consistente a livello industriale.** Già nel 2017 uno studio condotto da Statista ha documentato l'utilizzo della realtà aumentata da parte di grandi player manifatturieri statunitensi come Lockheed Martin e Caterpillar. Nel primo caso gli ingegneri indossano occhiali AR dotati di telecamere, profondità e sensori di movimento per ottenere immagini in tempo reale degli aerei; questo permette loro di avere a disposizione immagini di tutte le componenti del veicolo oltre che le istruzioni su come assemblarle. In Caterpillar invece la realtà aumentata consente ai tecnici di accedere a dati e immagini in tempo reale mentre eseguono le riparazioni dei macchinari; inoltre, l'azienda ha sviluppato un servizio denominato CAT LIVESHARE che consente

Fig. 3.7: Ricavi del metaverso per area geografica (€ miliardi, 2022)

Fonte: Statista Market Insights



ai meccanici di CAT, grazie all'utilizzo di device AR, di ricevere video istruzioni sulle riparazioni in tempo reale direttamente dall'azienda.

Parimenti a quanto visto per il metaverso, **il mercato principale a livello globale per AR e VR è quello statunitense** che nel 2022 ha generato ricavi per €6,7 miliardi, seguito dalla Cina con €5,2 miliardi. L'Europa si posiziona, ancora una volta, al terzo posto con €4,4 miliardi di ricavi generati nel corso del 2022 (Fig. 3.9).

Fig. 3.8: Ricavi di AR e VR a livello globale (€ miliardi)

Fonte: Statista Market Insights
*Dati previsionali

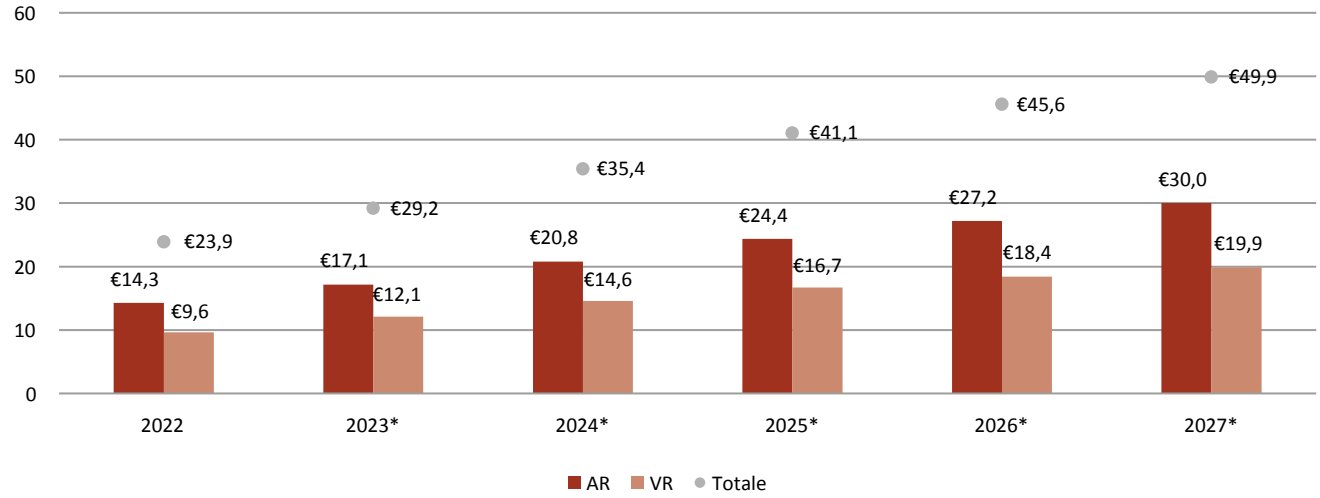
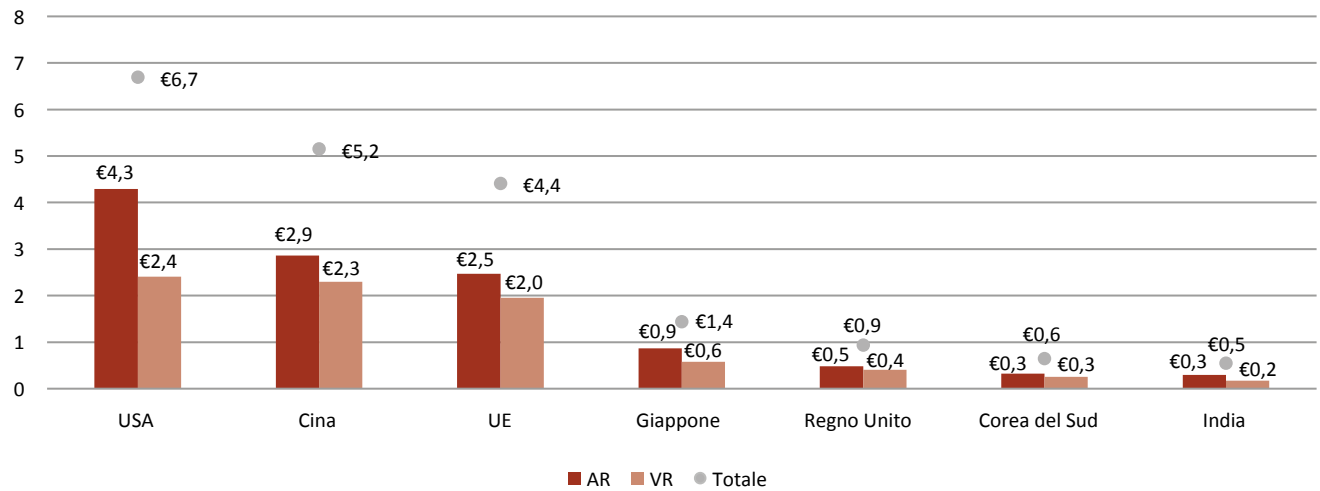


Fig. 3.9: Ricavi di AR-VR per area geografica (€ miliardi, 2022)

Fonte: Statista Market Insights



3.3. IL MERCATO ITALIANO DEL METAVERSO

Nel paragrafo precedente è stato approfondito l'andamento del mercato del metaverso a livello globale e il ruolo che l'UE sta giocando in questa partita. Appare però altrettanto interessante analizzare lo scenario interno all'Unione e, in particolare, **come performa l'Italia rispetto alle altre principali economie del vecchio continente** in quest'ambito. Osservando i dati sui ricavi in valori assoluti, emerge chiaramente la prevalenza del mercato tedesco che ha generato nel 2022 un giro d'affari pari a €1,68 miliardi (Fig. 3.10), seguito da quello francese (€1,87 miliardi) e da quello italiano (€752 milioni). Ponderando i ricavi generati al PIL nazionale vediamo però come la situazione cambi notevolmente, infatti, **il Paese che fa registrare il maggior impatto dei ricavi del metaverso sull'economia nazionale è la Francia (€450 mila euro per miliardo di PIL)**, seguita dalla Germania (€433 mila) e dalla Spagna (€405 mila). **L'Italia chiude il gruppo dei paesi considerati con €386 mila di ricavi generati per miliardo di PIL**, mostrando quindi un evidente ritardo rispetto alle altre principali economie UE.

Focalizzando l'attenzione sul mercato italiano vediamo che, sebbene la gerarchia dei settori che hanno generato più ricavi nel 2022 nel metaverso ricalchi quanto visto a livello globale, con il **primato dell'eCommerce,** nella penisola **il peso di questo comparto sul totale si ferma al 27,3%** facendo trasparire un **maggior equilibrio** rispetto al 41,6% emerso a livello mondo (Fig. 3.11). Di converso, **finalità non ludiche come lavoro ed educazione attirano nel panorama italiano una quota di ricavi pari al 10,1% e al 4%,** quindi ampiamente maggiore di quanto è possibile riscontrare a livello globale (rispettivamente 7,8% e 3,6%).

Passando all'analisi del mercato della realtà virtuale e di quella aumentata, è possibile notare come anche in questo caso **l'Italia si posiziona al terzo posto**

Fig. 3.10: Ricavi del metaverso delle principali economie UE in valori assoluti e in relazione al PIL nazionale (€ milioni, 2022)

Fonte: elaborazioni I-Com su dati Statista Market Insights ed Eurostat

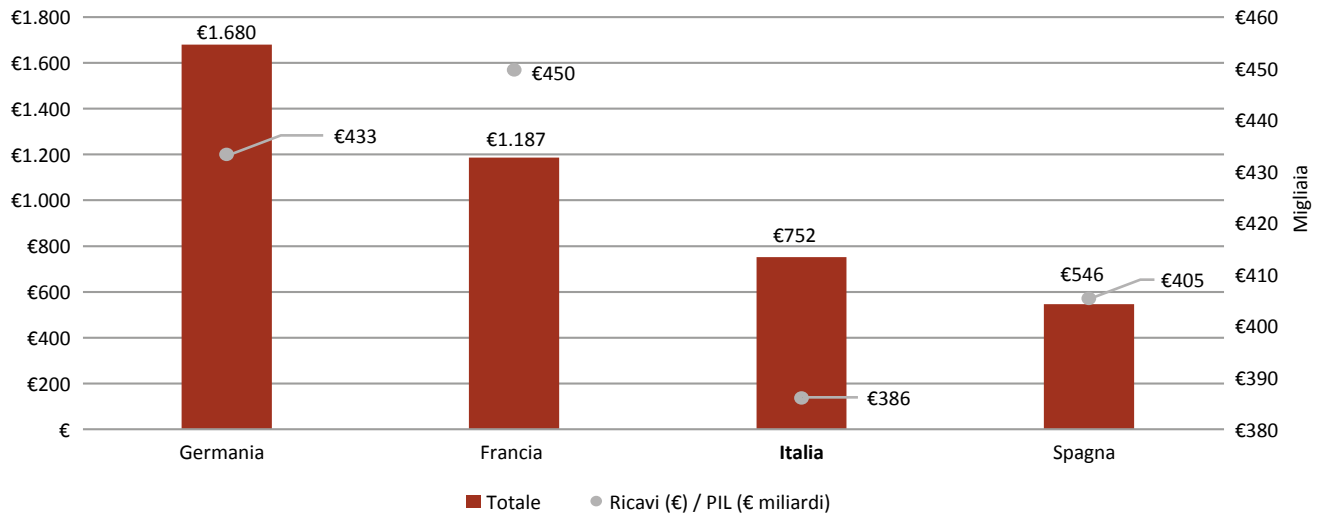
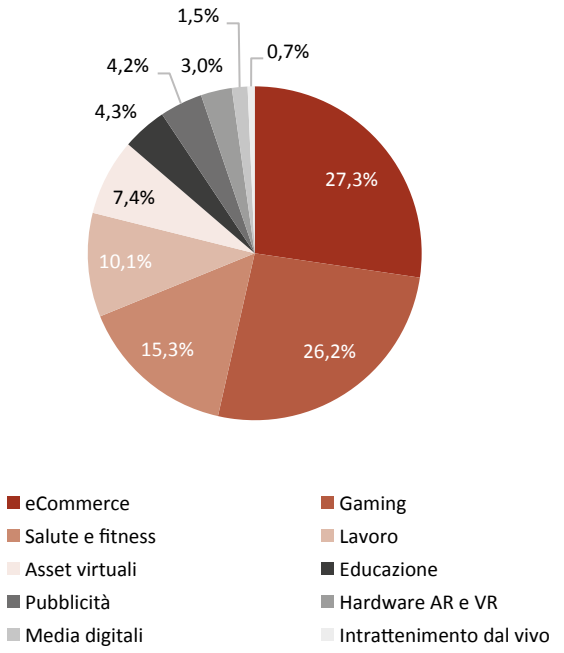


Fig. 3.11: Ricavi del metaverso in Italia per segmento di mercato (%, 2022)

Fonte: Statista Market Insights



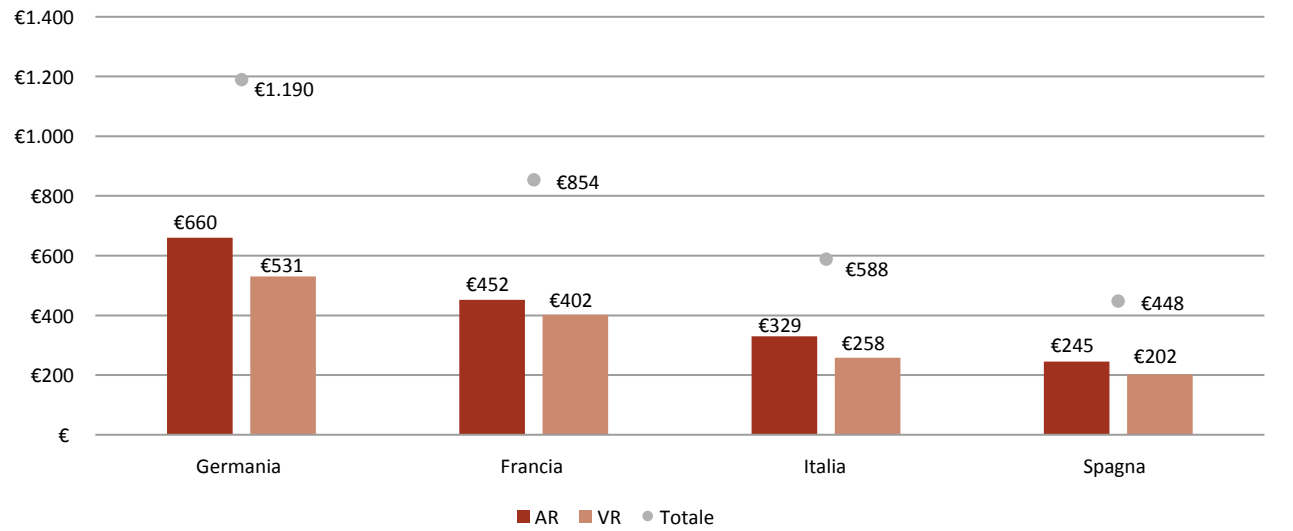
tra le principali economie UE in termini di ricavi realizzati nel 2022, con €588 milioni (Fig. 3.12). Osservando la scomposizione tra le due tecnologie, i valori riscontrati nella penisola ricalcano lo scenario globale con una, seppur lieve, prevalenza della VR, che lo scorso hanno ha generato un volume d'affari pari a €329 milioni.

3.4. LE NUOVE OPPORTUNITÀ PER LE IMPRESE NEL METAVERSO

Se le stime riportate evidenziano un notevole potenziale economico del metaverso per gli sviluppi futuri della filiera tech, è altrettanto evidente come una trasformazione così radicale del world wide web possa produrre effetti su una molteplicità di settori industriali. Una stima pubblicata da McKinsey a giugno 2022 prevede che **nel 2030 il metaverso potrebbe avere un impatto sull'economia globale fino a $5 trilioni**, interessando in particolare l'e-commerce (fino a $2,6 trilioni entro il 2030), la formazione (tra i

Fig. 3.12: Ricavi di AR e VR in Italia rispetto alle altre principali economie UE (€ milioni, 2022)

Fonte: Statista Market Insights



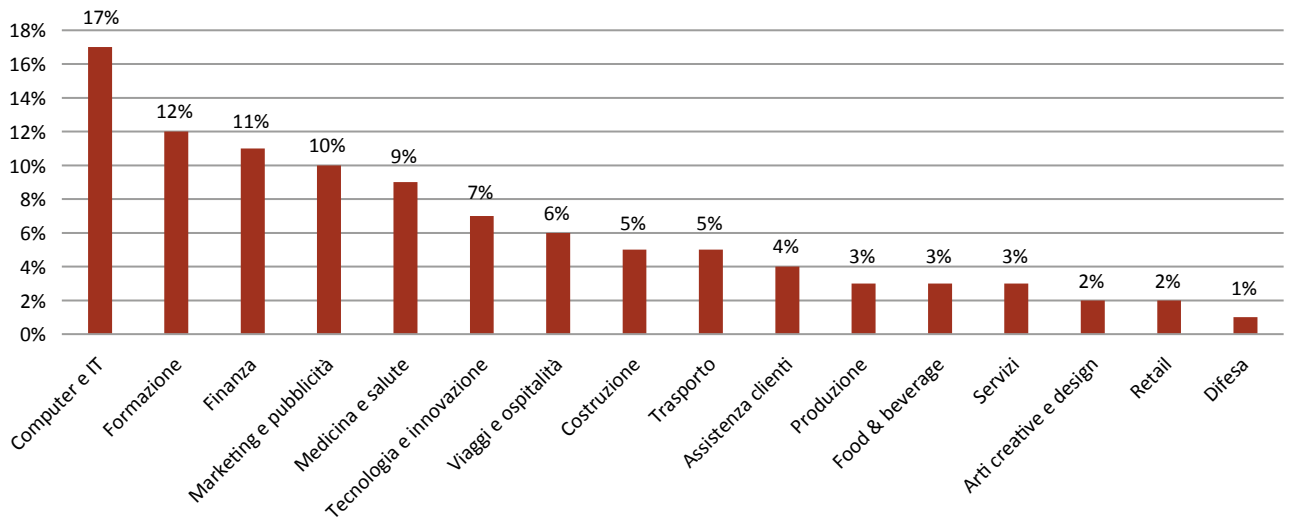
$180 miliardi e i $270 miliardi), la pubblicità (da $144 a $206 miliardi) e i giochi (da $108 a $125 miliardi).
Anche un sondaggio condotto a livello mondiale da Sortlist (aprile 2022) intervistando esponenti di 200 imprese provenienti da sei paesi (UK, Francia, Belgio, Germania, Spagna e USA) che già stanno investendo nel metaverso, mostra come il nuovo framework possa impattare su un numero piuttosto esteso di settori: **tra le aziende che hanno già investito nel metaverso solo il 17% appartiene al settore "computer e IT"**, mentre risultano attivi operatori di altri 14 comparti, tra i quali anche operatori finanziari, del settore medico, delle costruzioni, dei trasporti, del food&beverage e della difesa (Fig. 3.13).
A tal proposito, uno studio condotto da McKinsey dal titolo "Value creation in the metaverse" ha analizzato alcuni casi d'uso del metaverso per diversi settori industriali tradizionali, tra cui abbigliamento, moda e lusso; servizi finanziari e retail. In particolare, gli *use cases* individuati da McKinsey appartengono a quattro tipologie:

- **nuovi modelli di business** che permettono all'azienda di penetrare altri mercati (ad esempio i rivenditori che utilizzano il metaverso per guidare la vendita di prodotti fisici);
- operazioni che **migliorano la produttività e la collaborazione** a costi inferiori (ad esempio un'efficiente rete digitale di data center in più sedi contemporaneamente);
- **attività di branding**, marketing e user experience più coinvolgenti (ad esempio le organizzazioni che creano filiali nel metaverso offrendo una nuova visione del proprio marchio);
- **nuovi prodotti e servizi** (ad esempio prodotti completamente personalizzati utilizzabili in realtà mista).

Relativamente al **comparto moda**, uno degli esempi più interessanti di come il metaverso possa far evolvere il settore è costituito dalla "Metaverse Fashion Week" realizzata su Decentraland nel marzo 2022. Questo evento virtuale ha ricevuto una grandissima risonanza tra le imprese, tanto da richiamare brand del calibro di Dolce & Gabbana, Estée Lauder ed Etro.

Fig. 3.13: Principali settori industriali a livello mondiale che hanno già investito nel metaverso (%, 2022)

Fonte: Sortlist, 2022



Nel dettaglio, l'esperienza permetteva di acquistare capi virtuali come NFT e di indossarli digitalmente.
In generale, il metaverso può rappresentare per questo comparto un'opportunità completamente nuova, con ricadute positive anche sul business tradizionale dell'impresa. Ad esempio, la casa di moda Balenciaga ha lanciato contemporaneamente una collezione fisica e una linea di abbigliamento virtuale sul videogioco Fortnite, ottenendo un incremento di oltre il 40% delle ricerche online del proprio marchio già due giorni dopo il lancio.
Per quanto concerne il settore dei **servizi finanziari**, da anni tra i più digitalizzati, il fenomeno dello spostamento delle attività dalle filiali fisiche ai canali digitali costituisce già una realtà piuttosto consolidata. Per tali ragioni, il metaverso potrebbe costituire un'ulteriore opportunità di business per le istituzioni finanziarie che, ad esempio, avessero intenzioni di creare nuove filiali e/o servizi digitali in questo nuovo ecosistema. Esempi interessanti in tal senso sono rappresentati dalla fintech londinese Sokin, che sta costruendo un'infrastruttura per l'elaborazione di pagamenti, transazioni e investimenti nel metaverso, dalla Neobank Zelf, che sta lanciando servizi bancari incorporati per videogiocatori, e dalla società tecnologica nordamericana TerraZero, che sta lavorando al finanziamento di immobili virtuali nel metaverso.
Anche il **comparto retail**, dopo l'avanzata dell'e-commerce favorito anche dalla crisi del Covid, potrebbe costituire un ambito privilegiato per lo sviluppo di servizi nel metaverso. Ad esempio, device RV possono replicare l'esperienza di acquisto del negozio fisico in uno spazio 3D virtuale e navigabile, una direzione già intrapresa da Dyson con il lancio di un negozio digitale (accessibile tramite VR) che consente ai clienti di "camminare" e testare virtualmente i suoi prodotti. Parallelamente, diversi rivenditori di mobili statunitensi come Crate & Barrel, Walmart, West Elm e Wayfair

Tab. 3.1: Iniziative nel metaverso implementate fino a giugno 2022 dalle imprese per settore (%)

Fonte: McKinsey & Company, 2022

	Campagne o iniziative di marketing	Formazione dei dipendenti	Meeting nel metaverso	Eventi o conferenze	Progettazione di prodotti o digital twins	Reclutamento o onboarding di nuovi dipendenti	Acquisti dei clienti con cryptovalute
Tecnologia	68	64	54	64	54	39	23
Media e telco	82	36	36	43	54	18	25
Industria avanzata	64	55	36	64	64	36	9
Finanza e assicurazioni	67	63	56	49	56	25	31
Retail e fashion	95	56	59	41	50	41	14
Energia e minerali	54	85	69	46	69	31	8
Salute e settore pubblico	10	59	79	72	59	38	34
Turismo, trasporti e logistica	56	78	56	78	56	44	22
Totale	67	63	53	52	52	31	22

Livello di adozione

			Basso (<40%)	Medio (40%-70%)	Alto (<70%)		

stanno collaborando con Pinterest per utilizzare la realtà aumentata allo scopo di mostrare ai consumatori come appariranno i mobili nei loro salotti. Samsung ha lanciato un negozio virtuale in Decentraland, modellato su uno dei suoi negozi fisici di New York City, dove i clienti possono sia acquistare prodotti che completare missioni per guadagnare NFT.

Complessivamente, dal citato studio di McKinsey su 258 executive provenienti da imprese nordamericane, europee e asiatiche, è emerso come **la maggior parte delle iniziative sul metaverso sia incentrata su campagne di marketing, formazione dei dipendenti, meeting e eventi** (Tab. 3.1). Per ulteriori sviluppi industriali, è verosimile che occorrerà attendere ancora qualche anno.

La portata rivoluzionaria del metaverso in ambito business emerge chiaramente anche dal crescente interesse delle aziende in questo nuovo ecosistema. Secondo un'indagine condotta da Sortlist intervistando esponenti di 200 imprese provenienti da sei paesi (UK, Francia, Belgio, Germania, Spagna e USA) che già stanno investendo nel metaverso, è emerso come **nel 17% dei casi questa rappresenti la priorità aziendale**. In generale, **il 73% delle imprese rispondenti destinerà al metaverso oltre il 10% del proprio budget in marketing/innovazione** (Fig. 3.14).

Tra i progetti che le aziende intervistate intendono portare avanti in futuro (Fig. 3.15) risultano **al primo posto le criptovalute (53%),** seguite a breve distanza dagli NFT (Non Fungible Token, 44%). Questo dato segnala come anche nel metaverso ci sia ampio spazio per il paradigma del Web3 già menzionato nel primo paragrafo di questo capitolo.

Il 40% dei rispondenti sembra intenzionato a sfruttare gli spazi virtuali del metaverso per permettere ai propri dipendenti di lavorare a distanza, mentre il 30% sembra orientato a investire nel marketing e nel posizionamento della propria impresa. Rilevante appare anche la componente ludica, con il 26% delle aziende che intende investire nel gaming e il 15% che punta sull'intrattenimento e sulla creazione di un mondo virtuale.

D'altro canto, nonostante la rilevante crescita di mercato prevista per i prossimi anni, anche le aziende che già investono nel metaverso presentano alcune perplessità relative a questa innovazione, tra le quali la principale riguarda **la cybersecurity** (Fig. 3.16). Il numero di aziende preda di attacchi informatici è cresciuto in maniera vertiginosa negli ultimi anni ed è certamente ipotizzabile che il metaverso non ne sarà immune, soprattutto nelle prime fasi. Da ciò appare certamente

Fig. 3.14: Priorità di investimento delle compagnie che già investono nel metaverso (%, 2022)

Fonte: Sortlist, 2022

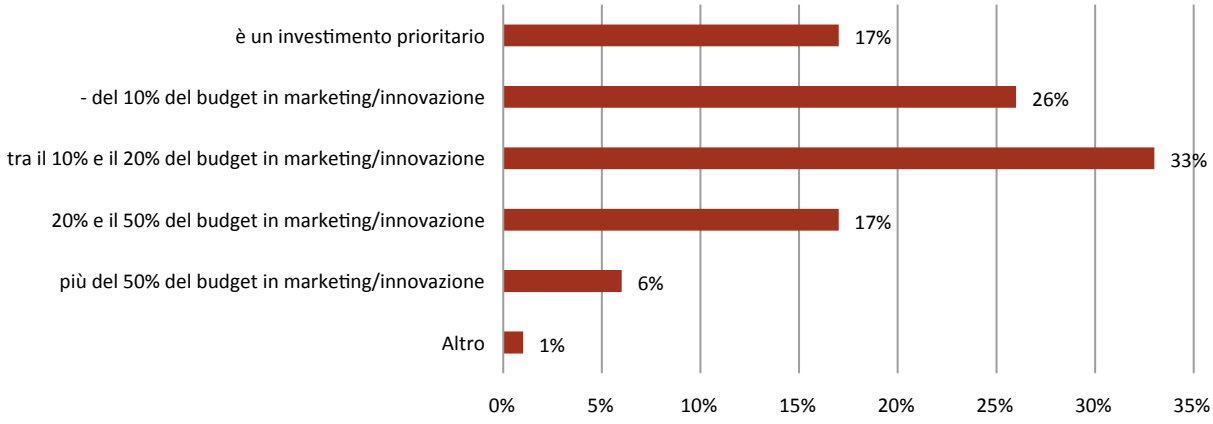
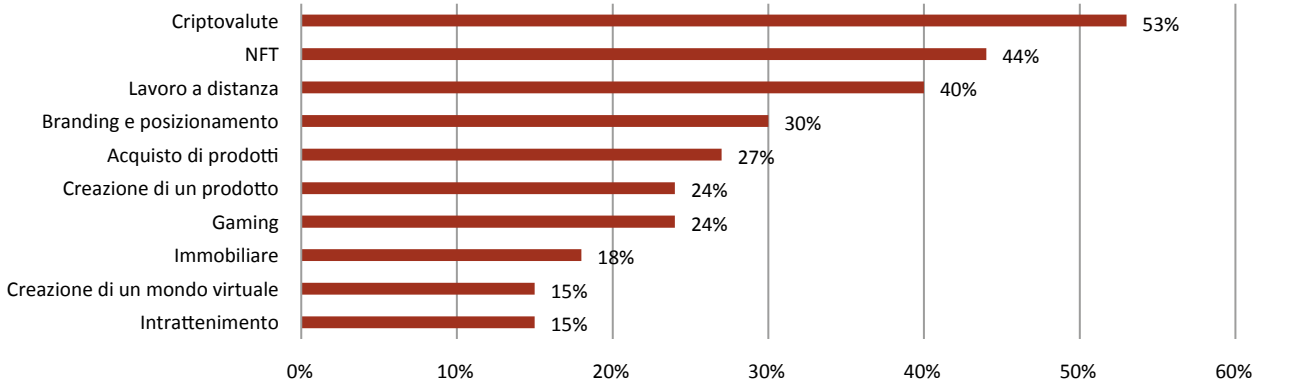


Fig. 3.15: Tipologie di progetti in cui le aziende hanno intenzione di investire nel metaverso (%, 2022)

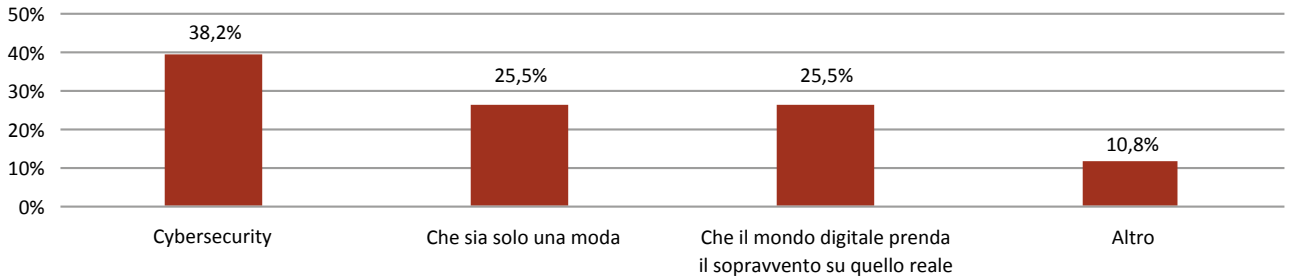
Fonte: Sortlist, 2022



comprensibile come **la cibersicurezza sia la preoccupazione più rilevante per il 38,2% delle imprese attive in quest'ambito**. Altre perplessità, che curiosamente denotano timori opposti – a riprova dell'incertezza che allo stato attuale riguarda le possibili evoluzioni del nuovo framework tecnologico – sono relative da un lato al rischio che il metaverso non riesca ad affermarsi, rappresentando solo una moda passeggera (25,5%), e dall'altro, paradossalmente, che questo possa addirittura arrivare a prevalere sul mondo reale (25,5%).
A prescindere dai dubbi riscontrati, appare verosimile che i tempi necessari per una diffusione consistente del metaverso siano ancora relativamente lunghi: p**er il 67,7% delle aziende intervistate da Sortilist, il metaverso potrebbe raggiungere il proprio picco di diffusione solo nei prossimi 5 anni** (Fig. 3.17). La tesi che questa nuova evoluzione del web necessiti ancora di tempo per arrivare a maturità trova conferma nella notizia, pubblicata lo scorso ottobre dal Wall Street Journal[17], della revisione al ribasso da parte di Meta delle stime sulla crescita di utenti di Horizon World., da 500 mila a 280 mila entro la fine del 2022[18].

Fig. 3.16: Principali timori relativi al metaverso (%, 2022)

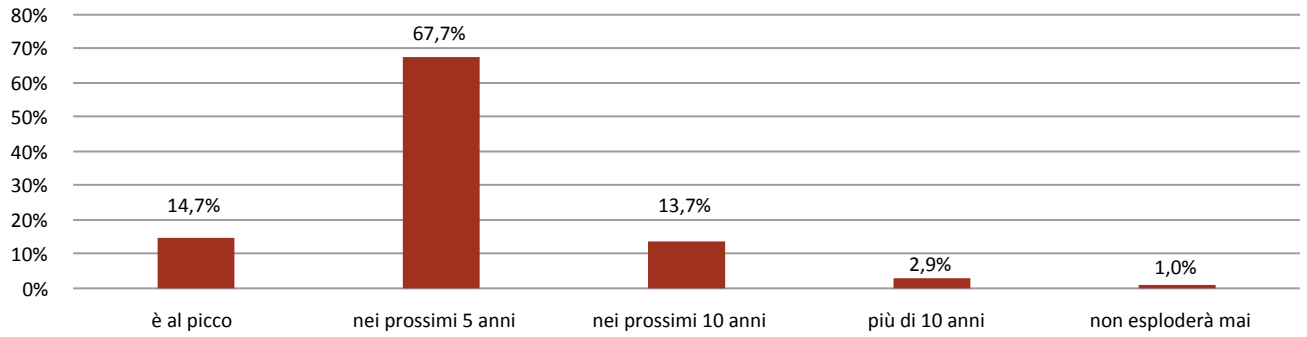
Fonte: Sortlist, 2022



17 The Wall Street Journal, 15 ottobre 2022.
18 Secondo il Wall Street Journal, alla data di pubblicazione dell'articolo il conteggio degli utenti si attestava a quota 200 mila unità e veniva evidenziato come, secondo statistiche interne, solo il 9% dei mondi costruiti dai creators sarebbe stato visitato da almeno 50 persone, mentre la maggior parte degli stessi non risulterebbe visitata da alcun utente.

Fig. 3.17: Tempistiche di massima diffusione del metaverso (%, 2022)

Fonte: Sortlist, 2022



3.5. IL METAVERSO: PRIME PROVE DI REGOLAMENTAZIONE

L'affermazione di un framework complesso come quello che potrebbe verosimilmente determinare il metaverso comporterebbe la coesistenza di numerosi servizi e fornitori capaci di interagire in maniera sempre più articolata ponendo all'attenzione una serie di implicazioni impattanti diverse aree del diritto che necessitano di essere identificate e adeguatamente valutate. **Al netto delle generali criticità e rischi connessi al tema della sicurezza, il primo ambito di assoluta rilevanza concerne senza dubbio la privacy e, dunque, la tutela dei dati personali**. Il metaverso, infatti, possiede la capacità di aggregare tecnologie e servizi che realizzano una convergenza tra reale e virtuale tale da "digitalizzare" la persona ed imporre un paradigma del tutto nuovo che si nutre dei dati in quanto risorsa indispensabile ad assicurare una *user experience* pienamente soddisfacente.

È chiaro che un modello come quello del metaverso, che si alimenta attraverso la presenza costante di informazioni e dati e che ruota intorno ad entità sempre più connesse, all'interno dell'ecosistema normativo disegnato dal GDPR pone una serie di complesse questioni, legate, tra l'altro, alla **difficoltà di definire a priori le finalità di trattamento** (da comunicare ai soggetti interessati), garantire **l'osservanza del principio di trasparenza** senza imporre di fornire indicazioni troppo puntuali sul funzionamento degli algoritmi da parte dei fornitori di servizi di IA, conciliare il **principio di minimizzazione dei dati** con i sistemi di IA che per natura sono progettati per trattare moli enormi di informazioni, distinguere in maniera agevole il titolare e l'incaricato del trattamento dei dati personali, **raccogliere un consenso esplicito** indispensabile per particolari categorie di dati come quelli **sanitari** e **biometrici**, giustificare trattamenti fondati su dati non raccolti presso l'interessato o un terzo ma autonomamente dedotti da sistemi di IA, individuare la giurisdizione competente, nonché conciliare le esigenze legate alla previsione by design di forme di anonimizzazione dei dati o costituzione di cluster così ampi da rendere irriconoscibili i singoli interessati, con la necessità degli utenti di assumere nuove identità digitali.

L'identità digitale, intesa come rappresentazione unica di un soggetto nell'ambito di una transazione online, sarà certamente un aspetto fondamentale per i mondi virtuali 4.0, incluso il metaverso. Sul tema, **sarà cruciale valutare gli effetti della proposta di Regolamento eIDAS 2.0, che modifica il Regolamento (UE) n. 910/2014**. In particolar modo, il nuovo framework normativo dovrà garantire una maggiore

interoperabilità tra i Portafogli Europei di Identità Digitale, nonché un livello elevato di sicurezza e protezione dei dati degli utenti.

Se appaiono complesse le questioni legate alla tutela dei dati personali, necessarie riflessioni si impongono anche con riguardo alla **proprietà intellettuale**. Ed infatti, il metaverso rappresenta uno spazio favorevole ed incentivante la creazione di contenuti, a partire da quelli generati dagli utenti (c.d. *user-generated contents*, UGC che grande spazio stanno conquistando soprattutto nel gaming) che possono essere creati ed utilizzati in ambienti diversi e che certamente, al ricorrere dei presupposti normativamente richiesti, possono rientrare nell'ambito di applicazione e dunque sotto la tutela della disciplina del diritto d'autore.

A ciò si aggiungono rilevanti tematiche connesse all'**utilizzo improprio dell'immagine, nonché di marchi e altri segni distintivi**. In materia di proprietà industriale, in particolare, è ormai nota la controversia americana tra il designer Rothschild ed Hermes per contraffazione ed uso non autorizzato del marchio in relazione alle Metabirkins, che ha posto all'evidenza, innanzitutto, la necessità di domandarsi, a livello generale, se i brand tutelati nel mondo reale godano di analoga tutela nel metaverso e, più in particolare, di definire in maniera chiara alcuni concetti come quello di NFT (acronimo di non fungible token) comprendendo se esso sia da considerare una copia o riproduzione dell'opera originale e dunque sia bisognoso di autorizzazione da parte del titolare dei diritti di proprietà intellettuale o se, invece, esso rappresenti una vera e propria creazione artistica (tenendo a mente che la maggior capacità degli NFT, rispetto ai canali tradizionali, di raggiungere le nuove generazioni, potrebbe suggerire agli stessi brand strategie di marketing non orientate a contestare eventuali usi illeciti dei segni distintivi bensì a beneficiare della notorietà conseguente a tali usi). Tale controversia si è conclusa con il riconoscimento della prevalenza dell'elemento artistico-creativo ma con l'accoglimento delle istanze di Hermes in considerazione dell'esplicita ingannevolezza e capacità di generare confusione nei consumatori della strategia di marketing utilizzata dall'artista.

Ad oggi sono diverse le regole immediatamente impattanti su tale universo parallelo, in primis, quelle sull'intelligenza artificiale. Ed infatti, a livello UE, **il 21 aprile 2021 la Commissione Europea ha presentato una proposta di Regolamento (AI Act)**, la cui procedura di adozione ancora è in corso, che mira a dettare regole armonizzate sull'Intelligenza Artificiale tese a disciplinare, tra gli altri, i sistemi di IA giudicati "ad alto rischio" (Allegato III), quale l'identificazione e la categorizzazione biometrica delle persone fisiche. È interessante evidenziare che **alcuni usi dell'IA rilevanti per un metaverso saranno vietati se potenzialmente suscettibili di violare i diritti fondamentali degli individui**, ad esempio, mediante la manipolazione delle persone attraverso tecniche subliminali, senza che tali persone ne siano consapevoli, oppure attraverso lo sfruttamento delle vulnerabilità di specifici gruppi, quali i minori o le persone con disabilità, ovvero altre pratiche manipolative o di sfruttamento che causano danni agli individui, fino a giungere a sistemi che mirano al *social score*.

Particolari cautele invece dovranno essere adottate per i sistemi di IA ad alto rischio, per i quali il regolamento in discussione prevede, tra l'altro, l'adozione e mantenimento di un sistema di gestione del rischio, una progettazione che consenta la supervisione umana e che assicuri un livello adeguato di accuratezza, robustezza e sicurezza informatica oltre alla previsione di specifici obblighi a carico dei fornitori (implementazione sistema di qualità, tenuta documentazione, *conformity assessment*, azioni correttive, ecc.), degli importatori, dei distributori e degli utilizzatori di sistemi ad alto rischio.

Posto che infrastruttura essenziale per l'esistenza stessa del metaverso è il cloud computing, in grado di creare una rete globale interconnessa di server di proprietà di soggetti diversi dislocati in varie aree del

mondo, e che il metaverso presenta il potenziale per diventare un infinito *marketplace*, si pone anche il tema dell'adeguamento alle nuove regole stilate dal legislatore europeo con l'adozione del **Digital Markets Act** (Reg. n. 1925/2022), pubblicato sulla Gazzetta Ufficiale UE lo scorso 12 ottobre ed in vigore a partire da maggio 2023. E infatti tale regolamento **classifica i servizi di cloud computing ed i servizi di intermediazione online che comprende evidentemente i *marketplace*, come "servizi di piattaforma di base" e i fornitori di tali servizi come "gatekeeper"** al ricorrere dei presupposti declinati all'art. 3. Dalla designazione come gatekeeper discende un'ampia serie di obblighi e divieti tra cui spicca, rispetto al tema del metaverso, il divieto di processare i dati raccolti tramite terze parti che si servono della piattaforma del gatekeeper per offrire servizi di pubblicità, il divieto di combinare i dati personali raccolti sulla piattaforma con quelli raccolti su qualsiasi altra piattaforma del gatekeeper o di terze parti, il divieto dell'uso incrociato di dati personali raccolti su una piattaforma con quelli provenienti da altri servizi offerti separatamente dallo stesso gatekeeper ed infine il divieto di iscrivere automaticamente l'utente ad altri servizi del gatekeeper per combinare i dati personali. **Se a ciò si aggiunge che al gatekeeper è prescritto di garantire agli utenti finali l'effettiva portabilità dei dati personali forniti dall'utente o generati da quest'ultimo mediante l'utilizzo del servizio di piattaforma di base, nonché l'accesso continuo e in tempo reale a tali dati, emerge chiaramente la complessità applicativa in relazione al metaverso**.

Oltre alla disciplina applicabile ai gatekeeper, è probabile che gli scambi commerciali di varia natura, da impresa a consumatore, da consumatore a consumatore, da consumatore a impresa, attraverso i giochi, mediante metodi di pagamento tradizionali o innovativi, etc. che saranno realizzati nel metaverso, avranno una rilevanza per **il Reg. n. 1150/2019 che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online**, disciplinando i rapporti tra i titolari delle piattaforme (o dei motori di ricerca) e gli utenti commerciali che forniscono ai consumatori beni e servizi attraverso le stesse, prevedendo obblighi di trasparenza (ad esempio, in materia di posizionamento degli utenti commerciali nella visualizzazione delle offerte da parte dei consumatori), parità di trattamento e fissando il contenuto minimo delle disposizioni previste nei contratti tra la piattaforma e gli utenti commerciali, nonché imponendo una procedura obbligatoria di reclamo interna alla piattaforma. A ciò si aggiunge **la Direttiva n. 2161/2019 per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori**, c.d. Direttiva Omnibus, che introduce sanzioni più elevate per le violazioni della direttiva sui diritti dei consumatori, della direttiva sulle pratiche commerciali sleali, della direttiva in materia di indicazione dei prezzi e della direttiva sulle clausole abusive.

Non meno rilevante la disciplina contenuta nel **Digital Services Act (Reg. n. 2065/2022)**, pubblicato lo scorso 27 ottobre, che mira ad armonizzare gli obblighi posti in capo ai prestatori di servizi della società dell'informazione con la declinazione di categorie ampie, così come le tipologie di intermediari online che ricadono nel suo ambito di applicazione, dai fornitori di accesso alle reti di comunicazione, ai servizi di cloud e di hosting, alle piattaforme online come i servizi di social media. **Il DSA, in particolare, ha introdotto un quadro orizzontale per tutte le categorie di contenuti, prodotti, servizi e attività sui servizi di intermediazione** nel quale viene delineato un regime di responsabilità diversificato in base ai servizi offerti ed alla dimensione del fornitore ed ha introdotto un'ampia gamma di obblighi di trasparenza ma anche organizzativi e procedurali che sarà importante declinare rispetto alle peculiarità del metaverso.

Peraltro, al fine di tutelare i diritti fondamentali degli individui nella società del futuro, **dovrà essere posta**

particolare attenzione verso la resilienza delle infrastrutture fisiche e digitali che permettono l'operatività e il funzionamento del metaverso, per cui è auspicabile che – in primo luogo – si ragioni su standard e regole giuridiche inerenti la sicurezza di reti, sistemi e servizi sia da un punto vista prettamente cibernetico (sul modello della **Direttiva NIS2**), ma anche con riguardo alla protezione fisica delle stesse (**Direttiva CER**). In secondo luogo, una possibile direzione potrebbe essere quella di emanare normative sempre più settoriali, che puntino a garantire la resilienza operativa digitale di quegli ambiti maggiormente critici per il corretto funzionamento del metaverso, sulla scia di quanto fatto con il **Regolamento DORA** per il settore finanziario dell'UE.

In terzo luogo, sarà di cruciale importanza garantire la sicurezza dei dispositivi e dei sensori che gli utenti dovranno necessariamente utilizzare per sfruttare appieno le opportunità del metaverso. In quest'ottica, **le istituzioni europee stanno finalizzando la proposta di Cyber-Resilience Act** (CRA), che mira a far rispettare una serie di requisiti di cybersicurezza lungo tutta la catena del valore (produttori, importatori e distributori) e durante l'intero ciclo di vita di prodotti con elementi digitali, il cui uso previsto (o ragionevolmente prevedibile) includa una connessione logica o fisica, diretta o indiretta, di dati a un dispositivo o a una rete, come nel caso del metaverso.

Inoltre, i mondi virtuali immersivi e interconnessi potranno portare con sé nuove tipologie di cyberattacchi, le cui caratteristiche dovranno essere note al legislatore, cosicché possa apportare le opportune modifiche al quadro normativo in materia di cybersicurezza. A titolo esemplificativo, è possibile richiamare: a) attacco ***human joystick***, che si realizza tramite la manipolazione dei sensori, dei dispositivi e delle tecnologie indossate (o in altro modo utilizzate) dall'utente, al fine di controllare la sua posizione e spostarlo nello spazio fisico, ad esempio, per motivi legati all'inganno, alla violenza o all'estorsione; b) **attacco *chaperone***, con cui si modificano i confini dell'ambiente virtuale per danneggiare fisicamente un individuo, ad esempio facendolo cadere da una rampa di scale che si trova nel mondo *offline*; c) ***avatar impersonation attacks***, realizzabili dall'attore malevolo sfruttando vulnerabilità di sicurezza dei sistemi di autenticazione o dei processi di verifica dell'identità, consentendogli di fingersi un altro utente (si pensi all'eventualità in cui si impersonifichi l'avatar di un personaggio influente, un politico, ecc.) e produrre attività illecite (es. furto di credenziali altrui) e diffondere messaggi d'odio e disinformazione fingendosi qualcun altro; d) **altre tipologie di cyberattacchi ad oggi non conoscibili**, dato che le tecnologie di riferimento non sono ancora sufficientemente diffuse o, addirittura, si trovano in fase di sviluppo.

Il dibattito sul metaverso riguarda, evidentemente, anche l'Italia dove, nell'aprile 2022, **la Commissione Affari Costituzionali del Senato ha avviato un'indagine conoscitiva**, poi interrotta a seguito della crisi del governo Draghi e della conseguente fine anticipata della legislatura, articolata in un ciclo di audizioni teso ad individuare le opportunità e le criticità connesse al metaverso. I contributi offerti dagli esperti auditi hanno posto all'attenzione una serie di importantissime questioni che vanno dalla definizione della governance e la difficoltà di individuare il soggetto competente a disciplinare il metaverso e a farne rispettare le regole, alle criticità legate alla necessità di assicurare, rispetto alle condizioni generali di contratto, adeguata trasparenza e consapevolezza da parte degli utenti, al bisogno di ripensare gli strumenti tradizionalmente pensati per garantire la privacy, all'esigenza di regolamentare il trasferimento transazionale dei dati, alla necessità di garantire la riconducibilità, in un universo fatto di avatar, delle azioni e delle relative responsabilità. A ciò si aggiungono le questioni legate alle maggiori tutele da garantire ai minori, alla conclusione di transazioni

finanziarie anche con monete virtuali, alla gestione della pubblicità occulta e/o reale ed alla riconducibilità di tale pubblicità ai marchi.

L'UE ha promosso un numero elevato di iniziative per disciplinare il metaverso. Ad esempio, **il 5 aprile 2023 la Commissione europea ha lanciato una consultazione pubblica**[19] aperta fino al 3 maggio 2023 **per sviluppare una strategia per i mondi virtuali emergenti, basata sul rispetto dei diritti digitali, delle leggi e dei valori dell'UE**. Il suo obiettivo è far sì che i Metaversi, aperti e interoperabili, possano essere utilizzati dal pubblico e dalle imprese in modo sicuro e fiducioso. Tale progetto ha affiancato un'ulteriore consultazione pubblica dell'UE in tema di ripartizione dei costi di espansione delle infrastrutture di rete[20], per cui si parte dal presupposto che l'aumento dei dati richiesti dalle nuove tecnologie, incluso il metaverso, richieda un inevitabile mutamento dell'infrastruttura digitale sottostante.

Anche la presidente della Commissione europea, Ursula von der Leyen, ha lanciato – il 23 febbraio scorso – un'iniziativa non legislativa sul metaverso[21] e, allo stesso modo, **il Parlamento europeo ha lavorato a un report sulle relative opportunità, sui rischi e sulle implicazioni politiche**[22].

A guidare la volontà regolatoria a livello comunitario è senza dubbio la Commissione, che l'11 luglio ha presentato **la prima strategia sul Web 4.0 e i mondi virtuali per guidare la futura transizione tecnologica nel rispetto dei principi di diritto**[23]. Tale intento è stato esplicitato per la prima volta il 14 settembre 2022 dalla già citata presidente von der Leyen nella sua lettera di intenti "*State of the Union*"[24]. La strategia rientra nell'ambito dell'"*European fit for the digital age*"[25] per contribuire al raggiungimento degli obiettivi europei di sovranità digitale.

All'interno della strategia, viene fatta una differenza tra i concetti di *Virtual worlds*, Web 3.0 e Web 4.0. Innanzitutto, i mondi virtuali sono ambienti persistenti e immersivi, basati su tecnologie come il 3D e la realtà estesa (XR), che consentono di fondere mondi fisici e digitali in tempo reale, per una varietà di scopi come la progettazione, la realizzazione di simulazioni, la collaborazione, l'apprendimento, la socializzazione, la realizzazione di transazioni o la fornitura di intrattenimento.

Il Web 3.0 è, invece, la terza generazione del *World Wide Web*. Le sue caratteristiche principali sono l'apertura, il decentramento e la piena responsabilizzazione degli utenti che consente loro di controllare il valore economico dei dati, gestire le identità online e partecipare attivamente nel governo della rete. Le funzionalità web semantiche consentono di collegare i dati tra pagine, applicazioni e file. Le tecnologie decentralizzate e i gemelli digitali agevolano le transazioni *peer-to-peer*, la trasparenza, la democrazia dei dati e l'innovazione lungo intere catene del valore.

Mentre con il termine Web 4.0 la Commissione fa riferimento all'incrocio delle tecnologie immersive, dell'*internet of things*, dell'intelligenza artificiale e della *blockchain* in luoghi digitali programmati per offrire agli utenti un tipo di esperienze che coadiuvano

19 EUROPEAN COMMISSION, Virtual worlds (metaverses) – a vision for openness, safety and respect, in europa.eu.
20 EUROPEAN COMMISSION, The future of the electronic communications sector and its infrastructure, in europa.eu.
21 EUROPEAN COMMISSION, Setting the grounds for the transformation of the connectivity sector in the EU Speech by Commissioner Thierry Breton, in europa.eu, 23/02/2023.
22 EUROPEAN PARLIAMENT, Virtual worlds: opportunities, risks and policy implications for the Single Market, in europa.eu, 2022.
23 EUROPEAN COMMISSION, Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition, in europa.eu, Strasburgo, 11/07/2023.
24 EUROPEAN COMMISSION, State of The Union 2022 Letter of Intent, in europa.eu, Brussels, 14/09/2022.
25 EUROPEAN COMMISSION, A Europe fit for the digital age Empowering people with a new generation of technologies, in europa.eu.

il mondo *online* e quello *offline* con un'attitudine immersiva altamente performante e intuitiva[26].

La Commissione osserva anche la possibile crescita futura del mercato globale dei mondi virtuali, che da 27 miliardi di euro registrati nel 2022 potrà raggiungere oltre 800 miliardi entro il 2030, offrendo in considerevoli settori circa 860.000 nuove occupazioni lavorative.

La strategia si conforma a quanto disposto dal "***Digital Decade Policy Programme***"[27] ed è composta da quattro pilastri, i quali prevedono di:

1. **affidare alle persone più potere e rafforzare le competenze per aumentare l'*awareness,* l'accesso a informazioni affidabili e costituire un centro di talenti capaci di giostrare il mondo virtuale**. Tra i propositi con scadenza 2023 rientra la promozione dei principi guida derivanti dal *Citizens' Panel* e la redazione, entro il 2024, di linee guida che fungeranno da "cassetta degli attrezzi per i cittadini". Peraltro, la Commissione sosterrà lo sviluppo delle competenze mediante progetti finanziati dal programma *Digital Europe*[28] e, per i creatori di contenuti digitali, dal programma *Creative Europe*[29];
2. **sostenere un ecosistema industriale Web 4.0 per aumentare l'eccellenza delle imprese e combattere il grave problema della frammentazione**. Importante iniziativa della Commissione è la proposta di un partenariato sui mondi virtuali nell'ambito di *Horizon Europe,* che dovrebbe avviarsi nel 2025 con lo scopo di scandire una tabella di marcia sia sul piano industriale, sia su quello tecnologico a disposizione delle esigenze dei mondi virtuali. La strategia tutelerà anche i *creator* e le *media company* europee;
3. **contribuire al pieno sostegno del progresso sociale e dei servizi pubblici virtuali**, già evidente da alcune iniziative dell'UE, tra cui *Destination Earth* (DestinE); *Local Digital Twins*, a favore delle *smart communities*, o *European Digital Twin of the Ocean* che incita il progresso scientifico puntando sui ricercatori, l'innovazione delle applicazioni di precisione, focalizzandosi sulle industrie, e il miglioramento dei processi decisionali informati e consapevoli da parte delle autorità competenti. Tra le recenti iniziative pubbliche lanciate dalla Commissione vanno annoverate: *CitiVerse* e *European Virtual Human Twin*. La prima vuole creare un ambiente urbano coinvolgente e utile per la gestione della città, mentre la seconda si concretizza in un gemello umano digitale, che riproduce l'anatomia del corpo umano in ogni sua componente per aiutare gli esperti in ambito sanitario nell'assunzione di decisioni cliniche e sulla scelta delle cure per il paziente;
4. **promuovere la creazione di standard globali, assicurando che i mondi virtuali e il Web 4.0 non siano dominati da pochi grandi attori**, sviluppando un modello di *governance* di internet valido a livello mondiale e in totale conformità con i valori e i principi comunitari.

26 EUROPEAN COMMISSION, Communication from The Commission to The European Parliament, The Council, cit., p.1.
27 EUROPEAN COMMISSION, Europe's Digital Decade, in europa.eu.
28 EUROPEAN COMMISSION, The Digital Europe Programme, in europa.eu.
29 EUROPEAN COMMISSION, About the Creative Europe Programme, in europa.eu.

icom
istituto per la competitività

CAPITOLO 4

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

4.1. LE INFRASTRUTTURE DI RETE FISSA

Continua inarrestabile il progresso delle tecnologie digitali che non solo stanno abilitando nuovi modelli di business, inediti strumenti relazionali, efficienti tecniche di produzione ed innovativi strumenti di definizione delle policy pubbliche ma stanno spianando la strada a mondi e realtà inimmaginabili fino a pochissimo tempo fa, prova ne è il metaverso, universo digitale che unisce mondi virtuali dalle innumerevoli e straordinarie opportunità e che pone, come tutte le grandi rivoluzioni, nuove e complesse sfide da affrontare dapprima per comprendere la portata del fenomeno e poi per governarlo.

È chiaro che in un contesto che si nutre di tecnologie sempre più sofisticate la cui potenza risiede innanzitutto nella capacità di raccogliere e analizzare moli enormi di dati ed in un panorama internazionale che incentra gran parte della propria competitività sullo sviluppo e l'offerta delle nuove tecnologie e dei servizi ad esse correlati, lo sviluppo di reti di telecomunicazione capillari e performanti costituisce una condizione imprescindibile per l'Unione Europea in generale e per l'Italia in particolare.

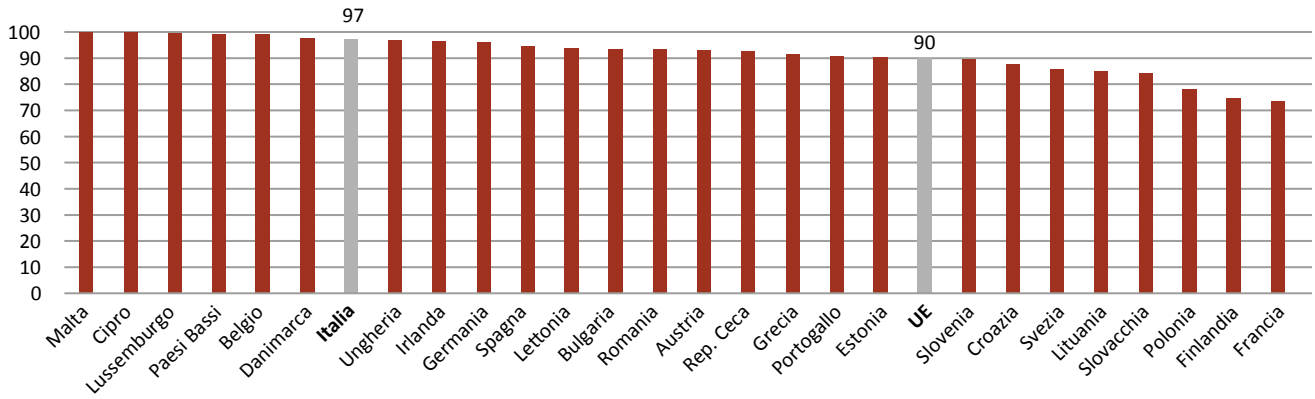
Il 27 settembre scorso è stato pubblicato il **Primo rapporto sullo stato del decennio digitale** che descrive i progressi registrati dai Paesi membri in materia di trasformazione digitale nelle quattro dimensioni del programma politico del Decennio digitale e, in particolare, competenze digitali, infrastrutture digitali, digitalizzazione delle imprese e digitalizzazione dei servizi pubblici.

Rispetto alle infrastrutture digitali, è noto che l'UE persegue l'obiettivo di raggiungere una copertura gigabit per tutti e reti 5G performanti in tutte le aree popolate, il 20% della produzione globale di semiconduttori, la distribuzione di almeno 10.000 nodi edge altamente sicuri e neutrali dal punto di vista climatico e la realizzazione del primo computer con accelerazione quantistica entro il 2025 (tre entro il 2030). Ebbene, se questi sono gli obiettivi e le tempistiche per il raggiungimento degli stessi, emerge a livello europeo ancora una forte disomogeneità e, in generale, la necessità, per essere all'altezza dei competitor internazionali, primi tra tutti Cina e Stati Uniti, di accelerare lo sviluppo delle reti VHCN e del 5G.

Entrando ora nel merito dei dati e partendo dai dati di copertura e take up relativi alle reti fisse, se da un lato prevedibilmente risulta ormai completata

Fig. 4.1: Copertura NGA (% di famiglie, 2022)

Fonte: Digital Scoreboard, 2022



(o quasi) nella grande maggioranza dei paesi UE la **copertura NGA** – che comprende le tecnologie FTTH, FTTB, Docsis 3.0 VDSL ed altre tecnologie che garantiscono almeno 30 Mbps in download – **con una percentuale di copertura di almeno il 90% in ben 19 Stati Membri** (Fig. 4.1) e l'Italia si trova in vetta nel confronto con alcuni dei principali Paesi europei grazie ad un indice di crescita che fotografa un incremento del 690% a fronte di tassi che non vanno oltre il 305% della Francia (Fig. 4.2), più complessa e meno raggiante appare la performance europea ed italiana in relazione a VHCN (che comprende FTTH, FTTB and Cable Docsis 3.1 ed esclude la copertura VDSL) ed FTTP.

Ed infatti, se i dati riportati nella Fig. 4.3 confermano il podio del 2021 con il primato di Malta con una copertura pari al 100%, seguita a stretto giro da Paesi Bassi e Danimarca con il 98% e 96% di copertura, l'Italia, nonostante un incremento di 19 p.p. circa rispetto al 2020, mostra una performance ancora non soddisfacente, registrando una percentuale inferiore di ben 20 punti rispetto alla media europea (53,7% vs 73,4%).

Ancor meno esaltante appare la copertura FTTP (Fig. 4.4) la cui media europea si ferma al 56,5% e quella italiana al 53,7%, sideralmente distante dal podio, che vede primeggiare Romania, Spagna e Portogallo con ben il 96%, 91 e 90,8% di copertura.

Più allarmanti, soprattutto se si pensa all'obiettivo fissato nel cap. II della Dichiarazione europea sui diritti e i principi digitali per il decennio digitale di garantire a tutti i cittadini europei accesso alla connettività digitale ad alta velocità a prezzi accessibili, i dati relativi alle aree rurali. Ed infatti i dati di copertura VHCN 2022 nelle aree rurali vedono il dato europeo fermo al 45% e quello italiano

Fig. 4.2: Grado di copertura NGA (% famiglie)

Fonte: Elaborazione I-Com su dati Commissione europea

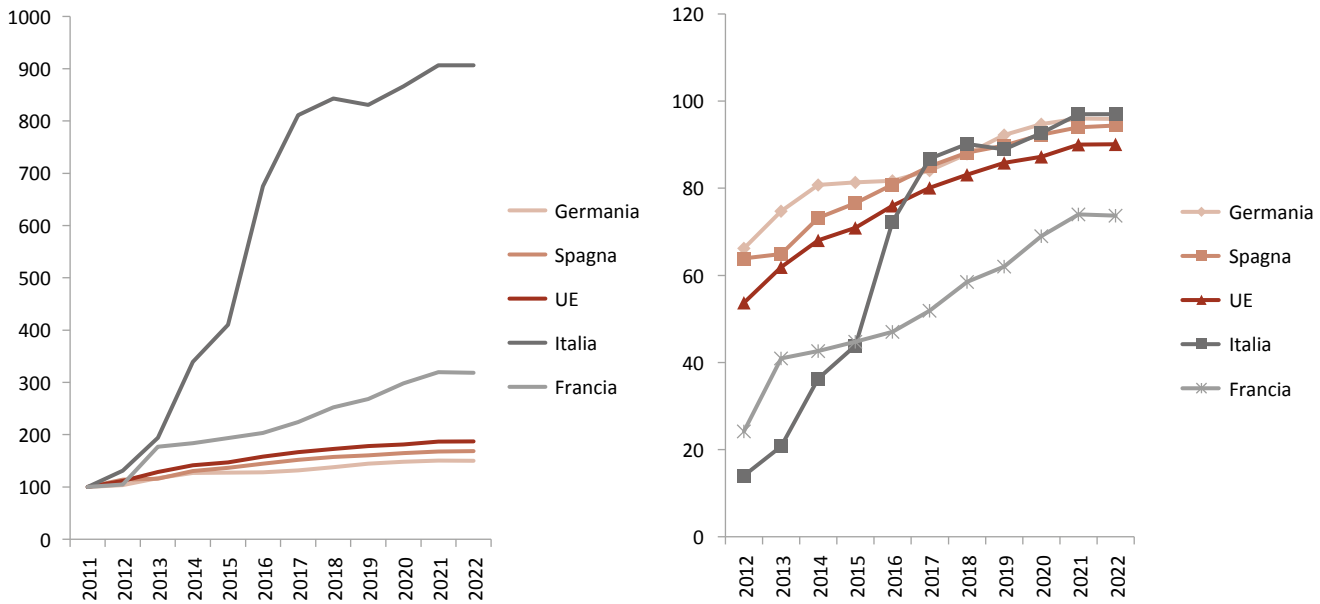


Fig. 4.3: Copertura VHCN (%, 2022)

Fonte: Digital Scoreboard

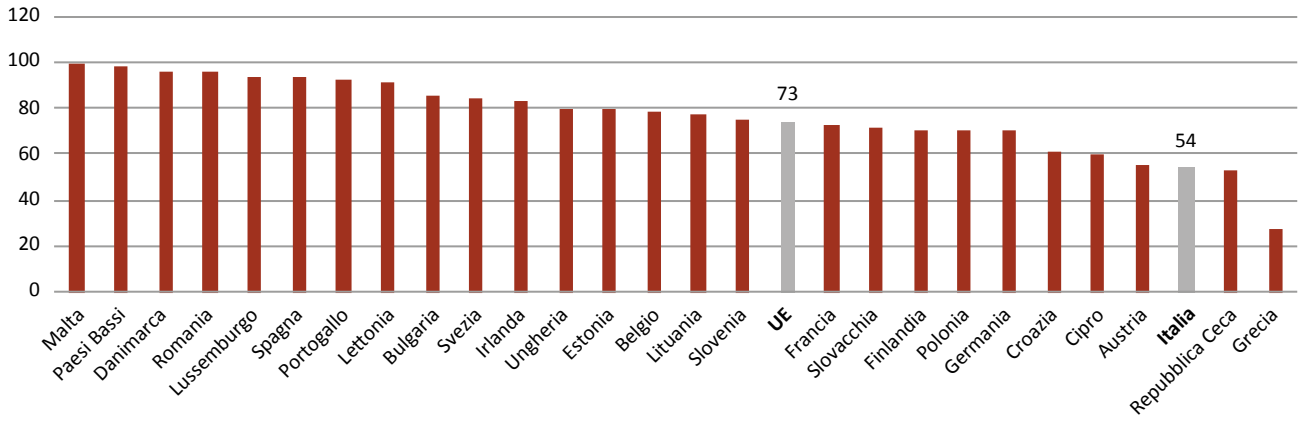
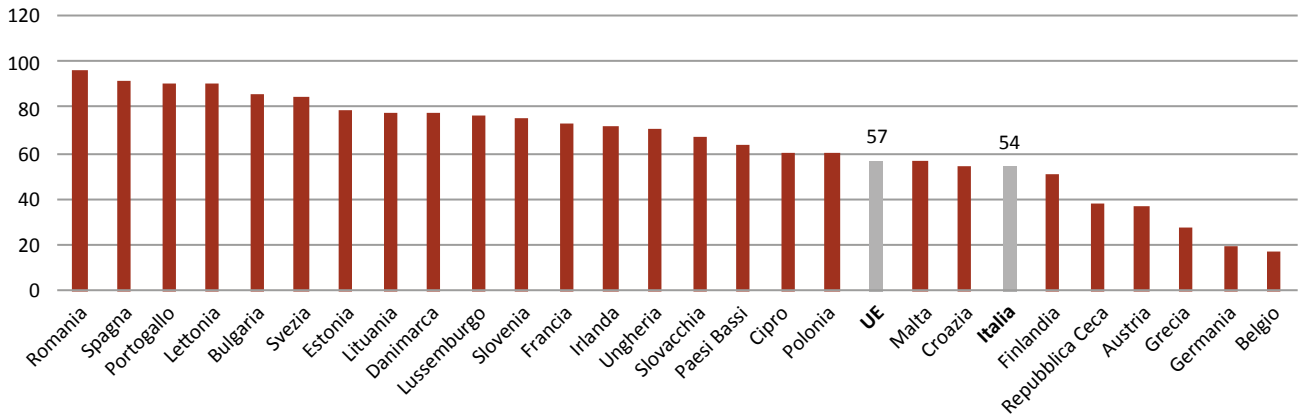


Fig. 4.4: Copertura FTTP (%, 2022)

Fonte: Digital Scoreboard



addirittura al 26% ad una distanza di ben 19 p.p. (Fig. 4.5) mentre la copertura FTTP nelle aree rurali nel 2022 (Fig. 4.6) si attesta al 41% a livello UE (l'Italia registra un modesto 26%).

Se l'analisi dei dati di copertura, anche relativi all'Italia, pur evidenziando la necessità di accelerare lo sviluppo delle reti per assicurare maggiore capillarità ed uniformità sul territorio europeo, consentono, alla luce dei progressi compiuti, di nutrire un moderato ottimismo rispetto al futuro, decisamente preoccupante e certamente più complessa da gestire, vista la concomitanza di innumerevoli cause, appare l'immaturità della domanda di connettività.

Ed infatti, la **percentuale di abbonamenti in fibra** (FTTH, FTTB e FTTP con esclusione di quelli FTTC) **sul totale degli abbonamenti** (Fig. 4.5) **a livello OECD è ferma al 38%.** Non mancano buone performance,

Fig. 4.5: Copertura VHCN aree rurali (%, 2022)

Fonte: Digital Scoreboard, 2022

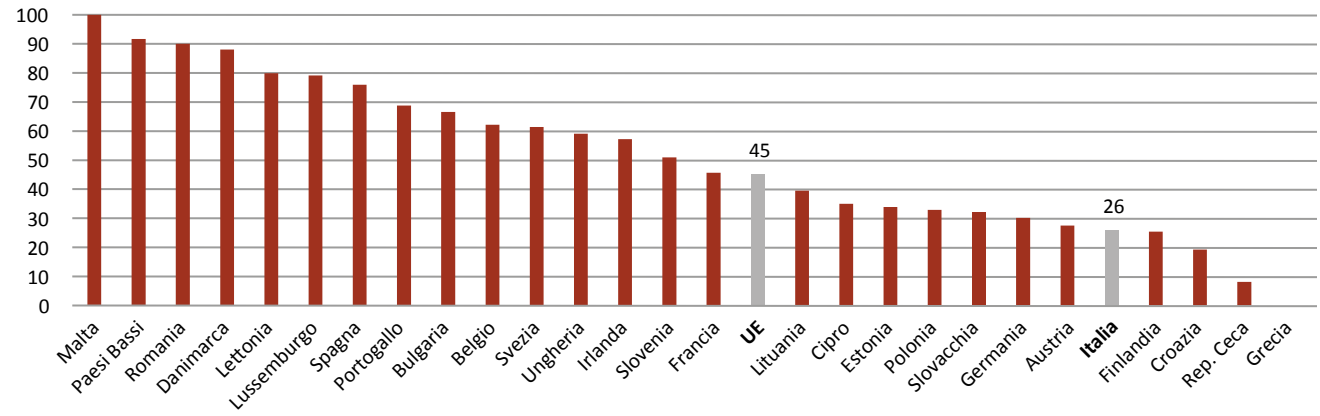
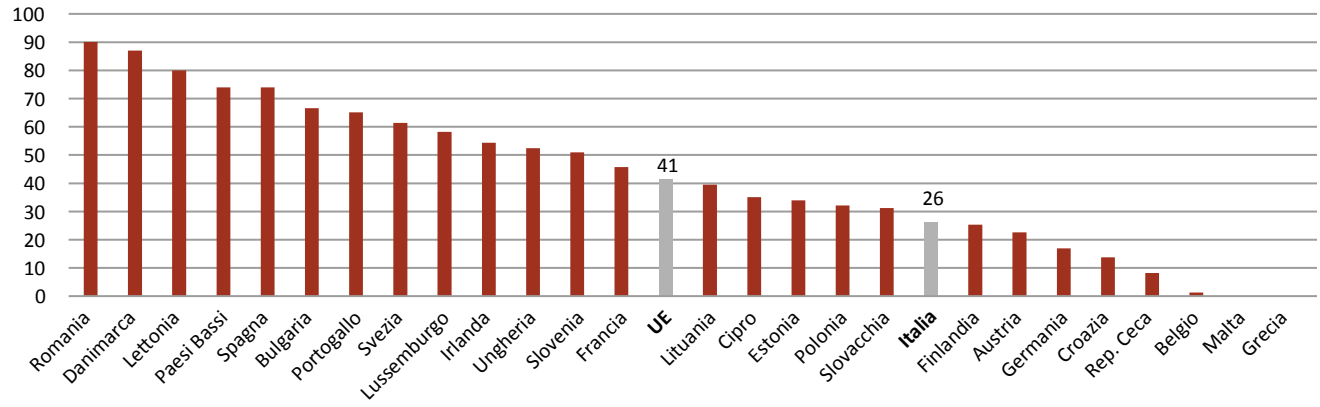


Fig. 4.6: Copertura FTTP aree rurali (%, 2022)

Fonte: Digital Scoreboard, 2022



come quella della Spagna che guida la classifica con l'83% di abbonamenti in fibra, seguita da Svezia (81%) e Lettonia (79%), ma al contempo spiccano risultati non esaltanti tra cui quello italiano che registra una percentuale del 19%.

Se si sofferma l'attenzione sui dati relativi alla **percentuale di abbonamenti ad almeno 100 Mbps sul totale di abbonamenti alla rete fissa (Fig. 4.8), la performance europea rivela ampi margini di miglioramento, con una percentuale del 55%** (l'Italia si pone leggermente sopra il dato europeo con una percentuale del 59,6%).

Estremamente significativa – circa 27 p.p. – la distanza dell'Italia dalla Spagna capolista che impone l'implementazione di ogni azione utile ad accrescere l'*awareness* della popolazione circa i benefici, in termini anche di servizi accessibili, garantiti da connessioni performanti e ad incentivarne dunque l'adozione.

Fig. 4.7: Percentuale di connessioni in fibra sul totale degli abbonamenti broadband (2022)

Fonte: OECD

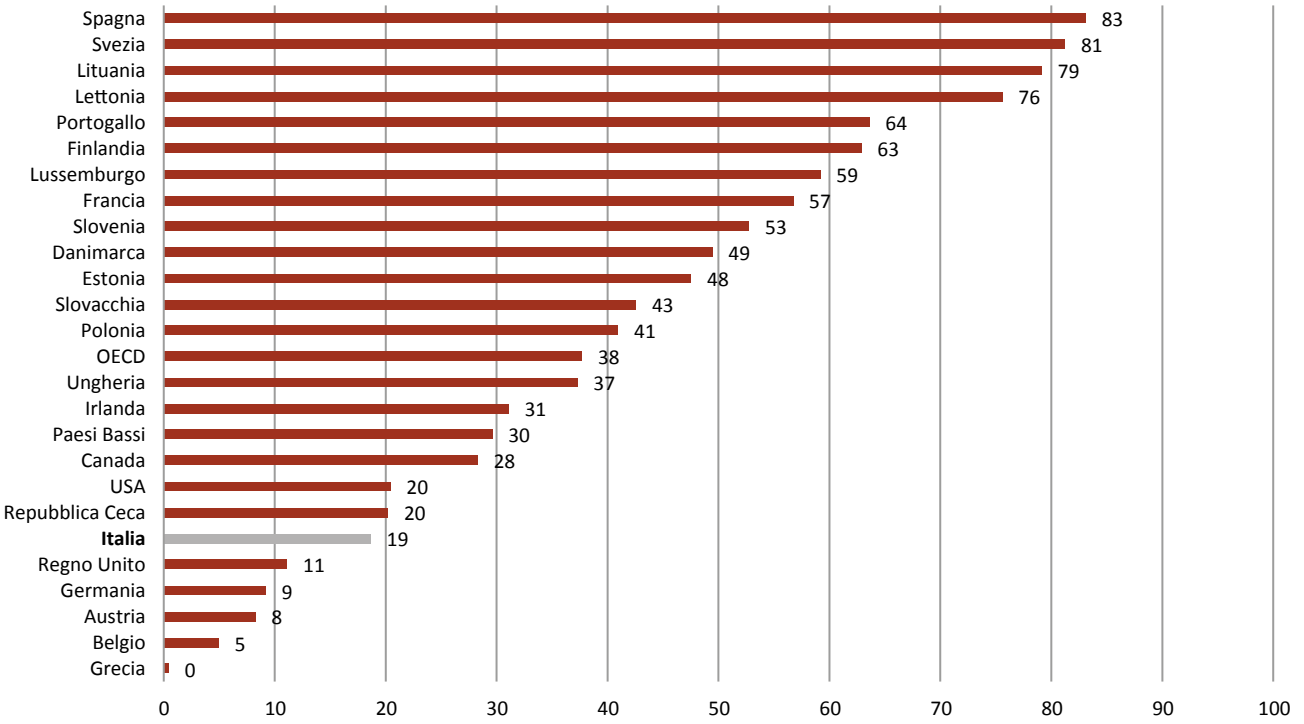
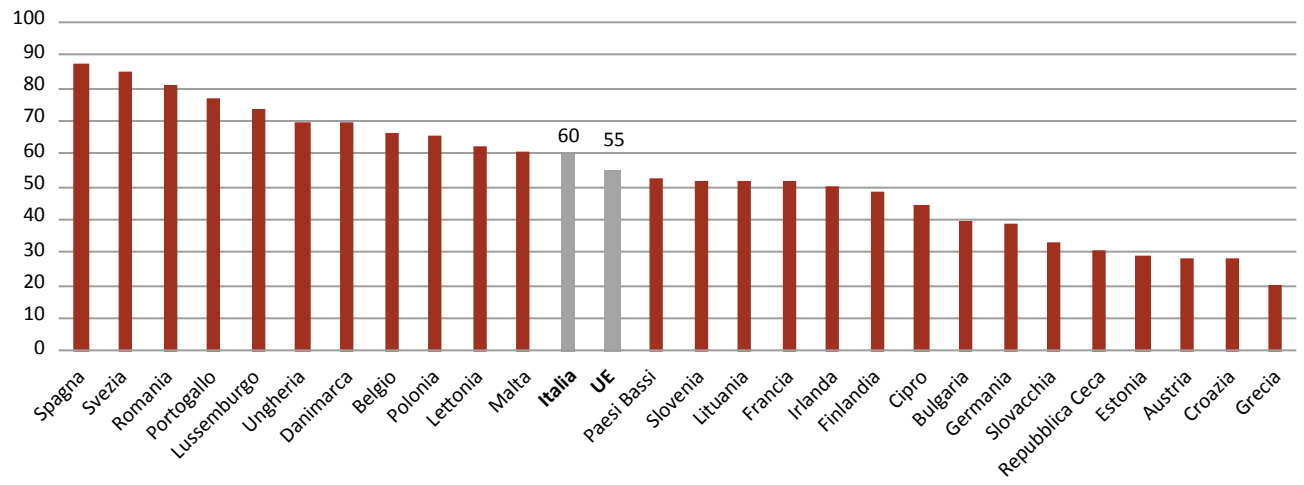


Fig. 4.8: Percentuale di abbonamenti ad almeno 100 Mbps (2022)

Fonte: Digital Scoreboard



Considerati i dati di copertura e la grave immaturità della domanda di connettività, non stupisce la performance europea in merito alla percentuale di famiglie che ha sottoscritto nel 2022 abbonamenti fissi ad almeno 1 Gbps. Dai dati emerge un grave ritardo generale, con una percentuale europea ferma al 13,8%, alla quale anche l'Italia risulta allineata con il 13,4%. Soltanto Francia e Ungheria registrano percentuali nettamente superiori pari, rispettivamente, al 40% e al 30% (Fig. 4.9).

Rispetto al mondo delle imprese, premesso che l'aggiornamento dei dati di copertura relativi alle connessioni veloci è fermo al 2019 e che dunque non è possibile ricostruire dettagliatamente il grado di maturità generale delle imprese rispetto alla connettività di ultima generazione, se si focalizza l'analisi sulle imprese dotate di connessione fissa, emerge, prevedibilmente, una grande maturità, con una percentuale europea che si attesta al 94% ed il dato più basso, quello lettone, che risulta comunque pari al 77%. L'Italia, con il 98%, si posiziona seconda dietro soltanto alla Danimarca (Fig. 4.10).

Fig. 4.9: Percentuale di abbonamenti ad 1 Gbps (2022)

Fonte: Digital Scoreboard

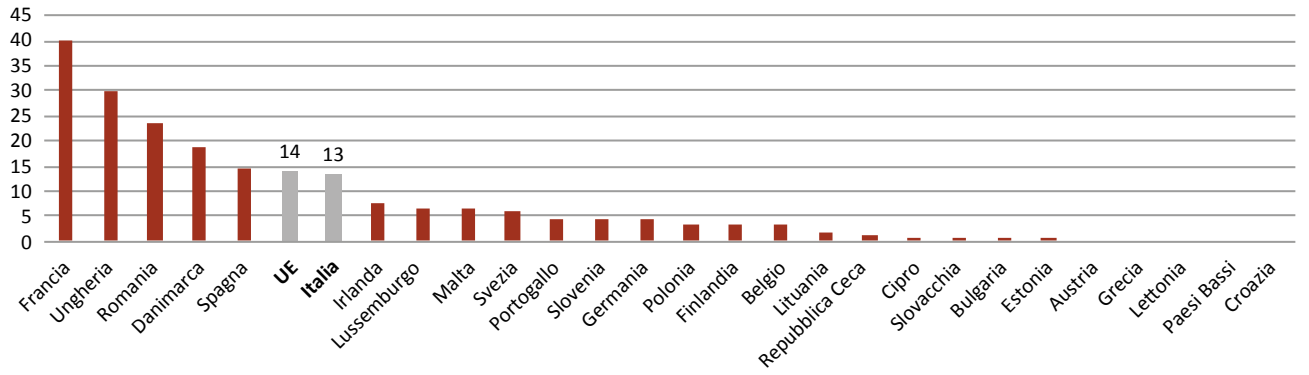
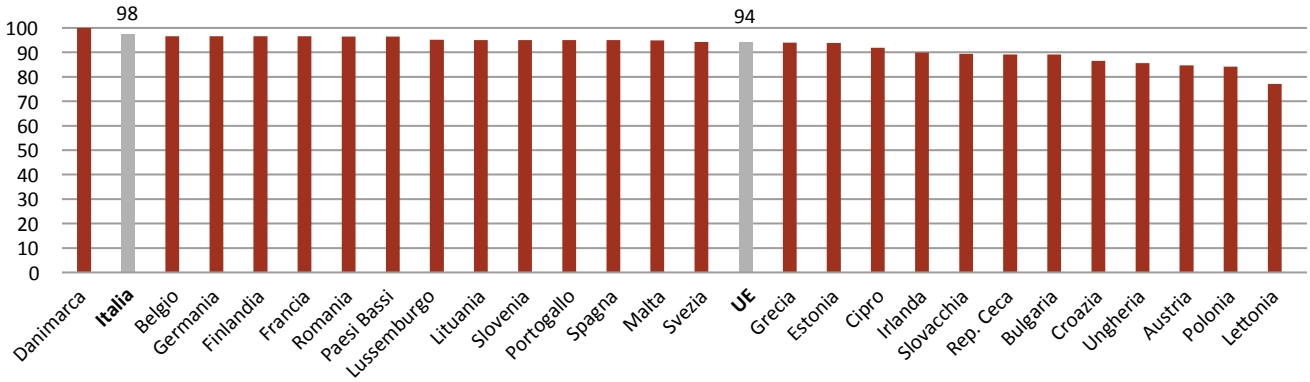


Fig. 4.10: Percentuale di imprese con connessione fissa (2022)

Fonte: Digital Scoreboard, 2022



4.2. LE INFRASTRUTTURE DI RETE MOBILE

Se l'analisi sin qui condotta ha evidenziato, rispetto alle reti fisse, la necessità, nonostante i progressi registrati negli ultimi anni, di accelerare lo sviluppo infrastrutturale, stessa esigenza si rinviene nel segmento mobile ed in particolare rispetto alle reti 5G.

L'Ericsson Mobility Report relativo al secondo trimestre 2023 quantifica in 8,3 mld il totale degli abbonamenti mobili a livello globale, di cui 1,3 mld sono abbonamenti 5G, in aumento di 175 mln rispetto al trimestre precedente. Lato offerta, salgono a **260** (rispetto ai 218 del secondo trimestre 2022) **gli operatori che hanno lanciato offerte commerciali 5G, di cui 35 (24 nel secondo trimestre 2022) relative a reti 5G standalone**, indispensabili per la fornitura di servizi ad elevata complessità come, ad esempio, l'automazione industriale e l'*automotive*.

In questo scenario globale l'Unione Europea continua la propria corsa al raggiungimento degli obiettivi fissati al 2030 che puntano anche ad uno sviluppo capillare di reti 5G. Guardando al presente, se da un lato appaiono confortanti i dati relativi alla **5G readiness** che dimostrano come le procedure di assegnazione delle frequenze 5G (700 MHz, 3,6 GHz e 26 GHz) siano state completate o siano ad un buon grado di avanzamento in molti paesi UE (Fig. 4.11), positivi risultano i dati di copertura 5G, soprattutto in termini di accelerazione a partire dal 2020. Ed infatti, con la doverosa precisazione che i dati non tengono conto della distinzione tra le coperture realizzate in modalità standalone e non-standalone, la Fig. 4.12 mostra una percentuale di copertura 5G che è passata a livello europeo dal 14% del 2020 al 81,2% in termini di famiglie raggiunte, a dimostrazione degli enormi sforzi compiuti dagli operatori. L'Italia, in particolare, è passata dall'8% del 2020 a ben il 99,7% di copertura 5G, risultando quarta in Europa, dopo Cipro, Malta e Paesi Bassi con rispettivamente il 100% ed il 99,9% di copertura 5G.

Considerato che il 5G usa tre fasce di frequenze (bassa, media e alta) e, in particolare, 694-790 Mhz, 3,6-3,8 GHz e 26,5-27,5 GHz e partendo dalla constatazione

Fig. 4.11: 5G readiness (2022)

Fonte: Digital Scoreboard, 2022

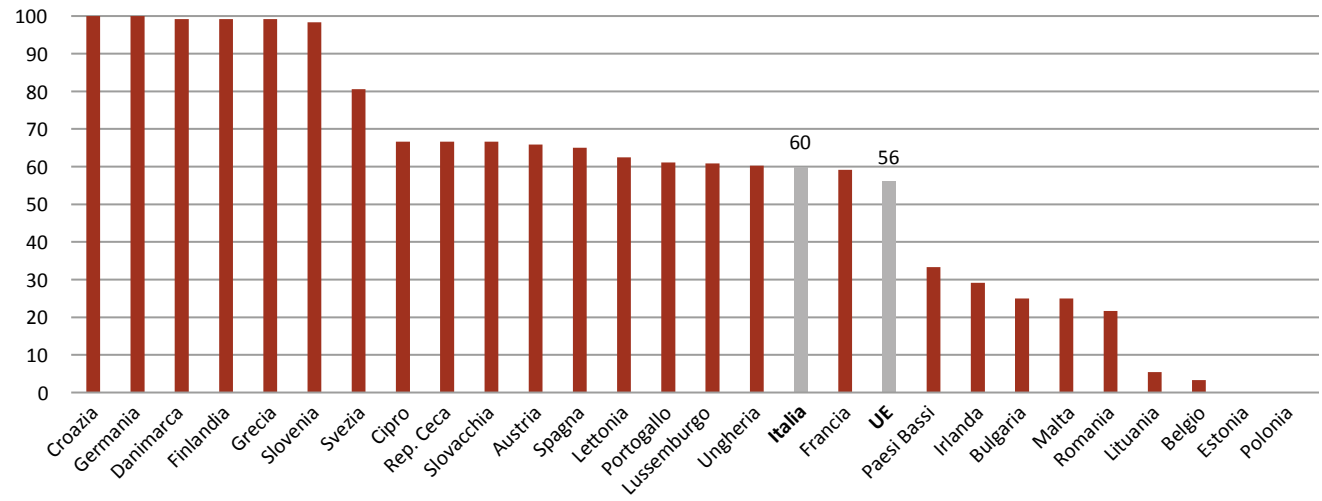
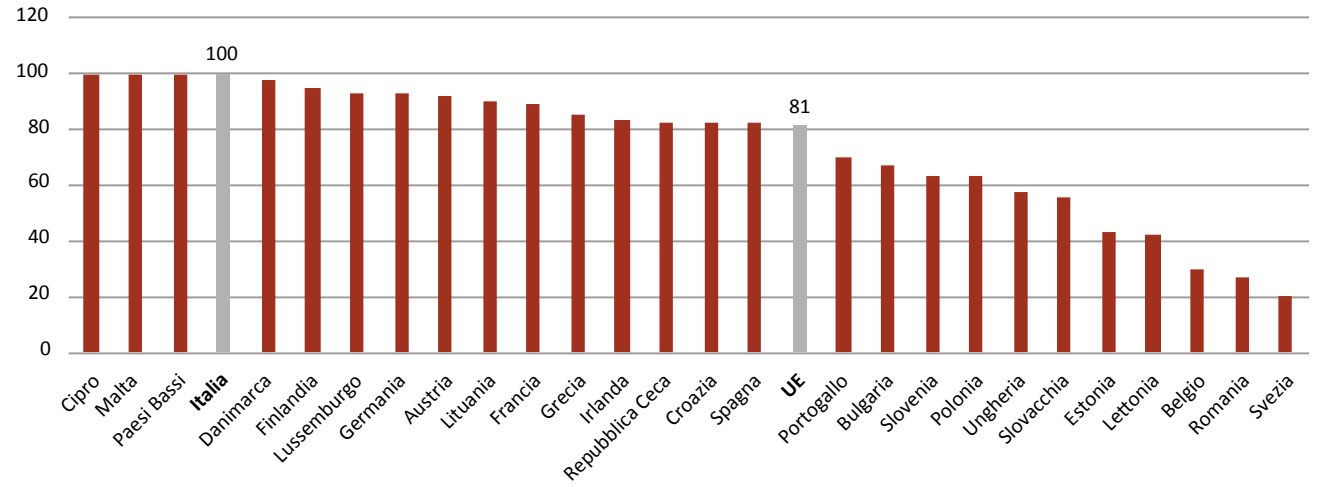


Fig. 4.12: Copertura 5G (%, 2022)

Fonte: Digital Scoreboard



che una frequenza bassa possiede la capacità di arrivare molto più lontano di una frequenza alta anche per la sua capacità di attraversare meglio gli ostacoli fisici, ma incontra il limite di riuscire a trasportare meno dati per unità di tempo mentre, al contrario, una frequenza bassa ha una portata molto inferiore ma ha la capacità di trasportare moltissimi dati per unità di tempo e che dunque le varie frequenze rispondono alle diverse esigenze che i vari use cases su reti 5G presentano, appaiono molto interessanti i dati relativi alla copertura 5G sulle frequenze 3,4-3,8 Ghz (Fig. 4.13). Sul punto il dato europeo si attesta al 41% con ben 15 paesi che registrano un dato inferiore alla media, mentre a primeggiare sono Finlandia, Italia e Danimarca con rispettivamente 84, 80 e 75% di copertura. Ciò dimostra quanto sia importante accelerare, per garantire l'effettiva possibilità di offrire e fruire dei servizi abilitati dalle reti 5G.

Fig. 4.13: Copertura 5G su frequenze 3,4-3,8 Ghz (%, 2022)

Fonte: Digital Scoreboard, 2022

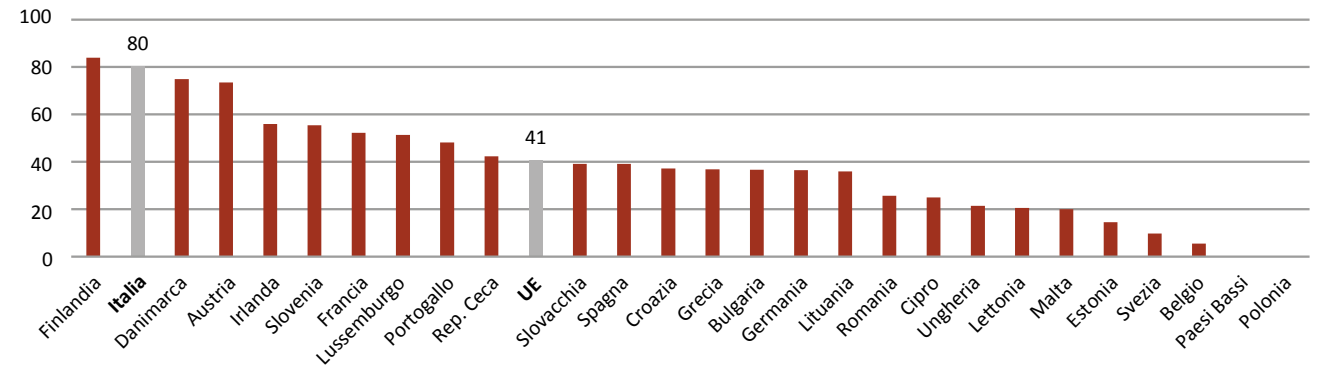


Fig. 4.14: Copertura 5G nelle aree rurali (%, 2022)

Fonte: Digital Scoreboard, 2022

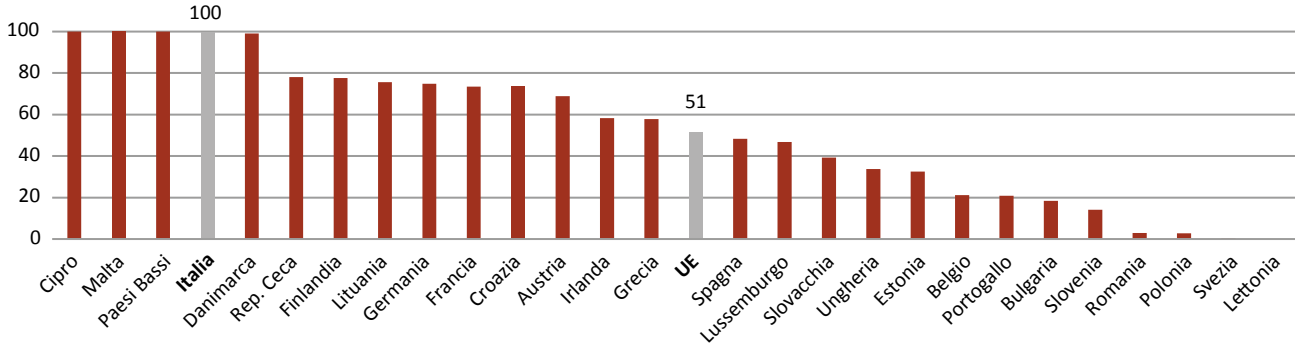


Fig. 4.15: Imprese che forniscono dispositivi portatili al proprio personale impiegato (%,2022)

Fonte: Digital Scoreboard, 2022

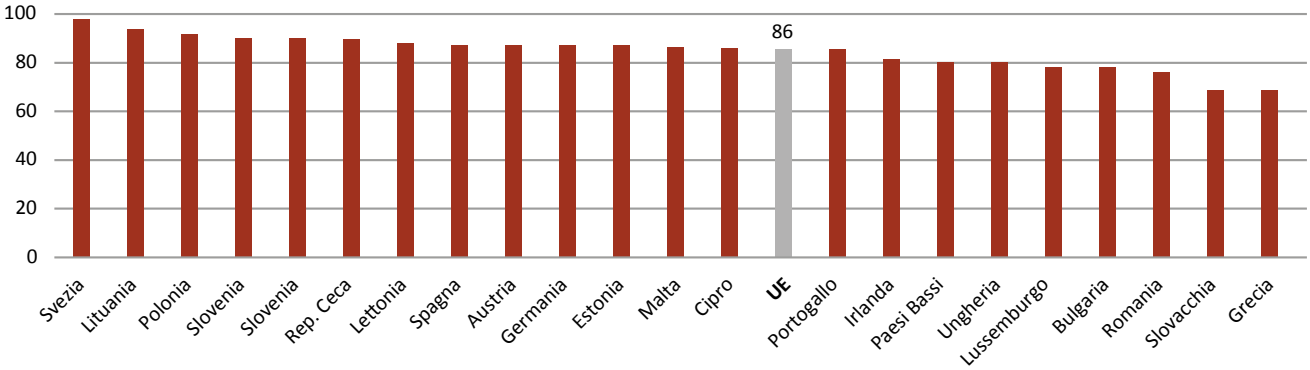
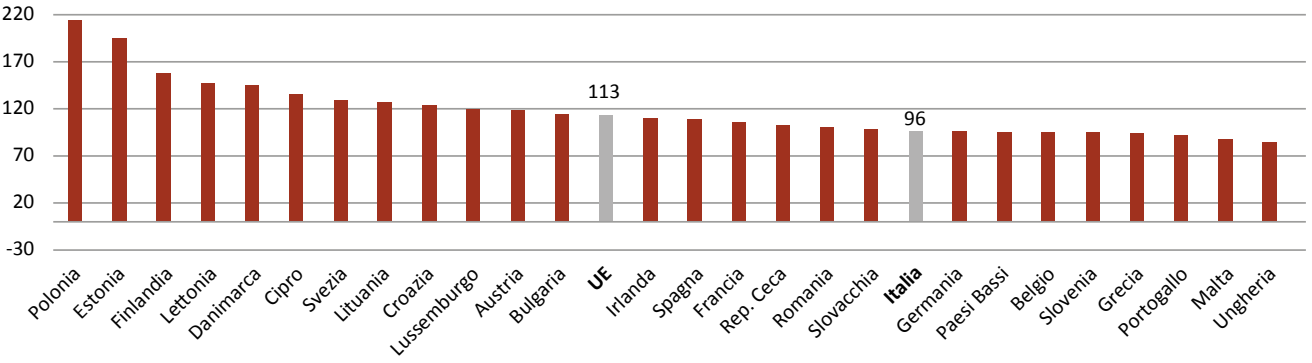


Fig. 4.16: Numero di SIM attive per 100 abitanti (2022)

Fonte: Digital Scoreboard, 2022



Rispetto alle aree rurali (Fig. 4.14), a primeggiare sono Italia, Cipro, Malta e Paesi Bassi dove la copertura appare completata, mentre il dato europeo si ferma al 51%.
L'analisi svolta dimostra la centralità rivestita dalle reti mobili che, soprattutto nell'ultimo triennio, complice la pandemia, hanno rappresentato uno strumento indispensabile anche per garantire la continuità delle attività del personale impiegato nelle aziende. A tale riguardo, è significativo che nel 2022 **l'86% delle imprese UE abbia fornito ai propri dipendenti dispositivi portatili** (Fig. 4.15).
L'interesse per la connettività mobile appare decisamente rilevante ove si consideri che a livello europeo sono ben 113 le SIM attive ogni 100 abitanti e che si registrano picchi del doppio in Polonia dove il numero sale a 215, seguita da Estonia e Finlandia con rispettivamente 195 e 158 SIM attive ogni 100 abitanti (Fig. 4.16).

icom
istituto per la competitività

CAPITOLO 5

IL DIGITALE NELLE POLITICHE DELL'UNIONE EUROPEA

5.1. DAGLI OBIETTIVI DI CONNETTIVITÀ AL CONNECTIVITY PACKAGE

Considerato che la diffusa disponibilità di reti performanti costituisce una condizione indispensabile per traguardare la transizione digitale, l'UE ha nel tempo fissato obiettivi di connettività sempre più ambiziosi, da ultimo con la Comunicazione *"Bussola digitale 2030: la via europea per il decennio digitale"* che ha punta, entro il 2030, ad una connettività di almeno 1 Gbps per tutte le famiglie europee e ad una copertura 5G in tutte le aree popolate.

In tale logica ed al fine di accelerare lo sviluppo delle reti, lo scorso 23 febbraio la Commissione ha lanciato il **"Connectivity Package"** che si compone di una proposta di regolamento che fornirà nuove norme per consentire una diffusione più rapida, economica ed efficace delle reti Gigabit in tutta l'UE (**Gigabit Infrastructure Act**), un progetto di raccomandazione sulla connettività Gigabit teso a fornire orientamenti alle autorità nazionali di regolamentazione sulle condizioni di accesso alle reti di telecomunicazione degli operatori che detengono un significativo potere di mercato, al fine di incentivare un più rapido abbandono delle tecnologie preesistenti e una diffusione accelerata delle reti Gigabit ed una consultazione esplorativa sul futuro del settore della connettività e delle relative infrastrutture per raccogliere opinioni sul modo in cui l'aumento della domanda di connettività e i progressi tecnologici potrebbero incidere sulle esigenze e sugli sviluppi futuri.

Il *Gigabit Infrastructure Act*, in particolare, partendo dalla constatazione della massiccia diffusione e penetrazione di reti a 30 Mbps e della loro inidoneità a supportare le nuove tecnologie digitali, si prefigge l'obiettivo di mettere in campo azioni tese ad accelerare lo sviluppo della banda ultra larga fissa e mobile e a ridurne i relativi costi di realizzazione.

A tal fine, la proposta di regolamento disciplina l'accesso alle infrastrutture fisiche esistenti (artt. 3-4), fissando gli elementi da considerare per la determinazione dei prezzi di accesso e individuando dettagliatamente le condizioni che giustificano un diniego, opponibile da parte di un soggetto pubblico o privato, a fronte di una richiesta di accesso (diniego da manifestare per iscritto con puntuali giustificazioni entro 1 mese dalla richiesta di accesso). Le ipotesi considerate, in particolare, consistono: nell'inidoneità tecnica dell'infrastruttura fisica ad accogliere elementi di rete ad altissima capacità, nella carenza di spazio in considerazione anche di future esigenze del fornitore di accesso sufficientemente dimostrate, nella sussistenza di criticità legate alla sicurezza e salute pubblica, preoccupazioni per l'integrità e la sicurezza di qualsiasi rete, in particolare delle infrastrutture critiche nazionali, il rischio di gravi interferenze dei servizi di comunicazione elettronica con la fornitura di altri servizi sulla stessa infrastruttura fisica o la disponibilità di validi mezzi alternativi di accesso fisico all'ingrosso alle reti di alle reti di comunicazione elettronica fornite dallo stesso operatore di rete e adatte alla fornitura di reti ad altissima capacità.

Nella logica di accelerare lo sviluppo delle reti, la proposta riconosce, da un lato, il diritto degli operatori di negoziare accordi sul coordinamento delle opere civili (art. 5), compresa la ripartizione dei costi e, dall'altro, fissa il dovere degli operatori che realizzino reti con fondi totalmente o parzialmente pubblici di soddisfare qualsiasi ragionevole richiesta scritta di coordinare tali opere civili a condizioni trasparenti e non discriminatorie, presentata dagli operatori al fine di installare elementi di reti ad altissima capacità o strutture associate (a patto che non vi siano costi aggiuntivi non recuperabili, l'operatore promotore dell'infrastruttura mantenga il coordinamento dell'opera e la richiesta di coordinamento sia presentata prima possibile, almeno 2 mesi prima della presentazione del progetto alle autorità nel caso sia necessario il rilascio di un'autorizzazione). Agli Stati spetta individuare le opere escluse perché rappresentanti

infrastrutture critiche o perché sottoposte a limitazioni specifiche. Molto rilevante la previsione secondo cui nel caso in cui la richiesta di coordinamento non risulti accoglibile (art. 6), l'operatore che realizza l'infrastruttura è chiamato a predisporre una capacità sufficiente a far fronte alle possibili future necessità di accesso di operatori terzi.

La stessa proposta si occupa poi della questione relativa alle procedure di rilascio dei permessi (art. 7) disponendo che gli Stati membri assicurino procedure uniformi su tutto il territorio nazionale, riconoscendo il diritto a ciascun operatore di inviare digitalmente le richieste di autorizzazione attraverso un unico punto che ne consenta anche il monitoraggio (da collegare a un unico punto di accesso nazionale) e fissando tempistiche stringenti entro cui pronunciarsi (15 gg per segnalare l'eventuale incompletezza della richiesta, pena la considerazione della domanda come completa, e 4 mesi dalla richiesta) sebbene siano previsti margini per prevedere tempistiche superiori con la precisazione che *"any extension shall be the shortest possible"*. Sul punto, qualsiasi rifiuto, ancora una volta, dovrà essere giustificato sulla scorta di criteri obiettivi, trasparenti e secondo i principi di non discriminazione e proporzionalità. Al mancato rispetto di questi requisiti, qualsiasi operatore che abbia sofferto un danno derivante da una mancata conformità ai termini specificamente indicati ha il diritto a ricevere un adeguato risarcimento, in base alla normativa nazionale.

Quanto alla fibra (art. 8), la proposta di regolamento riconosce il diritto di ciascun operatore di installare la propria rete a proprie spese fino al punto di accesso e di accedere all'infrastruttura esistente se la duplicazione è tecnicamente impossibile o economicamente inefficiente.

All'operatore è altresì riconosciuto il diritto di terminare la propria rete presso i locali dell'abbonato, previo accordo di quest'ultimo, a condizione di ridurre al minimo l'impatto sulla proprietà privata di terzi (art. 9). Queste ultime norme potrebbero essere determinanti per la realizzazione di infrastrutture fisiche all'interno degli edifici, soprattutto se di nuova costruzione. In questo modo, si andrebbero a ridurre i costi, anche in virtù del fatto che si eviterebbero interventi funzionali all'implementazione successiva di questo tipo di infrastrutture. Infatti, la proposta prevede che tutti gli edifici di nuova costruzione o soggetti a ristrutturazioni particolarmente significative, per le quali il permesso di costruire sia stato richiesto dopo un anno dall'eventuale entrata in vigore del Regolamento, dovranno essere dotati di infrastrutture per le reti ad alta velocità; faranno eccezione, ad esempio, i monumenti, gli edifici storici, gli edifici utilizzati per scopi militari o legati alla sicurezza nazionale, in base a quanto previsto dalle normative nazionali. Inoltre, anche per stimolare tale pratica, è stato previsto il rilascio di un'apposita certificazione ("fiber ready") per l'edificio che avrà raggiunto questi standard tecnici appositamente richiesti dall'art. 8 (4).

Per risolvere eventuali controversie in materia (artt. 11-12), la proposta ammette la possibilità di rivolgersi – oltre che direttamente all'Autorità giudiziaria – a una o più Autorità indipendenti a livello nazionale, non escludendo l'ipotesi che si possa attribuire una simile prerogativa anche ad Autorità indipendenti già esistenti negli Stati Membri, purché esse possano esercitare i rispettivi poteri in maniera imparziale, trasparente e tempestiva. Ovviamente, la proposta prescrive che tali Autorità devono essere dotate di adeguate risorse tecniche, finanziarie e umane per svolgere i compiti assegnatigli. In ogni caso, ciascuno Stato membro dovrà notificare alla Commissione l'individuazione di poteri e responsabilità in capo a una o più Autorità indipendenti, entro la data di entrata in vigore del Regolamento, mentre successive modifiche le dovranno essere sottoposte prima che siano produttive di effetti.

Per quanto concerne l'aspetto sanzionatorio (art. 14), è stato previsto che gli Stati Membri stabiliscano norme relative alle sanzioni – penali ed extra-penali

– applicabili alle violazioni del presente Regolamento e di qualsiasi decisione vincolante adottata dalle Autorità competenti ex art. 12. Tali sanzioni dovranno essere adeguate, efficaci, proporzionate e dissuasive. Inoltre, è richiesto ai singoli Stati di prevedere norme ad hoc per garantire un adeguato risarcimento finanziario per le persone che possano aver subito danni derivanti dall'esercizio dei diritti previsti dal Regolamento.

Il dossier sulla proposta della Commissione è stato attribuito, in Parlamento europeo, alla Commissione per l'Industria, la Ricerca e l'Energia (ITRE) che il 29 settembre scorso ha adottato la propria posizione introducendo una serie di proposte di modifica tra cui si segnala, per importanza: a) l'esplicito riferimento, in una logica di garanzia del principio di neutralità tecnologica, alla necessità di implementare reti ad altissima velocità con performance almeno equivalenti a quelle del 5G; b) l'inclusione delle autorità pubbliche, accanto ai soggetti privati, all'interno delle disposizioni relative al coordinamento delle opere civili; c) ferma restando la scelta dello strumento regolamentare, il riconoscimento della possibilità, per gli Stati membri, di operare scelte più ambiziose rispetto ai requisiti minimi richiesti (ad es. fissando termini più stringenti per il rilascio delle prescritte autorizzazioni oppure estendendo le previsioni sull'accesso alle infrastrutture fisiche esistenti agli edifici di proprietà privata); d) la precisazione circa la necessità che il prezzo di accesso ad infrastrutture esistenti garantisca un equo ritorno degli investimenti, non sia discriminatorio e rifletta le condizioni di mercato ed il modello di business; e) la fissazione delle condizioni in presenza delle quali è possibile per l'operatore, nella logica di garantire il superamento del gap esistente tra aree rurali ed urbane, richiedere l'accesso ad edifici commerciali esistenti (nello specifico, quando non ci sono reti VHCN nell'area e non sia previsto alcun piano di implementazione entro un anno dalla richiesta dell'operatore, non ci sono nell'area infrastrutture pubbliche o private esistenti in grado di ospitare elementi di reti VHCN, oppure l'operatore non sia riuscito ad ottenere aiuti di Stato per coprire quell'area o a trovare un co-investitore per sviluppare un'infrastruttura fisica); f) l'assegnazione alla Commissione, unitamente al BEREC, del compito di definire delle linee guida sull'accesso alle infrastrutture fisiche con la precisazione di considerare, nel fissare i prezzi, le caratteristiche ed modelli di business degli operatori nonché di determinare prezzi diversificati a seconda della tipologia di infrastruttura; g) il riconoscimento agli Stati membri della facoltà di chiedere informazioni sulle infrastrutture fisiche esistenti e sullo stato di occupazione delle medesime; h) la riduzione da 4 a 3 mesi (prolungabili per non più di altri 3 mesi in casi eccezionali e motivati) del termine assegnato alle autorità per concedere le autorizzazioni (nel caso di inutile decorso è previsto il formarsi del silenzio assenso); i) l'individuazione, ad opera degli Stati membri, di un singolo ente responsabile di coordinare le procedure di rilascio delle autorizzazioni.

Se questo è lo stato dell'arte della procedura di adozione del GIA, il 10 ottobre scorso è stata pubblicata dalla Commissione europea la sintesi della consultazione pubblica esplorativa sul futuro della connettività cui hanno preso parte **108 imprese, tra ECN provider e OTT**, associazioni di imprese, cittadini sia europei che extraeuropei, organizzazioni non governative, istituti di ricerca, organizzazioni di consumatori e **Autorità, di diversi settori e ambiti locali.** Per quanto concerne le tecnologie e lo **sviluppo del mercato della connettività**, è emerso dalla consultazione che le tecnologie maggiormente impattanti per la "connettività" saranno virtualizzazione della rete, intelligenza artificiale (a tale riguardo si segnala l'importanza di incentivare gli investimenti su tecnologie NaaS/Slicing di rete e sull'interfaccia di programmazione delle applicazioni (API) in quanto necessarie allo sviluppo dell'IA), reti aperte, edge cloud, tecnologie satellitari in orbita bassa (per consentire la diffusione di internet nelle aree

difficilmente raggiungibili in una logica di superamento del digital divide). Viene affrontato anche il tema del **traffico dati** mediante individuazione dei principali attori dell'ecosistema digitale e quello degli investimenti sostenuti e programmati. Particolarmente rilevante, in considerazione dell'ampio dibattito sul tema, quanto emerso in ambito **fair share**. In particolare, nella consultazione è emersa la contrapposizione tra quanti si sono mostrati contrati alla luce di considerazioni economiche, tecniche e di neutralità della rete oltre che dei possibili impatti sul mercato dei contenuti e quanti, al contrario, ritengono che il meccanismo di pagamento ipotizzato avrebbe un impatto positivo sull'intero ecosistema in quanto verrebbero incentivati gli investimenti in tecnologie più efficienti. Rispetto, invece, al tema della **gestione dello spettro radio**, sebbene con la precisazione di conservare quella flessibilità necessaria a tener conto delle specifiche esigenze nazionali, è emerso, a livello generale, un diffuso favor verso una maggiore integrazione a livello comunitario dello spettro partendo dall'idea che un approccio armonizzato possa produrre benefici per il mercato. In relazione, infine, al **Servizio Universale**, è emersa un'ampia gamma di posizioni anche se appare piuttosto radicata la preferenza per strumenti di inclusione sociale alternativi al servizio universale come i voucher sociali o di connettività.

Se questi sono gli obiettivi, molto complesso il percorso per centrarli. La Commissione, infatti, il 13 luglio scorso ha pubblicato lo studio "I*nvestment and funding needs for the Digital Decade connectivity targets"* realizzato da WIK Consult nel quale viene fatto il punto sullo stato dell'arte e sulle risorse necessarie a centrare gli obiettivi di connettività fissati per il 2030. Tale studio, nello specifico, se da un lato evidenzia come gli investimenti necessari per il deployment delle reti si stiano riducendo con l'avanzare della fase di implementazione, dall'altro, quantifica le risorse pubbliche e private necessarie per ultimare il deployment delle reti fisse e mobili. In particolare, per coprire il restante 30% delle famiglie con connettività Gigabit, è stimata in €114 miliardi, di cui circa €40 miliardi di finanziamenti pubblici, l'entità degli investimenti richiesti (con la possibilità di ridurre le cifre rispettivamente a €108 miliardi e €29 miliardi di sussidi pubblici nel caso in cui si faccia uso del 5G FWA nelle aree con meno di 30 ab/kmq) mentre sono stimati in €33,5 miliardi gli investimenti necessari per assicurare la copertura 5G SA. Il tutto per complessivi €148 miliardi di investimenti privati e €43 miliardi di sussidi pubblici se le reti fisse e mobili vengono sviluppate separatamente. Qualora, invece, le reti 5G ed FTTP fossero sviluppate congiuntamente, potrebbe realizzarsi una riduzione degli investimenti privati del 20% (che, dunque, passerebbero a €120 miliardi) e sarebbero necessari solo €33 miliardi di sussidi pubblici.

5.2. LA CORNICE NORMATIVA SUI DATI: DALLA STRATEGIA AL DATA GOVERNANCE ACT E AL DATA ACT

Le nuove tecnologie vivono e si nutrono di dati che dunque hanno assunto una centralità senza precedenti nelle politiche europee tese ad assicurare che la raccolta, il trattamento e la conservazione degli stessi avvenga nel pieno rispetto dei diritti fondamentali e a trovare un giusto equilibrio tra esigenze di apertura e necessità di tutela.

Tralasciando l'analisi del Regolamento n. 679/2016, che rappresenta il punto di riferimento imprescindibile e, ormai, modello globale per la tutela dei dati personali, il punto di partenza da cui partire per l'analisi dei principali interventi in materia che si sono succeduti negli ultimi due anni è rappresentato dalla **Strategia europea per i dati** del febbraio 2020 che, 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, mirava a 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 evidenziava la necessità di affrontare e risolvere una serie di criticità riguardanti disponibilità dei dati, squilibri nel potere di mercato nella fornitura di servizi cloud e infrastrutture di dati, ma anche in relazione ad accesso ed uso dei dati, interoperabilità e qualità, governance, infrastrutture e tecnologie, abilitazione degli individui a esercitare i loro diritti, competenze e alfabetizzazione, an che in chiave di 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 ad 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 ospitarli, elaborarli e utilizzarli, 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).

In attuazione della strategia, il 25 novembre 2020 la Commissione ha pubblicato la propria proposta di regolamento relativo alla governance europea dei dati culminata nell'adozione, il 30 maggio scorso, del **Regolamento n. 2022/868 (Data Governance Act).** Si tratta di un regolamento molto importante che, secondo la logica di armonizzazione massima che la Commissione europea ha fatto propria nel costruire l'ecosistema normativo per il digitale, istituisce un meccanismo per il riutilizzo di determinate categorie di dati protetti detenuti da enti pubblici. Ci si riferisce, in particolare, ad un riutilizzo 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, riservatezza statistica e riservatezza commerciale) rispetto al quale vengono individuate una serie di condizioni armonizzate di base che ne consentano l'effettiva realizzazione. Nello specifico, il regolamento vieta la stipula di accordi di esclusiva che abbiano per oggetto o per effetto quello di impedire o limitare la disponibilità di dati per il riutilizzo da parte di entità diverse dalle parti coinvolte nell'accordo e disciplina le modalità concrete del riutilizzo, prescrivendo agli enti pubblici che lo consentono, da un lato di attrezzarsi in maniera da garantire la piena tutela della protezione dei dati, della privacy e della riservatezza attraverso l'anonimizzazione dei dati personali e l'aggregazione di dati ed informazioni commerciali riservate e, dall'altro, di predisporre un ambiente di trattamento fisico o digitale (nel caso di accesso da remoto) sicuro, fornito o controllato dall'ente pubblico. Gli enti pubblici che consentono il riutilizzo possono, da regolamento, imporre tariffe – il cui ammontare deve tenere conto di una serie di costi necessari individuati dallo stesso regolamento – che devono essere trasparenti, non discriminatorie, proporzionate, oggettivamente giustificate e non limitanti la concorrenza, ferma restando comunque la possibilità per gli stessi enti di prevedere una tariffa ridotta o nulla, in particolare per le PMI e le start-up, la società civile e gli istituti di istruzione per incentivare il riutilizzo dei dati per fini non commerciali. Il termine entro cui evadere le richieste di riutilizzo è fissato in 20 gg. prorogabile al massimo di 30 gg. nel caso di richieste eccezionalmente cospicue e complesse (è sancito il diritto al ricorso per il soggetto richiedente).

Dal punto di vista della governance e dell'enforcement del regolamento, gli Stati membri sono chiamati a designare uno o più organismi competenti (nuovi o già esistenti) deputati ad assistere gli enti pubblici che concedono o rifiutano l'accesso al riutilizzo ed ad istituire, presso un ente nuovo o uno già esistente, uno **sportello unico** – che può essere collegato a sportelli settoriali, regionali o locali – competente per il ricevimento delle richieste di informazioni e delle richieste di riutilizzo. Tale sportello, nello specifico, deve mettere a disposizione per via elettronica un elenco consultabile delle risorse di dati disponibili, tra cui, se del caso, quelle disponibili presso gli sportelli settoriali, regionali e locali, contenente informazioni pertinenti che descrivono i dati disponibili, compresi almeno il formato e le dimensioni dei dati e le condizioni per il loro riutilizzo con possibilità di prevedere un canale di informazione distinto, semplificato e ben documentato per le PMI e le start-up.

Lo stesso regolamento fissa, al Capo III, 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 a ciò 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), prevede un **regime di notifica** per i fornitori di servizi di condivisione dei dati che ha ad oggetto una serie nutrita di informazioni che lo stesso regolamento indica e, fissando le condizioni per la fornitura di servizi di intermediazione dei dati e dando particolare enfasi alle tematiche dell'interoperabilità, della sicurezza e della tutela dei diritti degli interessati. Ai fini della ricezione delle suddette notifiche e l'espletamento dell'attività di monitoraggio, il regolamento prescrive agli Stati membri di individuare autorità competenti a livello nazionale.

Tema particolarmente interessante quello dell'**altruismo dei dati** e, dunque, i dati messi a disposizione su base volontaria da parte di individui o imprese per il bene comune, rispetto al quale è riconosciuta la possibilità per le organizzazioni che lo intendono praticare di registrarsi, confluendo, qualora in possesso di determinati requisiti, nei registri pubblici previsti a livello nazionale ed europeo. Agli Stati membri, spettano la designazione delle Autorità competenti per la registrazione di organizzazioni per l'altruismo dei dati e l'attività di monitoraggio della conformità. La Commissione è invece chiamata ad adottare atti di esecuzione per l'istituzione e l'elaborazione di un modulo europeo di consenso all'altruismo dei dati (previa consultazione del comitato europeo per la protezione dei dati, tenendo conto del parere del comitato europeo per l'innovazione in materia di dati e coinvolgendo opportunamente i pertinenti portatori di interessi), al fine di facilitare la raccolta dati su tali basi.

Dal punto di vista dell'assetto istituzionale, il regolamento ha istituito 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 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.

In un contesto che vede proliferare tecnologie che si nutrono di enormi moli di dati, ad integrazione del Data Governance Act, il 23 febbraio scorso la Commissione ha lanciato la proposta di **Data Act**, la seconda iniziativa in attuazione della descritta strategia, su cui Parlamento e Consiglio hanno raggiunto un accordo politico nel giugno scorso. Il Data Act, in particolare, mira a stabilire una serie di regole comuni che disciplinino la condivisione dei dati, sia personali che industriali/commerciali ed il loro riutilizzo in determinati settori.

Il regolamento proposto, in particolare, nella logica di favorire la circolazione dei dati, al Capo II disciplina la **condivisione dei dati da impresa a consumatore e da impresa ad impresa,** prescrivendo che la progettazione e fabbricazione siano tali da rendere, per impostazione predefinita, accessibili i dati generati in modo facile e sicuro (e ove opportuno anche diretto). A tale obbligo si ricollega quello di fornire, prima di concludere un contratto di acquisto, affitto o noleggio di un prodotto o di un servizio correlato, la fornitura all'utente, in modo chiaro e comprensibile, di una serie di informazioni tra cui spiccano, per rilevanza, le indicazioni concernenti le modalità attraverso le quali l'utente può chiedere che i dati siano condivisi con terzi. Il diritto degli utenti di accedere ai dati generati dall'uso di prodotti o servizi correlati e di utilizzarli è puntualmente declinato all'art. 4 che prescrive, tra l'altro, al titolare dei dati la messa a disposizione tempestiva e gratuita (e in modo continuo ed in tempo reale ove applicabile) dei dati prodotti all'utente e subordina l'utilizzo di dati personali da parte del titolare dei dati alla previa conclusione di un accordo contrattuale con l'utente.

Ampio spazio ed attenzione è riservato, da un lato, al **diritto di condividere i dati con terzi** (art. 5) che vede dettare specifici divieti a carico dei fornitori di servizi di piattaforma di base designati gatekeeper a norma del DMA nella logica di scongiurare rischi di condizionamento o alterazione delle scelte dell'utente; dall'altro, agli **obblighi dei terzi che ricevono dati su richiesta dell'utente**, chiamati, in particolare, a trattare i dati messi a propria disposizione solo per le finalità e alle condizioni concordate con l'utente e fatti salvi i diritti dell'interessato per quanto riguarda i dati personali e a cancellare i dati quando non sono più necessari per la finalità concordata. A ciò si aggiunge il divieto di condizionare o manipolare l'autonomia dell'utente, utilizzare i dati per profilazione di persone fisiche, mettere i dati a disposizione di terzi (a meno che non sia necessario per offrire il servizio all'utente), fornire i dati che riceve a disposizione di un'impresa che fornisce servizi di piattaforma di base per i quali uno o più di tali servizi sono stati designati come *gatekeeper*, utilizzare i dati per sviluppare un prodotto in concorrenza con il prodotto da cui provengono i dati consultati (né condividere i dati con un altro terzo a tal fine) ed impedire all'utente, anche attraverso impegni contrattuali, di mettere i dati che riceve a disposizione di altre parti.

Il Capo V invece istituisce un quadro armonizzato per l'utilizzo, da parte degli enti pubblici e delle istituzioni, agenzie e organismi dell'Unione, dei dati detenuti dalle imprese, in situazioni in cui vi sia una necessità eccezionale dei dati richiesti. Nello specifico, si ritiene sussistente una situazione di necessità eccezionale quando i dati richiesti siano necessari per rispondere a un'emergenza pubblica, per prevenire un'emergenza pubblica o per contribuire alla ripresa dopo un'emergenza pubblica (se la richiesta è limitata nella durata e nella portata) e per lo svolgimento di un compito specifico di interesse pubblico non altrimenti realizzabile, a patto che l'ente in questione non sia stato in grado di ottenere tali dati con mezzi alternativi, anche acquistandoli sul mercato ai prezzi di mercato oppure l'ottenimento dei dati in conformità della procedura stabilita nel presente capo possa ridurre considerevolmente l'onere amministrativo per i titolari dei dati o per altre imprese. A fronte di una richiesta ai sensi del presente Capo – i cui contenuti sono dettagliatamente fissati dallo stesso regolamento – è prescritto al titolare dei dati di fornire riscontro senza indebito ritardo, ferme restando le ipotesi in cui è possibile per il ricevente, opporre un rifiuto o richiedere una modifica della richiesta. Rispetto a tali ipotesi, non è previsto un compenso e, ove previsto, non deve eccedere i costi tecnici ed organizzativi sostenuti per dar seguito alla richiesta. Al di fuori di tali casi, è riconosciuto il diritto di un ente pubblico o un'istituzione, un'agenzia o un organismo dell'Unione di condividere i dati ricevuti con persone o organizzazioni al fine di svolgere

ricerche o analisi scientifiche, compatibili con la finalità per la quale sono stati richiesti i dati, o con istituti nazionali di statistica ed Eurostat per l'elaborazione di statistiche ufficiali.
Nella logica di tutela della concorrenza e della libertà di scelta dell'utente, viene puntualmente disciplinato il diritto passaggio da un fornitore di servizi di trattamento dei dati a un altro prevedendo l'abolizione graduale delle tariffe di passaggio e sono dettate previsioni specifiche tese a garantire l'interoperabilità.
Al fine di assicurare l'osservanza del regolamento e favorire la cooperazione sovranazionale, gli Stati Membri sono chiamati ad individuare una o più autorità nazionali competenti, nuove o già esistenti.
Se questi sono i principali elementi della proposta, Parlamento e Consiglio, dopo non poche difficoltà, nel giugno 2023 hanno trovato un accordo provvisorio (cui seguirà l'approvazione definitiva da parte di entrambe le istituzioni europee) su una serie di punti, tra cui si segnalano per importanza: a) la definizione del **campo di applicazione** del regolamento, nella logica di consentire a tutti gli utenti di dispositivi connessi, siano essi destinati ad un utilizzo privato che industriale, di accedere ai dati che vengono generati dai dispositivi nel corso del loro utilizzo e di poter operare un maggior controllo sui propri dati avendo maggior consapevolezza delle informazioni condivide con produttori e fornitori; b) la previsione di misure volte ad **impedire l'abuso degli squilibri contrattuali** nei contratti di condivisione dei dati; c) la garanzia di un livello adeguato di protezione dei **segreti commerciali** e dei diritti di proprietà intellettuale, accompagnato dalle relative garanzie contro eventuali comportamenti abusivi da parte dei titolari dei dati; d) l'individuazione di mezzi che consentono agli **enti pubblici**, alla Commissione, alla Banca centrale europea e agli organismi dell'Unione di accedere ai dati detenuti dal settore privato ed utilizzarli, ove necessario, in circostanze eccezionali come emergenze pubbliche quali inondazioni e incendi boschivi per svolgere un compito di interesse pubblico; e) l'adozione di misure tese a consentire ai clienti di **passare efficacemente** da un fornitore di servizi di trattamento dei dati a un altro e la previsione di ulteriori garanzie contro il trasferimento illecito di dati; f) la definizione di ulteriori orientamenti in merito al **compenso ragionevole** per le imprese per la messa a disposizione dei dati, nonché ad adeguati **meccanismi di risoluzione delle controversie**; g) la formulazione di chiarimenti circa l'**interazione** tra la normativa sui dati e la legislazione orizzontale e settoriale vigente, ad esempio il regolamento sulla governance dei dati e il regolamento generale sulla protezione dei dati (GDPR).

5.3. L'UE E LA SFIDA DELL'INTELLIGENZA ARTIFICIALE: L'AI ACT

L'IA rappresenta, come evidenziato nel cap. 2, una delle rivoluzioni tecnologiche a più elevato impatto per le strabilianti opportunità che essa offre a privati e pubbliche amministrazioni e per il contributo che può offrire all'Unione Europea e agli Stati membri quale leva di competitività nel contesto globale.
Alle enormi opportunità si accompagnano tuttavia una serie di questioni e temi nuovi da comprendere e governare che hanno spinto la Commissione europea, sin dal 2018, con la comunicazione "**IA per l'Europa**", ad avviare una serie di iniziative 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 per un "**regolamento del Parlamento europeo e del Consiglio che stabilisce norme armonizzate in materia di intelligenza artificiale e che modifica alcuni atti legislativi dell'Unione**" (AI Act), con il quale si istituisce un quadro di riferimento legale volto a normare il mercato dell'UE dell'IA.
Tale proposta, in particolare, si rivolge ai 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 ed ai fornitori ed utenti di sistemi di IA situati in un paese terzo, laddove l'output prodotto dal sistema sia utilizzato nell'UE, e persegue la finalità di accrescere la fiducia dei cittadini europei nell'IA.
Dal punto di vista metodologico, il regolamento proposto declina obblighi diversificati che seguono un approccio basato sul rischio, che distingue tra usi dell'IA che creano un rischio inaccettabile, un rischio elevato ed un rischio basso o minimo, da cui discendono evidentemente conseguenze diverse. Nello specifico, è previsto un divieto per le 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, 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 secondo procedure dettagliatamente descritte. Il regolamento a tale riguardo 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 evidenziando la necessità di utilizzare tali sistemi conformemente alle istruzioni per l'uso.
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 startup.
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.

A presidio dell'osservanza della disciplina contenuta nel regolamento, la proposta individua 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 startup e della loro sostenibilità economica.

L'*iter* normativo, ancora non concluso sebbene si trovi ormai alle battute finali, si è rivelato particolarmente complesso. Sin dalla presentazione della proposta della Commissione si è infatti acceso un ampio e complesso dibattito a livello internazionale che se da un lato ha espresso generale apprezzamento per la scelta di stabilire un quadro armonizzato nel campo dell'IA e di aderire ad un approccio basato sul rischio focalizzato sulla tutela dei diritti e degli interessi degli individui, dall'altro ha espresso qualche perplessità di carattere generale in merito alla capacità, dello strumento prescelto, di stare al passo con la rapidità dell'innovazione, nonché, nello specifico, in merito alla insufficiente determinatezza di alcuni obblighi, alla necessità di riservare maggior attenzione alle possibili applicazioni ed usi delle tecnologie IA (piuttosto che alle tecnologie in sé) e valutare l'entità dei costi gravanti soprattutto sulle PMI e le startup oltre all'impatto della disciplina proposta su concorrenza ed innovazione.

Il 6 dicembre 2022 il Consiglio ha adottato il proprio orientamento generale formulando una serie di importanti proposte di modifica tra cui si segnalano, per importanza, l'esclusione dal campo di applicazione della legge sull'IA degli scopi di sicurezza nazionale, difesa militare e autorità di contrasto, l'estensione ai privati del divieto di utilizzare l'IA per il social scoring, una più puntuale definizione dei requisiti di IA ad alto rischio con particolare focalizzazione sulla capacità degli stessi di causare gravi violazioni dei diritti fondamentali o altri rischi significativi, l'inserimento di nuove disposizioni tese a considerare le situazioni in cui i sistemi di IA possono essere utilizzati per scopi diversi (IA per scopi generali), l'inserimento di nuove disposizioni per accrescere la trasparenza e accogliere i reclami degli utenti, l'introduzione di importanti modifiche alle disposizioni riguardanti le misure a sostegno dell'innovazione (es. sandbox normative).

Anche il Parlamento ha adottato la propria posizione (nel giugno 2023) introducendo anch'esso modifiche sostanziali al testo proposto dalla Commissione, tra cui la modifica dell'elenco dei sistemi di intelligenza artificiale vietati nell'UE al fine di includervi i sistemi di identificazione biometrica nell'UE sia per l'uso in tempo reale che ex post (tranne in casi di criminalità grave e previa autorizzazione giudiziaria per l'uso ex post) e non solo per l'uso in tempo reale come proposto da parte della Commissione. Il Parlamento, in particolare, ha proposto di vietare tutti i sistemi di categorizzazione biometrica che utilizzano caratteristiche sensibili, sistemi di polizia predittiva, sistemi di riconoscimento delle emozioni e sistemi di intelligenza artificiale che utilizzano lo scraping indiscriminato di dati biometrici dai social media o filmati CCTV per creare database di riconoscimento facciale.

Rispetto invece ai sistemi ad alto rischio, mentre la Commissione ha proposto di classificare automaticamente come ad alto rischio tutti i sistemi che rientrano in determinate aree o casi d'uso, il Parlamento ha introdotto un correttivo proponendo l'inserimento di un requisito aggiuntivo, ossia la verifica che i sistemi presentino un "rischio significativo" per essere considerati ad alto rischio e la previsione di un obbligo

di verifica in capo a coloro che implementano un sistema ad alto rischio nell'UE circa l'impatto sui diritti fondamentali, compresa una consultazione con l'autorità competente e le parti interessate.
Per i sistemi di IA di uso generale, tra i quali rientrano i modelli fondazionali alla base dell'IA generativa, inizialmente fuori dal testo proposto dalla Commissione, il Parlamento ha sancito l'obbligo di garantire una solida protezione dei diritti fondamentali, della salute, della sicurezza, dell'ambiente, della democrazia e dello Stato di diritto, mentre con riferimento ai modelli di IA generativa (come Chat GPT) che utilizzano modelli linguistici di grandi dimensioni per generare arte, musica e altri contenuti, ha delineato rigorosi obblighi di trasparenza.
Con riguardo al modello di governance, il Parlamento ha proposto un rafforzamento delle competenze delle autorità nazionali e l'istituzione di un Ufficio IA, un nuovo organismo dell'UE per sostenere l'applicazione armonizzata della legge sull'IA, fornire orientamenti e coordinare indagini transfrontaliere congiunte.
Nella logica di sostenere l'innovazione, il Parlamento concorda che le attività di ricerca e lo sviluppo di componenti IA gratuiti e open source siano in gran parte esentati dal rispetto delle norme della legge sull'IA.
Attualmente sono in corso i triloghi tra i legislatori UE che dovrebbero concludersi prima della fine dell'anno con un accordo.

5.4. L'EVOLUZIONE DEL REGOLAMENTO SULL'IDENTITÀ DIGITALE

Nel tentativo di diventare leader nella trasformazione digitale, l'UE si trova a fronteggiare una serie di sfide tra cui quella dell'identità digitale che presenta un'elevata complessità comprendendo non solo innovazione tecnologica, ma anche scelte politiche e normative, indispensabili per creare un sistema di identificazione digitale fluido, efficiente e sicuro. Quando si parla di *digital identity* non si può infatti prescindere da alcune esigenze irrinunciabili, come garantire la confidenzialità della comunicazione e far in modo che non sia alterata da soggetti non autorizzati, assicurarsi che le credenziali siano gestite da un ente affidabile ed assicurare un adeguato livello di fiducia da parte degli utenti.
Partendo da tali considerazioni e perseguendo l'obiettivo di creare un'identità digitale europea, nelle conclusioni del 2 ottobre 2020, il Consiglio europeo ha richiesto la revisione del quadro eIDAS invitando la Commissione a presentare una proposta, entro la metà del 2021, su una firma digitale interoperabile. Inoltre, nell'ambito della Bussola Digitale per il 2030 che, come noto, ha individuato la digitalizzazione dei servizi pubblici come uno dei punti cardinali insieme a competenze, trasformazione digitale delle imprese e sviluppo di infrastrutture digitali sicure e sostenibili, fissando come obiettivi specifici il 100% dei principali servizi pubblici online, il 100% dei cittadini che hanno accesso alle cartelle cliniche e l'80% dei cittadini che utilizzano l'ID digitale, il 3 giugno del 2021 la Commissione ha pubblicato una raccomandazione avente ad oggetto un **pacchetto di strumenti comuni** dell'Unione per un approccio coordinato verso un quadro europeo relativo a un'identità digitale e una **proposta di regolamento** che modifichi quanto previsto dall'eIDAS, istituendo un quadro normativo per la creazione di uno strumento europeo di identità digitale armonizzato, basato sul concetto di portafoglio europeo di identità digitale "EUDI wallet".
Quest'ultima punta a offrire portafogli digitali e personali agli utenti, che consentano un accesso sicuro e semplice a diversi servizi, sia pubblici che privati. Inoltre, si mira a creare un nuovo servizio fiduciario qualificato per l'attestazione di attributi legati all'identità quali l'indirizzo, l'età, il sesso, lo stato civile, il nucleo familiare, la nazionalità, le qualifiche e i titoli professionali e di studio, le patenti e altre licenze o

permessi, i dati di pagamento, che possono essere offerti, condivisi e scambiati a livello transfrontaliero in piena sicurezza, nel rispetto della protezione dei dati personali. L'obiettivo di fondo è quello di rispondere alle dinamiche dei mercati e agli sviluppi tecnologici – attraverso la regolamentazione di tre nuovi servizi fiduciari qualificati inerenti: l'archiviazione elettronica di documenti elettronici, la registrazione di dati elettronici in un registro elettronico e la gestione di dispositivi per la creazione di firme elettroniche e sigilli elettronici a distanza – nonché garantire un approccio armonizzato alla sicurezza, sia per i cittadini che si affidano a un'identità digitale europea che li rappresenti adeguatamente online, sia per i fornitori di servizi digitali, i quali potranno fare pieno affidamento su soluzioni di identità digitale indipendentemente dal luogo in cui queste vengono emesse. Tale obiettivo viene perseguito mediante il passaggio da soluzioni nazionali di identità digitale alla fornitura di attestati elettronici di attributi che siano validi a livello europeo.

Analizzando le modifiche proposte dalla Commissione, il Regolamento inserisce alcuni articoli che: a) prescrivono a ciascuno Stato membro di rilasciare un Portafoglio Europeo di Identità Digitale entro 12 mesi dall'entrata in vigore del Regolamento; b) individuano le attività consentite agli utenti (richiedere e ottenere, conservare, selezionare, combinare e condividere in modo sicuro, trasparente e tracciabile, i dati giuridici di identificazione personale e l'attestazione elettronica degli attributi necessari per l'autenticazione online e offline, al fine di utilizzare servizi pubblici e privati online, oltre che firmare mediante firma elettronica qualificata); c) definiscono i requisiti dei Portafogli di Identità Digitale (come la previsione di un'interfaccia comune e di un elevato livello di sicurezza, la garanzia di un'identificazione univoca della persona fisica o giuridica, l'impossibilità per i fornitori di servizi fiduciari che forniscono attestati qualificati di ricevere informazioni sull'utilizzo di tali attributi, nonché la presenza di un meccanismo per assicurare che la parte facente affidamento sia in grado di autenticare l'utente e ricevere gli attestati elettronici di attributi); d) prescrivono agli Stati Membri di predisporre meccanismi di convalida per i Portafogli Europei di Identità Digitale, al fine di verificare l'autenticità degli attestati di attributi e dei dati di identificazione personale attribuiti; e) stabiliscono che i Portafogli Europei di Identità Digitale siano emessi nell'ambito di un regime di identificazione elettronica notificato il cui livello di garanzia sia "elevato" e gratuito per le persone fisiche; f) danno all'utente il pieno controllo del Portafoglio di Identità Digitale, vietando la raccolta di informazioni non necessarie per la prestazione dei servizi del portafoglio e prescrivendo che i dati personali relativi alla fornitura dei portafogli europei di identità digitale siano tenuti fisicamente e logicamente separati dagli altri dati detenuti; g) prescrivono agli Stati Membri di attuare un meccanismo comune per l'autenticazione delle parti facenti affidamento sul servizio; h) conferiscono alla Commissione il potere di stabilire un elenco di standard per la certificazione dei portafogli di identità digitale europei, entro 6 mesi dall'entrata in vigore del Regolamento, e obbligare gli Stati Membri di comunicare alla Commissione i nomi e gli indirizzi degli organismi di certificazione pubblici o privati; i) prevedono la preparazione e la pubblicazione da parte della Commissione di un elenco di Portafogli europei di identità digitale certificati, sulla base delle informazioni fornite dagli Stati Membri sui Portafogli già emessi; l) regolamentano il ricorso transfrontaliero ai portafogli europei di identità digitale, prescrivendone l'accettazione in una serie di ipotesi, ossia quando è necessario per accedere ai servizi online prestati da un organismo del settore pubblico, o qualora l'autenticazione forte dell'utente è richiesta dalle parti private facenti affidamento

per finalità di identificazione online o per obblighi contrattuali, anche nei settori dei trasporti, dell'energia, dei servizi bancari e finanziari, della previdenza sociale, della sanità, dell'acqua potabile, dei servizi postali, dell'infrastruttura digitale, dell'istruzione o delle telecomunicazioni, o ancora da piattaforme digitali molto grandi; m) disciplinano il riconoscimento reciproco di altri mezzi di identificazione elettronica; n) fissano i requisiti per un servizio qualificato per la gestione di dispositivi adibiti alla creazione di firme elettroniche a distanza; o) regolamentano il servizio di conservazione qualificato per le firme elettroniche qualificate; p) stabiliscono i requisiti per un servizio qualificato per la gestione di dispositivi per la creazione di sigilli elettronici a distanza e per i certificati qualificati per l'autenticazione di siti web; q) definiscono i requisiti per i registri elettronici qualificati, tra cui l'unicità, l'autenticità e la corretta sequenza dei dati ivi registrati, nonché la rispettiva accuratezza circa la data e l'ora di inserimento dei dati, in modo tale che qualsiasi modifica successiva sia immediatamente rilevabile; r) prescrivono agli Stati Membri di raccogliere – e presentare alla Commissione entro il mese di marzo di ogni anno – le statistiche relative al funzionamento dei Portafogli europei di Identità Digitale da mettere a disposizione del pubblico, con riferimento al numero di persone fisiche e giuridiche che dispongono di un tale Portafoglio europeo, sul tipo e sul numero di servizi che accettano l'uso del Portafoglio, sugli incidenti e sui tempi di inattività dell'infrastruttura che impedisce l'utilizzo del Portafoglio stesso; s) attribuiscono alla Commissione il potere di riesaminare l'applicazione del Regolamento e di riferire al Parlamento e al Consiglio europeo entro 24 mesi dalla sua entrata in vigore; t) introducono nuove figure, tra cui il "*wallet provider*" che avrà il compito di fornire il supporto tecnologico per il dislocamento del sistema e per l'aggregazione dei diversi certificati, e i "*Providers of attestations*" (fornitori di attestati certificati e non certificati) che contribuiranno ad accrescere il valore dell'identità digitale europea, rilasciando certificati che consentano di convalidare determinati attributi dell'utente (sia certificati, come il possesso di un titolo di studio rilasciato dalla propria università, ma anche non certificati, sino a poter includere qualsiasi badge o carta che abbiamo nel nostro portafoglio, come la tessera dei trasporti o le carte fedeltà).

Il 6 dicembre 2022 il Consiglio è giunto a formulare il proprio orientamento generale, mentre nel marzo 2023 il Parlamento europeo ha approvato una Relazione sulla proposta della Commissione con conseguente avvio del trilogo negoziale che ha condotto ad un **accordo provvisorio** nel giugno scorso.

Nell'accordo, in particolare, si enfatizza l'importanza di assicurare un livello di sicurezza elevato che fornisca la garanzia che la persona che sostiene di avere una determinata identità sia effettivamente la persona cui tale identità è stata assegnata, viene sancita la gratuità per le persone fisiche dell'emissione, dell'uso per l'autenticazione e della revoca dei portafogli così dell'apposizione di firme elettroniche, viene ampliato l'elenco di servizi fiduciari attraverso l'inserimento di nuovi servizi fiduciari qualificati (tra cui la prestazione di registri elettronici e la gestione di dispositivi per la creazione di firme e sigilli elettronici a distanza), vengono introdotte nuove norme tese a delineare un'architettura tecnica e un quadro di riferimento comuni, nonché norme comuni da sviluppare con gli Stati membri al fine di inaugurare un approccio armonizzato alla sicurezza per i cittadini che fanno affidamento su un'identità digitale europea che li rappresenti online e per i prestatori di servizi online che potranno fare pieno affidamento su soluzioni di identità digitale e accettarle indipendentemente dal luogo in cui sono state emesse. A ciò si aggiunge l'allineamento alla legislazione esistente in materia di cibersicurezza, mediante designazione,

ad opera degli Stati membri, di organismi pubblici e privati accreditati per certificare il portafoglio come previsto dal regolamento sulla cibersicurezza e l'introduzione di un obbligo per gli Stati membri di effettuare un abbinamento di identità inequivocabile per i servizi transfrontalieri.

5.5. LA CORNICE EUROPEA SULLA CYBERSECURITY. DALLA NIS2 AL CYBER RESILIENCE ACT (CRA)

Al crescere della digitalizzazione si accompagna, inevitabilmente, un'estensione della superficie di attacco e la conseguente necessità di apprestare misure in grado di ridurre i rischi. L'UE ha dunque negli anni dedicato crescente attenzione al tema della cybersecurity nell'ottica di disegnare una cornice normativa efficace, capace di assicurare un ecosistema sicuro.
Il 2020 rappresenta un anno particolarmente importante per le politiche europee sulla cybersecurity che ha visto il lancio, da parte della Commissione europea, del "Cybersecurity package", costituito dalla "Strategia dell'UE in materia di cibersicurezza per il decennio digitale", una nuova direttiva sulla resilienza delle entità critiche ed una proposta di direttiva relativa alle misure necessarie per conseguire un elevato livello comune di cibersicurezza in tutta l'Unione (direttiva NIS rivista).
La strategia, in particolare, ha declinato proposte concrete di iniziative politiche, di regolamentazione e di investimento per rafforzare resilienza, sovranità tecnologica e leadership, sviluppare capacità operative di prevenzione, dissuasione e risposta e promuovere un ciberspazio globale e aperto.
All'esito di un ampio ed articolato dibattito, il 27 dicembre 2022 è stata pubblicata sulla G.U. dell'UE la Direttiva n. 2557/2022 sulla resilienza dei soggetti critici (**Direttiva CER – Resilience of Critical Entities**) che abroga la direttiva 2008/114/CE, il cui termine di recepimento per gli Stati membri è fissato al 17 ottobre 2024. Tale direttiva, in particolare, mira ad aumentare la resilienza di soggetti, negli Stati membri, che sono fondamentali per la fornitura di servizi essenziali per il mantenimento di funzioni vitali della società o di attività economiche nel mercato interno, in una serie di settori che sono alla base del funzionamento di molti altri settori dell'economia dell'Unione. Sono esclusi dal campo di applicazione della direttiva gli enti della pubblica amministrazione operanti nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa o dell'attività di contrasto, compresi l'indagine, l'accertamento e il perseguimento di reati.
La direttiva CER detta norme armonizzate volte a garantire la fornitura di servizi essenziali nel mercato interno, accrescere la resilienza dei soggetti critici e migliorare la cooperazione transfrontaliera tra le autorità competenti e prevede che entro il 17 luglio 2026 ogni stato individui i soggetti critici per i settori dell'energia, dei trasporti, bancario, delle acque potabili, delle acque reflue, della produzione, trasformazione e distribuzione di alimenti, della sanità, dello spazio, delle infrastrutture dei mercati finanziari e delle infrastrutture digitali, e di determinati aspetti della pubblica amministrazione. La stessa direttiva fissa per i soggetti critici obblighi volti a rafforzare la loro resilienza e la loro capacità di fornire servizi nel mercato interno, stabilisce norme riguardanti la vigilanza sui soggetti critici e l'esecuzione, definisce procedure comuni di cooperazione e comunicazione sull'applicazione della stessa e prescrive misure intese a raggiungere un livello di resilienza elevato dei soggetti critici al fine di garantire la fornitura di servizi essenziali nell'Unione e migliorare il funzionamento del mercato interno.
A carico degli Stati membri è posto l'obbligo di adottare, entro il 17 gennaio 2026, una strategia per rafforzare la resilienza dei soggetti critici di cui vengono dettagliatamente individuati i contenuti minimi

e di compiere una valutazione del rischio sulla base di un elenco non esaustivo dei servizi essenziali nei settori e nei sottosettori indicati dalla Commissione entro il 17 novembre 2023 e dei criteri individuati dalla stessa direttiva.
Gli stessi Stati sono chiamati a sostenere i soggetti critici nel rafforzamento della loro resilienza e a cooperare con gli altri Stati consultandosi per i soggetti critici che utilizzano infrastrutture critiche fisicamente collegate tra due o più Stati membri, fanno parte di strutture societarie collegate o associate a soggetti critici in altri Stati membri e sono stati individuati come soggetti critici in uno Stato membro e forniscono servizi essenziali ad altri Stati membri o in altri Stati membri.
I soggetti critici, invece, una volta ricevuta la relativa designazione, sono tenuti ad effettuare una valutazione dei rischi rilevanti (compresi tutti quelli naturali o di origine umana) che potrebbero perturbare la fornitura dei loro servizi essenziali e ad adottare misure tecniche, di sicurezza e organizzative adeguate e proporzionate per garantire la propria resilienza, in base alle informazioni pertinenti fornite dagli Stati membri in merito alla valutazione del rischio dello Stato membro e in base ai risultati della valutazione del rischio dagli stessi compiute. Agli stessi soggetti critici è richiesto, altresì, di notificare senza indebito ritardo all'autorità competente gli incidenti che perturbano o possono perturbare in modo significativo la fornitura di servizi essenziali.
Specifiche previsioni sono dettate al Capo IV per l'individuazione dei soggetti critici di particolare rilevanza europea.
Dal punto di vista istituzionale, è istituito il gruppo per la resilienza dei soggetti critici, composto da rappresentanti degli Stati membri e della Commissione, con compiti di assistenza alla Commissione, chiamato a favorire la condivisione delle migliori prassi, ad agevolare lo scambio di informazioni e ad analizzare strategie e relazioni.
A livello nazionale, ogni Stato membro è chiamato a designare o istituire una o più autorità competenti responsabili dell'applicazione della direttiva a livello nazionale e un punto di contatto unico con funzioni di collegamento e obblighi di relazione alla Commissione, entro il 17 luglio 2028, e successivamente ogni due anni, in merito alle notifiche ricevute e alle azioni intraprese.
Nella medesima data – 27 dicembre 2022 – è stata infine pubblicata la **Direttiva n. 2555/2022 (NIS2)**, entrata in vigore lo scorso 17 gennaio 2023 e da recepire entro il 17 ottobre 2024.
Attraverso la NIS2, l'UE punta ad incrementare e rendere omogeneo il livello di cybersecurity negli Stati membri, creare e ad apprestare misure in grado di fronteggiare in maniera efficace l'incremento dei rischi per la sicurezza conseguenti alla diffusa digitalizzazione dei processi e dei servizi.
In tale logica, pur confermando gran parte degli obiettivi e degli strumenti della direttiva NIS, la NIS2, partendo dalla constatazione del rafforzamento del ruolo di alcune categorie di soggetti e del sopraggiungere di rischi nuovi in settori ulteriori rispetto a quelli individuati, è innanzitutto intervenuta ampliando la platea di soggetti destinatari della normativa dalla stessa fissata.
Se l'originaria Direttiva NIS si rivolge – e si rivolgerà fino alla sua abrogazione – a quegli operatori privati che svolgono la loro attività nei settori ritenuti "essenziali" dall'Unione europea, ovverosia quelli dell'energia, dei trasporti, delle banche, delle infrastrutture dei mercati finanziari, dell'acqua potabile, della sanità e delle infrastrutture digitali, cui si affiancano anche i fornitori di servizi digitali, la Direttiva NIS 2 ha incluso nel proprio campo di applicazione ulteriori soggetti attivi in settori definiti "ad alta criticità", ovvero quelli delle acque reflue, della gestione dei servizi ICT (business-to-business), della pubblica amministrazione e dello spazio. Inoltre, ha previsto anche la tipologia dei c.d. "altri settori critici", includendovi

i servizi postali e di corriere, la gestione dei rifiuti, la fabbricazione, la produzione e la distribuzione di sostanze chimiche, la produzione, la trasformazione e la distribuzione di alimenti, la fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro, la fabbricazione di computer e prodotti di elettronica e ottica, la fabbricazione di apparecchiature elettriche, la fabbricazione di macchinari e apparecchiature n.c.a., la fabbricazione di autoveicoli, rimorchi e semirimorchi e di altri specifici mezzi di trasporto e i fornitori di servizi digitali (mercati online, motori di ricerca e piattaforme di servizi di social network).

All'ampliamento dell'ambito di applicazione si accompagna anche il superamento della precedente impostazione legata ai concetti di "operatore di servizi essenziali" e di "fornitore di servizi digitali", liberamente identificati dagli Stati membri dell'Unione Europea attraverso criteri spesso disomogenei, in favore di due nuove categorie di attori, quella dei "soggetti essenziali" e quella dei "soggetti importanti" e l'introduzione di un criterio dimensionale tale per cui la disciplina si applica a tutti quei soggetti pubblici o privati ricompresi nelle tipologie denominate "alta criticità" o "altri settori critici" che prestino i loro servizi o svolgano le loro attività all'interno dell'Unione e siano considerati medie imprese ai sensi all'articolo 2, paragrafo 1, dell'allegato alla raccomandazione 2003/361/CE, o che superino i massimali per le medie imprese di cui al paragrafo 1 del medesimo articolo. Queste ultime, in particolare, sono quelle con un numero di dipendenti pari almeno a 50 unità ed un fatturato annuo superiore ai 10 mln di euro.

Inoltre, indipendentemente dalle dimensioni, vengono comunque assoggettate alla Direttiva NIS 2 anche ulteriori particolari tipologie di soggetti, tra cui i fornitori di reti di comunicazione elettroniche pubbliche o di servizi di comunicazione elettronica accessibili al pubblico, coloro che forniscono servizi di registrazione dei nomi di dominio, taluni enti della pubblica amministrazione, nonché i soggetti definiti c.d. "critici" dalla Direttiva 2022/2557 (Direttiva CER) sopra descritta. Agli Stati membri è riconosciuta la facoltà di prevedere che la direttiva si applichi ad enti della pubblica amministrazione a livello locale e ad istituti di istruzione, in particolare ove svolgano attività di ricerca critiche.

Sono espressamente esclusi dall'ambito di applicazione della direttiva gli enti della pubblica amministrazione che svolgono le loro attività nei settori della sicurezza nazionale, della pubblica sicurezza o della difesa, del contrasto, comprese la prevenzione, le indagini, l'accertamento e il perseguimento dei reati. Se questi sono i riferimenti normativi, spetterà comunque agli Stati membri stilare (entro il 17 aprile 2025), anche attraverso le informazioni fornite dai soggetti interessati, un elenco dei soggetti essenziali ed importanti.

Per quanto concerne gli obblighi a carico dei soggetti rientranti nel campo di applicazione della direttiva, sono previste misure più stringenti e specifiche in termini di *cyber risk management*, di segnalazione e condivisione delle informazioni relative agli incidenti di sicurezza e viene introdotto un approccio basato sul concetto del c.d. "multirischio".

Ciò comporta che le misure tecniche, operative e organizzative comprendano almeno i seguenti aspetti: a) le politiche di analisi dei rischi e di sicurezza dei sistemi informatici; b) la gestione degli incidenti; c) la continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e la gestione delle crisi; d) la sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi; e) la sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità; f) le strategie e le procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza; g) le pratiche di igiene informatica di base e di formazione in materia di cibersicurezza; h) le politiche e le procedure relative all'uso della crittografia e, se del caso, della cifratura; i) la sicurezza delle

risorse umane, le strategie di controllo dell'accesso e gestione degli attivi; l) l'uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.

Cruciali gli obblighi di segnalazione in caso di "incidente significativo", ossia un incidente che abbia causato o sia in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato e/o si sia ripercosso o sia in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli. In presenza di tali condizioni, la direttiva prevede che i soggetti interessati trasmettano un preallarme entro il termine di 24 ore dalla conoscenza dell'incidente, una notifica entro il termine di 72 ore dalla conoscenza dell'incidente, che aggiorni – se necessario – le informazioni del preallarme, un report intermedio se richiesto dall'autorità/CSIRT ed una relazione finale entro un mese dalla trasmissione della notifica, con l'analisi dell'incidente e la descrizione delle misure di mitigazione adottate.

Gli organi di gestione dei soggetti rientranti nell'ambito applicativo della direttiva sono dunque chiamati a garantire la sicurezza della rete e dei sistemi informativi, la compliance alla disciplina della direttiva ed un'attività di collaborazione con le autorità competenti in materia.

Molto rilevanti le misure di vigilanza e di esecuzione, alle quali saranno sottoposti – in misura differente – i soggetti essenziali e importanti e che includono audit regolari e mirati sulla sicurezza, scansioni di sicurezza, ovvero ispezioni in loco, vigilanza e richieste di informazioni (solo ex post, in caso di soggetti importanti).

Le sanzioni per la violazione delle misure di gestione dei rischi di cybersecurity o degli obblighi di segnalazione potranno arrivare a un massimo di almeno 10 milioni di euro (ridotti a 7, in caso di soggetti importanti) o a un massimo di almeno il 2% (ridotto all'1,4%, in caso di soggetti importanti) del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto appartiene, se superiore.

Sempre in attuazione di quanto previsto nella Strategia lanciata nel 2020 e partendo dalla constatazione della necessità, per assicurare un ecosistema europeo complessivamente sicuro, di garantire che i dispositivi utilizzati da cittadini, imprese e pubbliche amministrazioni rispondano a standard di sicurezza adeguati, il 15 settembre 2022 la Commissione ha pubblicato una proposta di regolamento sui requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020 (***Cyber Resilience Act*** **– CRA**).

Tale proposta, in particolare, mira a salvaguardare i consumatori e le imprese che acquistano o utilizzano prodotti o software con una componente digitale attraverso la fissazione di regole armonizzate per l'immissione sul mercato di prodotti o software con una componente digitale, l'individuazione di requisiti di cybersecurity che disciplinano la pianificazione, la progettazione, lo sviluppo e la manutenzione di tali prodotti, la fissazione di obblighi per ogni fase della catena del valore e la declinazione di un obbligo generale di diligenza per l'intero ciclo di vita di tali prodotti.

In particolare, la proposta della Commissione parte dalla constatazione che i prodotti hardware e software sono sempre più soggetti ad attacchi informatici di successo, il cui costo globale stimato è di 5,5 trilioni di euro entro il 2021 e che ciò sia conseguenza di un basso livello di sicurezza informatica e dell'incapacità degli utenti di scegliere dispositivi.

Nel definire l'ambito applicativo, la proposta si riferisce ai prodotti con elementi digitali il cui uso previsto o ragionevolmente prevedibile include una connessione logica o fisica diretta o indiretta di dati a un dispositivo o a una rete, individuando tra i prodotti con elementi digitali, quelli critici (suddivisi in Classe I e II) e fissa una serie corposa di obblighi a carico di produttori, importatori e distributori.

I prodotti definiti come critici e rientranti nella Classe II, in particolare, non possono essere oggetto di autocertificazione di base da parte del produttore, ma necessitano del rilascio di una certificazione da parte di un ente di certificazione accreditato.

I produttori, nello specifico, sono chiamati a:

e. realizzare un *assessment* dei rischi cyber associati al prodotto con elementi digitali – da includere nella documentazione tecnica da produrre ai fini dell'immissione sul mercato – e di tenerne conto durante la progettazione, lo sviluppo, la produzione, la distribuzione ed in tutte le fasi di vita del prodotto allo scopo di minimizzare i rischi di cybersecurity, prevenire gli incidenti di sicurezza e ridurne gli impatti;
f. osservare obblighi di diligenza nel caso in cui decidano di integrare componenti provenienti da terze parti nella logica di garantire che non ci siano compromissioni della sicurezza del prodotto;
g. documentare in maniera proporzionata alla natura del prodotto ed ai rischi, gli aspetti concernenti il prodotto, incluse le vulnerabilità di cui venga a conoscenza;
h. dotarsi di appropriate policy e procedure, incluse quelle di identificazione e gestione delle vulnerabilità;
i. fornire informazioni ed istruzioni sul prodotto che siano chiare e comprensibili;
j. mettere in atto correttivi nel caso in cui emerga o vi sia ragione di pensare che il prodotto o i processi messi in atto non siano conformi alla disciplina prevista;
k. cooperare con le autorità di vigilanza fornendo informazioni chiare e comprensibili, mettendo in atto misure per eliminare i rischi di cibersicurezza ed anche informando le stesse autorità dell'eventuale incapacità di essere *compliant* con le norme dettate;
l. informare l'ENISA (entro 24 ore) di eventuali vulnerabilità e/o incidenti (ENISA informa EUCyCLONe nel caso in cui le informazioni ricevute siano rilevanti per la gestione coordinata di incidenti di cybersecurity su larga scala ed inserisce tali informazioni nel report biennale da inviare al Gruppo di Cooperazione);
m. informare gli utenti dell'incidente, fornendo informazioni su eventuali azioni da compiere per mitigarne l'impatto.

Tali obblighi si applicano anche a importatori o distributori che immettano sul mercato il prodotto sotto il proprio nome o marchio o apportino una modifica sostanziale al prodotto. Alla medesima conclusione si giunge rispetto a qualunque persona fisica o giuridica che apporti una modifica sostanziale al prodotto.

Agli importatori, è inoltre prescritto di verificare che il produttore abbia attivato le procedure di conformità di cui all'art. 24 ed abbia prodotto la redazione tecnica, che il prodotto sia munito della marcatura CE e che sia accompagnato dalle informazioni ed istruzioni per l'uso (di cui devono verificare la chiarezza e comprensibilità) e di non mettere sul mercato il prodotto nel caso in cui ritenga che lo stesso non abbia i requisiti essenziali prescritti (informando anche il produttore e l'autorità di vigilanza nel caso di rischi di cybersecurity). Agli stessi è altresì richiesto di comunicare, senza ritardo, al produttore, eventuali non *compliance* con la normativa e vulnerabilità (nel caso di significativo rischio è prescritta anche la comunicazione, senza ritardo, alle autorità di vigilanza degli Stati in cui gli importatori rendono disponibile il prodotto), conservare per 10 anni dall'immissione sul mercato del prodotto, la documentazione attestante la conformità dello stesso ai requisiti richiesti e collaborare con le autorità di sorveglianza.

Ai distributori, infine, è prescritto di verificare che il prodotto possieda la marcatura CE e che produttore e importatore abbiano osservato gli obblighi sugli stessi gravanti. Anche ai distributori è vietato immettere sul mercato il prodotto nel caso in cui ritengano che

lo stesso non possieda i requisiti essenziali previsti, è fatto obbligo di informare il produttore e l'autorità di vigilanza nel caso sussistano significativi rischi di cibersicurezza, di cooperare con le autorità e di comunicare eventuali impossibilità di essere *compliant* con la disciplina prevista dal regolamento.

Ciò che emerge dall'analisi della proposta è la definizione di un articolato set di obblighi tesi a creare, di fatto, una catena di verifica e controllo reciproco molto robusta tra produttori, importatori e distributori.

Dal punto di vista procedurale, la proposta descrive accuratamente le procedure di verifica della conformità dei prodotti con elementi digitali ai requisiti prescritti ed attribuisce agli Stati membri il compito di individuare un'autorità di notifica ("*notifying authority*") – di cui vengono declinati i requisiti essenziali – deputata a definire le procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e per il loro monitoraggio.

Rispetto a questi ultimi, in particolare, la proposta fissa stringenti requisiti di indipendenza, professionalità, competenza, vietando espressamente che la remunerazione dei manager e del personale possa essere collegata al numero o all'esito degli *assessment* compiuti e prescrivendo specifici obblighi di segretezza rispetto a tutte le informazioni ricevute nello svolgimento delle proprie attività.

Molto rilevante la previsione dell'art. 18 "Presunzione di conformità" con la quale viene attribuito alla Commissione il potere di specificare, mediante atti di esecuzione, i sistemi europei di certificazione della cibersicurezza adottati a norma del regolamento (UE) 2019/881 che possono essere utilizzati per dimostrare la conformità ai requisiti essenziali o a parti di essi di cui all'allegato I.

Inoltre, se del caso, la Commissione specifica se un certificato di cibersicurezza rilasciato nell'ambito di tali sistemi elimina l'obbligo per un fabbricante di effettuare una valutazione di conformità da parte di terzi per i requisiti corrispondenti.

Rispetto a sorveglianza ed *enforcement*, la proposta di regolamento affida agli Stati membri la designazione di un'autorità deputata alla sorveglianza del mercato e dei prodotti con elementi digitali (con la garanzia che tale autorità disponga delle necessarie risorse umane e finanziarie), alla cooperazione con le medesime autorità degli altri Stati membri e, ove opportuno, con quelle preposte alla supervisione dell'osservanza della normativa sulla protezione dei dati (queste ultime, in particolare, hanno il potere, per l'esercizio delle proprie funzioni, di accedere alla documentazione prevista dalla proposta in esame).

Molto rilevanti i poteri attribuiti alla Commissione. Ed infatti, per i prodotti che presentino un elevato rischio di cybersecurity, la proposta prevede che, nel caso in cui l'autorità di sorveglianza accerti una non *compliance* non limitata al territorio nazionale, la stessa avvisi la Commissione e gli altri Stati membri fornendo informazioni anche sui risultati delle valutazioni compiute e sulle azioni che l'operatore è stato chiamato ad attuare. In caso di disaccordo di uno Stato membro circa le misure adottate o nell'ipotesi in cui la Commissione le ritenga contrarie al diritto UE, la proposta prevede che quest'ultima attivi una consultazione (*Union safeguard procedure*, art. 44) con gli Stati membri e gli operatori interessati all'esito della quale – entro 9 mesi dalla notifica – la stessa valuti se la misura nazionale sia giustificata o no.

Sempre con riguardo ai prodotti che presentino un significativo rischio di cybersecurity, alla Commissione è anche riconosciuto il potere di richiedere ad un'autorità nazionale di sorveglianza di operare la relativa valutazione e, in eccezionali circostanze che giustifichino un immediato intervento per preservare il buon funzionamento del mercato interno, in mancanza di un intervento dell'autorità di sorveglianza nazionale, il potere di azionare l'ENISA informando prontamente l'autorità nazionale.

Aspro il regime sanzionatorio che prevede sanzioni

amministrative pecuniarie fino a 15.000.000 di euro o, se il trasgressore è un'impresa, fino al 2,5% del suo fatturato mondiale totale annuo per l'esercizio precedente, a seconda di quale sia il valore più elevato nel caso di violazione delle disposizioni contenute negli artt. 10 e 11 e dunque degli obblighi a carico dei produttori. Tali importi scendono a 10.000.000 di euro o al 2% nel caso di inosservanza degli altri obblighi e a 5.000.000 o l'1% nel caso di invio di informazioni scorrette, incomplete o fuorvianti agli organismi di valutazione o all'autorità di vigilanza a seguito di richiesta.

Se questi sono i contenuti essenziali della proposta lanciata dalla Commissione, in Parlamento europeo quest'ultima è stata assegnata alla commissione ITRE (rapporteur Nicola Danti) che lo scorso 19 luglio ha adottato la **relazione** sulla proposta presentata il 31 marzo scorso, proponendo una serie di importanti modifiche che, anche in una logica di semplificazione degli adempimenti a carico delle imprese, allineano le procedure a quanto previsto dalla NIS2 ed introducono precisazioni utili in una logica di garanzia della certezza del diritto soprattutto per le PMI che evidentemente si trovano a dover affrontare il tema della sicurezza con un rigore crescente che implica un ripensamento del proprio modello organizzativo ed investimenti decisamente rilevanti.

In particolare, tra le varie modifiche proposte si segnalano, per importanza:

a. PRECISAZIONE DEL CAMPO DI APPLICAZIONE. Il testo approvato include tutti i prodotti con elementi digitali ma esclude gli sviluppatori di software open source nei casi in cui gli stessi non ricevano alcun ritorno finanziario per i loro progetti ed amplia l'elenco dei prodotti critici di classe I, per includere anche i sistemi di automazione domestica e i prodotti che migliorano la sicurezza privata, come telecamere e serrature intelligenti;
b. DURATA DEL PRODOTTO ED AGGIORNAMENTI. Il rapporto propone una durata flessibile per la durata prevista del prodotto, che dovrebbe comunque essere chiaramente indicata e fissa l'obbligo per i produttori di fornire aggiornamenti di sicurezza automatici e di distinguere tra aggiornamenti di sicurezza e funzionalità ove possibile;
c. ALLINEAMENTO CON LA NIS2. Si dispone l'allineamento alla direttiva NIS2 per semplificare gli obblighi per i produttori e rendere obbligatoria solo la segnalazione di incidenti significativi e vulnerabilità sfruttate attivamente, in un approccio in più fasi (24 ore, 72 ore, 1 mese). L'Agenzia dell'Unione europea per la sicurezza informatica (ENISA) dovrebbe diventare lo sportello unico per le segnalazioni e dovrebbe essere rafforzata per poter svolgere i compiti aggiuntivi stabiliti nel regolamento;
d. APPLICAZIONE DEL REGOLAMENTO. La relazione propone di prorogare di 40 mesi la data a partire dalla quale il regolamento si applica così da consentire alle micro, piccole e medie imprese di ricevere un sostegno sufficiente per garantire la loro conformità e di disporre l'entrata in vigore di norme armonizzate, specifiche comuni o sistemi europei di certificazione della cibersicurezza per sei mesi prima che venga applicata la procedura di valutazione della conformità. La Commissione dovrebbe fornire linee guida con maggiori dettagli sull'attuazione.
e. FORMAZIONE E COMPETENZE. Il rapporto sottolinea l'importanza dei professionisti della sicurezza informatica e propone un rafforzamento delle competenze e la riqualificazione dei lavoratori;
f. COMMERCIO INTERNAZIONALE. Per promuovere il commercio internazionale, il rapporto sottolinea l'importanza di concludere accordi di mutuo riconoscimento (MRA) con paesi terzi per garantire lo stesso livello di protezione

fornito dalle CRA. Per quanto riguarda il monitoraggio dei fattori di rischio non tecnici, l'ENISA e le autorità di vigilanza del mercato dovrebbero effettuare i necessari controlli sui venditori che potrebbero presentare un profilo di rischio più elevato.

Il 13 settembre scorso, il Parlamento ha disposto l'avvio dei negoziati interistituzionali.

In sede di Consiglio, invece, i rappresentanti degli Stati membri hanno raggiunto una **posizione comune** il 19 luglio 2023, consentendo al Consiglio di avviare negoziati con il Parlamento europeo. Anche il Consiglio ha proposto una serie di modifiche ed in particolare l'eliminazione della nozione di "critico" dai prodotti con elementi digitali e la cancellazione di un numero considerevole di prodotti elencati nell'allegato III. Il Consiglio ha inoltre introdotto tre categorie di prodotti, fondamentali per le entità essenziali come definite dalla NIS2, che rientrerebbero nella certificazione europea obbligatoria della cibersicurezza mediante un atto delegato. Il Consiglio ha spostato la segnalazione degli incidenti di cibersicurezza e delle vulnerabilità attivamente sfruttabili dall'ENISA ai team nazionali di risposta agli incidenti di sicurezza informatica (CSIRT) in un processo in due fasi: una prima notifica dopo 24 ore e una seconda dopo 72 ore. Quanto all'applicazione del regolamento, il Consiglio ha proposto di rinviarne l'applicazione a 36 mesi.

icom
istituto per la competitività

CAPITOLO 6

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

6.1. METODOLOGIA

L'**I-Com Ultrabroadband Index (IBI)**, giunto alla decima 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.

L'IBI è un indice sintetico pensato per riassumere le informazioni riguardanti domanda e offerta di connettività negli Stati membri dell'Unione. I dati su cui si effettua il calcolo provengono dalla banca dati del DESI-Digital Economy and Society Index e da Eurostat. Le variabili selezionate per l'edizione 2023[30] sono 12 in totale, sei relative alla domanda di connettività e sei relative all'offerta. Per la domanda di connettività, le variabili scelte sono le seguenti:

1. PMI che vendono online – almeno l'1% del fatturato (in % delle imprese);
2. individui che hanno utilizzato internet, negli ultimi 12 mesi, per interagire con le autorità pubbliche su siti web o su applicazioni mobili (in % degli individui);
3. occupati che hanno accesso a internet per scopi aziendali (in % del totale occupati);
4. famiglie che hanno una connessione di banda larga fissa – almeno 100 Mbps (in % delle famiglie);
5. imprese con una connessione di banda larga fissa (in % delle imprese);
6. utenti internet con competenze digitali almeno di base (in % degli individui).

Per l'offerta di connettività, le sei variabili riguardano i dati di copertura relativi alle tre reti di maggiore capacità, con una distinzione tra copertura generale e copertura dei territori rurali[31]. Le variabili sono quindi:

7. copertura 5G (in % delle famiglie);
8. copertura 5G nei territori rurali (in % delle famiglie);
9. copertura Fiber to the Premises (in % delle famiglie);
10. copertura fiber to the Premises nei territori rurali (in % delle famiglie);
11. copertura Very High Capacity Network (in % delle famiglie);
12. copertura Very High Capacity Network nei territori rurali (in % delle famiglie) [32].

6.2. RISULTATI DELL'ANALISI

La **Danimarca**, con un punteggio pari a 78, continua a guidare la classifica complessiva europea (Tab. 6.1). Le ragioni di questo successo risiedono in un elevatissimo grado di informatizzazione delle imprese e in una copertura 5G e VHCN, che raggiunge la quasi totalità della popolazione, sia in ambito cittadino che nelle aree rurali. A ciò va ad aggiungersi la rilevante diffusione dell'e-government, che vede oltre il 90% dei cittadini interagire con le pubbliche autorità tramite internet.

Sul podio, seguono **Paesi Bassi** e **Spagna**. Quest'ultima recupera ben due posizioni rispetto al 2020, a svantaggio della **Svezia** che retrocede in sesta posizione.

L'ottimo risultato della Spagna è motivato da una percentuale elevata di famiglie – il dato più alto nell'UE – che ha sottoscritto un abbonamento in banda larga fissa e da una più alta penetrazione delle reti VHCN e FTTP. La Svezia, che nelle versioni IBI precedenti si alternava con la capolista per le posizioni apicali, si trova

30 I dati oggetto di elaborazione si riferiscono alla versione DESI 06/2022

31 Un territorio è considerato rurale quando la densità abitativa è minore di 100 persone per km2.

32 Va precisato che per alcuni stati membri il dato per la copertura VHCN e quello per copertura FTTP coincidono. Questo fatto non è sorprendente e sta solo a significare che, per quegli stati, la penetrazione della rete a very high capacity (ovvero a velocità di almeno 100 Mbps) avviene solo sotto forma di tecnologia di fiber to the premises.

Tab. 6.1: I-Com Broadband Index, classifica generale

Fonte: elaborazioni I-Com su dati DESI e Eurostat

	IBI				Ranking			
	2021	2022	2023	Δ2023-2021	2021	2022	2023	Δ2021-2023
Danimarca	69	74	78	**9**	1	1	1	**0**
Paesi Bassi	57	66	73	**16**	2	2	2	**0**
Spagna	49	56	67	**18**	5	4	3	**+2**
Irlanda	38	52	62	**24**	13	5	4	**+9**
Lussemburgo	49	52	60	**11**	6	6	5	**+1**
Svezia	55	57	60	**5**	3	3	6	**-3**
Malta	44	46	59	**15**	8	9	7	**+1**
Francia	34	43	57	**23**	19	12	8	**+11**
Finlandia	40	43	56	**16**	9	13	9	**0**
Lituania	38	43	55	**17**	12	11	10	**+2**
Portogallo	47	50	54	**7**	7	8	11	**-4**
Ungheria	37	41	53	**16**	14	15	12	**+2**
Lettonia	50	51	53	**3**	4	7	13	**-9**
Romania	39	45	51	**12**	10	10	14	**-4**
Cipro	25	32	51	**26**	26	26	15	**+11**
Italia	**26**	**38**	**51**	**25**	**25**	**20**	**16**	**+9**
Slovenia	39	41	49	**10**	11	14	17	**-6**
Germania	31	37	47	**16**	22	22	18	**+4**
Croazia	29	32	47	**18**	23	25	19	**+4**
Bulgaria	34	39	47	**13**	16	18	20	**-4**
Estonia	37	40	47	**10**	15	16	21	**-6**
Austria	33	39	47	**14**	21	19	22	**-1**
Rep. Ceca	27	34	45	**18**	24	24	23	**+1**
Slovacchia	34	36	44	**10**	18	23	24	**-6**
Belgio	34	40	44	**10**	17	17	25	**-8**
Polonia	33	37	41	**8**	20	21	26	**-6**
Grecia	22	25	36	**14**	27	27	27	**0**

questa volta in retrocessione soprattutto per la scarsa copertura 5G sia in ambito cittadino che rurale.

Tuttavia, si osserva come alcuni Paesi abbiano davvero premuto l'acceleratore nel corso di questi ultimi anni, avanzando di diverse posizioni in classifica. I progressi più impressionanti sono quelli della

Francia e di Cipro, che guadagnano 11 posizioni, e dell'Italia e dell'Irlanda, che risalgono la classifica di ben 9 gradini dal 2021 al 2023. **Concentrandosi solo sull'ultimo anno, se la Francia passa dal dodicesimo posto all'ottavo, Cipro addirittura avanza dal ventiseiesimo al quindicesimo mentre l'Irlanda consolida il salto dell'anno precedente avvicinando il podio al quarto posto, dietro la Spagna, l'Italia riesce a piazzarsi sedicesima, risalendo dal ventesimo posto del 2022.**

In particolare, Cipro raggiunge il massimo della copertura 5G nelle aree rurali e in quelle urbane ed inoltre evidenzia un incremento della copertura delle reti fisse nonché, dal lato della domanda, un aumento della percentuale di famiglie con connessione in banda larga fissa. La **Francia** oltre ad avere un buono sviluppo dell'e-government presenta anch'essa un'interessante crescita della copertura delle reti fisse. Inoltre, la copertura 5G ha subito un interessante incremento sia nelle aree popolate sia in ambito rurale. **La performance italiana** è, invece, riconducibile a molteplici fattori, tra i quali risulta determinante l'imponente **crescita della copertura 5G**, che si attesta a circa il 100% nel 2022.

Un importante passo in avanti si registra anche nel campo dell'e-government, dove oltre il 40% degli italiani ha interagito con la PA via web, anche se il dato resta inferiore alla media UE. Inoltre, un avanzamento considerevole riguarda la **diffusione delle reti fisse**, indicate dalla copertura VHCN e FTTP a livello rurale, a testimonianza dell'evoluzione dei piani di cablatura dei numeri civici nelle aree grigie e bianche.

Per l'**Irlanda** invece, tutte le variabili di copertura di rete hanno visto un incremento considerevole a cui si aggiunge un miglioramento del livello di digitalizzazione delle imprese e dei cittadini.

La classifica per la componente dell'offerta (Tab. 6.2) è ancora una volta dominata da **Danimarca**, **Paesi Bassi** e **Spagna**, così come la classifica generale. Buoni posizionamenti si notano anche per **Irlanda** e **Romania**. Soprattutto nel caso dell'Irlanda la progressione tra 2020 e 2022 è stata importante, infatti, ha guadagnato 13 posizioni grazie anche all'investimento nella diffusione delle reti VHCN ed FTTP[33].

L'**Italia** si trova al dodicesimo posto, con un salto di 12 posizioni rispetto al 2021 e di 2 rispetto al 2022. Come già evidenziato in precedenza, in termini di penetrazione del 5G tra i paesi europei, l'Italia risulta ai primi posti. La copertura 5G continua ad avere un ruolo preponderante nel determinare il piazzamento finale, nonostante le due variabili relative pesino per solo un terzo del totale della componente offerta. È interessante notare come i Paesi che hanno conosciuto la maggiore variazione positiva tra ranking 2020 e 2022 si trovino tutti al di sopra della media UE quanto a copertura del 5G. Questa variabile è, tra l'altro, determinante nel definire anche il podio della classifica generale: le prime tre posizioni sono attribuite a Paesi aventi copertura 5G superiore alla media UE ed è proprio questa la discriminante che ha relegato la Svezia al quarto posto, favorendo la Spagna.

Inoltre, nel nostro Paese aumenta la copertura delle reti fisse. Anche se in questo caso i dati risultano ancora al di sotto del valore medio UE.

La classifica lato domanda (Tab. 6.3) mostra invece una dinamica molto più lenta rispetto a quanto emerso per l'offerta. Il vertice della classifica continua ad essere ad appannaggio della **Svezia** sia per l'ampia diffusione di e-commerce e soprattutto di e-government sia per l'elevato numero di famiglie che hanno sottoscritto servizi di connettività di banda larga.

Un esempio virtuoso in termini di domanda è fornito dall'**Ungheria** che sale di ben nove posizioni grazie soprattutto alla performance relativa all'e-government, che vede oltre l'80% della popolazione fare uso dei servizi online della pubblica amministrazione.

33 Per entrambi i paesi non esiste una distinzione tra le misurazioni delle due variabili.

Tab. 6.2: I-Com Broadband Index, classifica lato offerta

Fonte: elaborazioni I-Com su dati DESI e Eurostat

	IBI				Ranking			
	2021	2022	2023	Δ2023-2021	2021	2022	2023	Δ2021-2023
Danimarca	76	83	90	**14**	1	1	1	**0**
Paesi Bassi	55	73	84	**29**	2	2	2	**0**
Spagna	44	55	73	**29**	6	3	3	**+3**
Irlanda	24	48	65	**41**	17	8	4	**+13**
Romania	43	53	64	**20**	8	5	5	**+3**
Lussemburgo	48	51	61	**13**	4	7	6	**-2**
Malta	40	40	61	**21**	9	11	7	**+2**
Francia	21	35	61	**40**	19	13	8	**+11**
Bulgaria	38	47	60	**22**	10	10	9	**+1**
Lituania	28	36	57	**29**	12	12	10	**+2**
Lettonia	54	54	57	**3**	3	4	11	**-8**
Italia	**14**	**35**	**57**	**43**	**24**	**14**	**12**	**+12**
Portogallo	47	51	56	**9**	5	6	13	**-8**
Cipro	10	22	55	**45**	25	24	14	**+11**
Finlandia	21	27	51	**30**	18	22	15	**+3**
Ungheria	27	31	51	**24**	13	17	16	**-3**
Svezia	44	47	51	**7**	7	9	17	**-10**
Germania	15	28	50	**35**	22	20	18	**+4**
Croazia	15	20	50	**34**	21	26	19	**+2**
Slovenia	31	34	46	**16**	11	15	20	**-9**
Austria	18	29	45	**27**	20	19	21	**-1**
Estonia	26	31	44	**18**	15	18	22	**-7**
Slovacchia	24	28	44	**20**	16	21	23	**-7**
Rep. Ceca	8	21	38	**31**	26	25	24	**+2**
Polonia	26	31	37	**11**	14	16	25	**-11**
Grecia	6	10	31	**25**	27	27	26	**+1**
Belgio	14	22	28	**14**	23	23	27	**-4**

L'**Italia** non tiene il passo degli altri paesi membri, rimanendo relegata al ventitreesimo posto in classifica, davanti solo a Slovacchia, Grecia, Romania e Bulgaria. Gli indicatori relativi all'e-government, all'e-commerce e alle competenze sono decisamente al di sotto della media europea anche se, tuttavia, per ognuno di questi si evidenzia un miglioramento rispetto al passato.

Tab. 6.3: I-Com Broadband Index, classifica lato domanda

Fonte: elaborazioni I-Com su dati DESI e Eurostat

		IBI				Ranking		
	2021	**2022**	**2023**	**Δ2023-2021**	**2021**	**2022**	**2023**	**Δ2021-2023**
Svezia	65	67	69	**4**	1	1	1	**0**
Danimarca	62	64	65	**3**	2	2	2	**0**
Paesi Bassi	59	60	62	**3**	3	3	3	**0**
Finlandia	58	60	62	**4**	4	4	4	**0**
Spagna	53	57	61	**7**	6	5	5	**+1**
Belgio	53	57	59	**6**	5	6	6	**-1**
Irlanda	51	57	59	**8**	7	7	7	**0**
Lussemburgo	49	53	59	**9**	8	8	8	**0**
Malta	48	52	56	**8**	9	9	9	**0**
Ungheria	46	51	56	**10**	19	12	10	**+9**
Francia	46	51	54	**7**	18	10	11	**+7**
Lituania	48	51	53	**4**	10	11	12	**-2**
Portogallo	48	49	52	**4**	12	14	13	**-1**
Slovenia	47	49	51	**5**	17	15	14	**+3**
Rep. Ceca	47	48	51	**3**	14	18	15	**-1**
Lettonia	47	49	50	**3**	16	17	16	**0**
Estonia	47	49	50	**3**	13	13	17	**-4**
Austria	48	49	49	**1**	11	16	18	**-7**
Cipro	39	42	47	**7**	23	24	19	**+4**
Polonia	40	43	45	**5**	22	22	20	**+2**
Germania	47	46	45	**-2**	15	19	21	**-6**
Croazia	42	44	45	**3**	21	20	22	**-1**
Italia	**39**	**42**	**44**	**6**	**25**	**23**	**23**	**+2**
Slovacchia	43	43	43	**1**	20	21	24	**-4**
Grecia	39	40	41	**3**	24	25	25	**-1**
Romania	35	37	39	**4**	26	26	26	**0**
Bulgaria	30	32	34	**4**	27	27	27	**0**

In controtendenza rispetto a questo scenario negativo è il dato relativo alla digitalizzazione delle imprese. In questo caso, infatti, l'Italia è al di sopra della media europea (94%), con una porzione pari al 98% delle imprese aventi una connessione in banda larga.

Al fine di misurare il grado di sviluppo digitale dei Paesi UE e la dinamica di questo nel corso del tempo, determinata dalla variazione percentuale del punteggio

IBI che intercorre tra un anno e l'altro, si opera una distinzione tra i Paesi secondo le seguenti categorie:

- *Last movers:* paesi che registrano valori bassi nell'indice IBI e un basso tasso di crescita;
- *First movers:* paesi che si attestano tra i primi in classifica, ma il cui tasso di crescita è minore rispetto alla media delle variazioni degli altri paesi;
- *Best movers:* paesi che occupano i gradini più alti della classifica e che presentano una crescita superiore alla media UE;
- *Fast movers:* paesi che presentano un grado di variazione elevato ma che partono da un IBI basso.

L'**Italia** continua a posizionarsi nel cluster dei Paesi *fast movers*, ossia quelli che, pur partendo da livelli di sviluppo digitale inferiore alla media, presentano una buona dinamica di crescita nel tempo. Ciò significa che, nonostante un posizionamento non elevato nella classifica generale, il relativo miglioramento rispetto all'anno precedente è stato netto e superiore al miglioramento medio degli altri Paesi. Indubbiamente, questo risultato è guidato dai progressi ottenuti sul lato dell'offerta, specie per quanto riguarda la copertura della rete 5G. Infatti, nel grafico *movers* sull'offerta di connettività, l'Italia si posiziona tra i Paesi *best movers* (Fig. 6.2).

Sul fronte della domanda, il nostro Paese si trova tra i ***fast movers*** (Fig. 6.3) e tale posizionamento denota che seppur partendo nella maggior parte dei casi da valori al di sotto della media europea per quasi la totalità degli indicatori relativi alla domanda di connettività, l'Italia evidenzia una buona dinamica di crescita nel tempo, con una variazione percentuale più marcata rispetto alla media, soprattutto grazie alla crescita dell'e-government, della connessione in banda larga delle famiglie e della digitalizzazione delle imprese. Un segnale incoraggiante che tuttavia andrebbe accelerato qualora l'Italia voglia conseguire nel volgere di pochi anni una posizione di vantaggio rispetto alla media UE, come peraltro ha già fatto da qualche anno un Paese a noi affine come la Spagna.

Fig. 6.1: Livello e dinamica della digitalizzazione complessiva

Fonte: elaborazioni I-Com su dati DESI e Eurostat

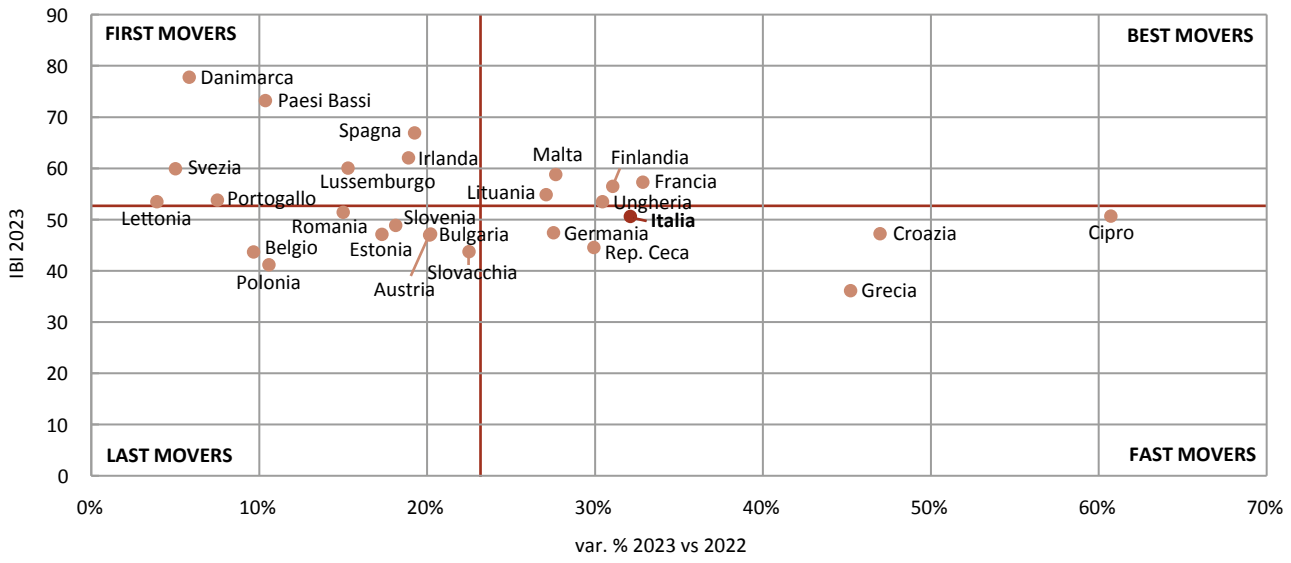


Fig. 6.2: Livello e dinamica della offerta digitale

Fonte: elaborazioni I-Com su dati DESI e Eurostat

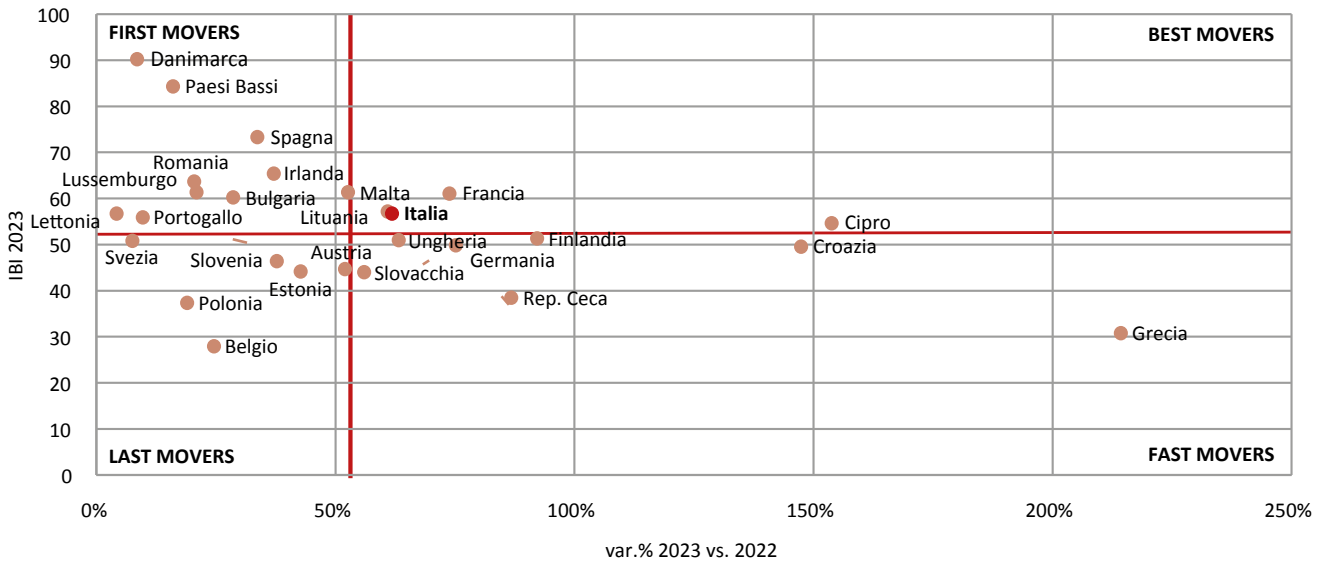
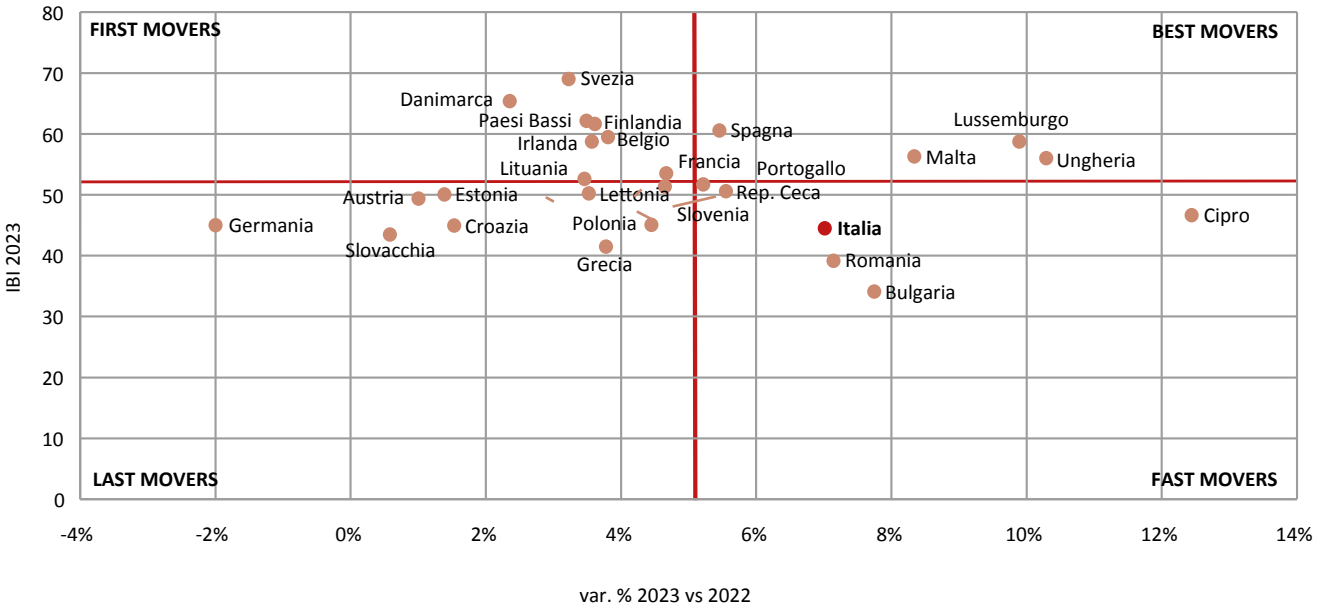


Fig. 6.3: Livello e dinamica della domanda digitale

Fonte: elaborazioni I-Com su dati DESI e Eurostat



6.3. NOTA DI CALCOLO

L'indice complessivo viene calcolato come una normalizzazione in cui il massimo e il minimo sono due ipotetici stati del mondo corrispondenti all'assoluta perfezione in termini di domanda e/o offerta di connettività (tutte le percentuali corrispondono al 100%) o all'assenza completa di domanda e/o offerta di connettività (tutte le percentuali pari allo 0%).

Una normale formula di normalizzazione è $(x_i - x_{min})/(x_{max} - x_{min})$. Nel caso specifico, il valore minimo di *x* è stato posto uguale a 0, mentre il valore massimo corrisponde a 100. La normalizzazione viene svolta per tre volte:

- Per l'IBI complessivo, seguendo la formula $IBI = \sum_{i=1}^{12} x_{i,c,t} /1200$, in quanto contiene 12 variabili per le quali il valore massimo è posto uguale a 100. $x_{i,c,t}$ è il valore di una cella che riporta il dato di un variabile *i,* per un paese *c*, in uno specifico anno *t.*
- Per le componenti di domanda e offerta si calcola invece $IBI_{dom/off} = \sum_{i=1}^{6} x_{i_{dom/off},c,t} /600$, perché ciascuna componente consta di 6 variabili, ciascuna delle quali ha valore massimo posto uguale a 100.

Ogni punteggio IBI viene poi moltiplicato per 100, in modo da trasformare il valore percentuale sottoforma di numero[34].

La comparazione annuale avviene su tre anni (2020, 2021, 2022), per i quali sono disponibili i dati.

Si è verificato il caso di alcuni valori mancanti per il 2021 e il 2022. È stato possibile stimare tali valori grazie al dato 2020, secondo due fattispecie:

1. Quando il dato mancante è quello per il 2021, questo si stima come la media aritmetica tra dato 2020 e dato 2022,
2. Quando il dato mancante è quello per il 2022, il valore viene calcolato applicando la seguente formula al dato dell'anno precedente:

$$x_{2022} = x_{2021} + [\frac{x_{2021}(x_{2021} - x_{2020})}{x_{2020}}]$$

Per l'anno 2020, i valori laddove mancanti sono stati conteggiati come 0.

34 Per maggiori informazioni circa la nuova metodologia adoperata per il calcolo dell'IBI si veda il RAPPORTO OSSERVATORIO RETI E SERVIZI DI NUOVA GENERAZIONE OTTOBRE 2022: Le politiche per muovere la trasformazione digitale dell'Italia tra bussola UE e PNRR – https://www.i-com.it/wp-content/uploads/2022/10/Rapporto_Ores_2022-2.pdf

icom
istituto per la competitività

CAPITOLO 7

LO STATO DI AVANZAMENTO DEI PROGETTI DEL PNRR IN AMBITO DIGITALE

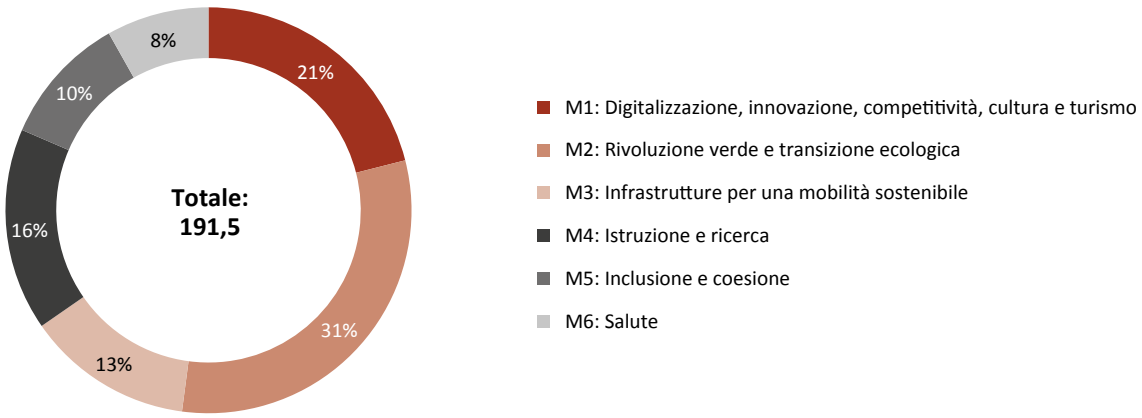
7.1. IL DIGITALE NEI 6 PILLAR DEL PNRR

Il Piano Nazionale di Ripresa e Resilienza non rappresenta esclusivamente uno slancio per il ripresa dell'economia nazionale a seguito della crisi pandemica ma anche un volano utile a dar vita ad una **crescita più robusta, sostenibile e inclusiva** del nostro Paese. Il PNRR ha una dotazione economica di **191,5 miliardi** di euro e si articola in **6 Missioni**, ovvero aree tematiche principali su cui intervenire attraverso investimenti e riforme, individuate in piena coerenza con i pilastri del **Next Generation EU**: transizione verde; trasformazione digitale; coesione economica, produttività e competitività; coesione sociale e territoriale; resilienza sanitaria, economica, sociale e istituzionale; politiche per le prossime generazioni.
Le sei missioni in cui si articola il PNRR sono denominate (Fig. 7.1): Digitalizzazione, innovazione, competitività, cultura e turismo; Rivoluzione verde e transizione ecologica; Infrastrutture per una mobilità sostenibile; Istruzione e ricerca; Inclusione e coesione; Salute.
La digitalizzazione ricopre un ruolo cruciale nella pianificazione essendo il tema connotante del primo dei sei pilastri del PNRR. Alla Missione 1 sono destinati complessivamente **€40,29 miliardi, pari al 21% del totale**, il che la rende la seconda per volume di risorse assegnate. Il 70% di tali fondi è destinato ad investimenti specificatamente legati alla transizione digitale del sistema paese. Ciascuna delle parti della Missione ha come obiettivo principale il potenziamento di specifici settori dell'economia nazionale: la Pubblica Amministrazione (C1), le Imprese (C2), e il settore Turismo e Cultura (C3).
Per quanto concerne la prima componente, sono stati stanziati €9,72 miliardi per sostenere la Pubblica Amministrazione nel suo processo di transizione digitale e innovazione. La componente 1 è ulteriormente suddivisa in tre sotto-componenti:

- **Digitalizzazione della PA** (10 iniziative, 7 investimenti e 3 riforme): Questo settore si concentra principalmente sul miglioramento delle infrastrutture digitali, del processo di acquisto delle tecnologie informatiche, sulla creazione di un cloud nazionale, sulla digitalizzazione dei principali uffici amministrativi, sull'aggiornamento e lo sviluppo dei servizi digitali per i cittadini e delle relative piattaforme, sull'incremento delle competenze digitali del personale e sull'interoperabilità delle banche dati delle

Fig. 7.1: Le 6 Missioni del PNRR

Fonte: PNRR, Italia Domani



pubbliche amministrazioni. Inoltre, sono stati destinati **€620 milioni alla cybersicurezza**.

- **Innovazione della PA** (6 iniziative, 3 investimenti e 3 riforme): Questa sotto-componente si concentra sulla modernizzazione della Pubblica Amministrazione italiana, includendo la riforma del processo di selezione del personale attraverso una nuova piattaforma digitale per il reclutamento, la creazione di una task-force temporanea per semplificare e velocizzare alcune procedure amministrative, il potenziamento delle competenze del personale e la completa digitalizzazione dei processi interni della PA.
- **Innovazione del Sistema Giudiziario** (2 investimenti): Questa parte prevede investimenti nel capitale umano e per rafforzare il settore della giustizia amministrativa.

Come già anticipato, la prima Missione del PNRR non si limita alla riforma della PA, ma investe anche nell'innovazione del sistema produttivo nazionale. La seconda componente infatti è denominata "Digitalizzazione, Innovazione e Competitività nel Sistema Produttivo" ed è composta da 7 misure (6 investimenti e una riforma) con un budget di €23,89 miliardi. Il principale focus di investimento è rappresentato dal programma denominato **"Transizione 4.0"** un piano pluriennale concepito per promuovere la trasformazione digitale dei processi produttivi, stimolare la ricerca sia applicata che di base, e incentivare gli investimenti in beni immateriali (vedi par. 7.2.1). Per questo ambizioso progetto è stato destinato un budget di €13,38 miliardi, posizionandolo come uno degli investimenti più rilevanti non solo nell'ambito della digitalizzazione e dell'innovazione ma dell'intero PNRR. Altri provvedimenti contemplati includono **lo sviluppo delle reti VHCN** (Very High Capacity Network) e investimenti nel campo della tecnologia satellitare. Ulteriori risorse sono dirette a sostenere le Piccole e Medie Imprese (PMI), promuovendo la loro internazionalizzazione e migliorando il quadro normativo in materia di proprietà industriale.

La terza e ultima componente della Missione 1 si concentra sul rilancio del settore turistico e culturale, due pilastri cruciali dell'economia italiana che hanno subito profonde ripercussioni a causa della pandemia. Il budget assegnatole ammonta a €6,68 miliardi destinato ad incrementare l'attrattività del Paese mediante l'ammodernamento delle sue attrazioni turistiche e la valorizzazione dei siti storici e culturali. Essa si articola in 14 interventi, di cui 12 sono investimenti e 2 sono riforme, distribuiti in quattro principali ambiti: la preservazione del patrimonio culturale per le future generazioni, la valorizzazione dei luoghi di interesse religioso e rurale, l'evoluzione dell'"**industria della cultura 4.0**" e l'innovazione del settore turistico con il concetto di "**turismo 4.0"**. Tra i vari interventi, quelli più strettamente connessi al settore digitale includono gli investimenti 1.1, focalizzati sulla "Strategia digitale e piattaforme per i beni culturali," e gli interventi 3.1 e 3.2, incentrati sull'"industria culturale e creativa 4.0.

Tab. 7.1: L'allocazione delle risorse della Missione 1 del PNRR (€ miliardi)

Fonte: PNRR, Italia Domani

40,29 **Totale Missione 1**	M1C1 – DIGITALIZZAZIONE, INNOVAZIONE E SICUREZZA NELLA PA	9,72
	M1C2 – DIGITALIZZAZIONE, INNOVAZIONE E COMPETITIVITÀ NEL SISTEMA PRODUTTIVO	23,89
	M1C3 – TURISMO E CULTURA 4.0	6,68

Pur avendo un ruolo primario nell'ambito della Missione 1, l'elemento digitale (*digital tag*) è trasversale rispetto a tutte le altre missioni del piano (come evidenziato nella tabella 7.2). Questo rappresenta infatti un prerequisito necessario e non trascurabile per raggiungere gli obiettivi delineati in tutto il PNRR. **Considerando l'insieme delle missioni, l'ammontare totale delle risorse allocate alla transizione digitale è di €48,09 miliardi**, circa il 25% del totale della dotazione del Piano. Questa percentuale è in linea con il requisito stabilito dall'Unione Europea, che richiede di destinare almeno il 20% delle risorse agli obiettivi digitali.

Nella Missione 2, intitolata "Rivoluzione verde e transizione ecologica," sono stati stanziati €59,46 miliardi. Il 3% di questi fondi (€1,91 miliardi) sarà utilizzato per implementare misure legate alla digitalizzazione. L'investimento più rilevante in questo contesto è presente nella seconda componente della missione, incentrata su "Energia rinnovabile, idrogeno, rete e mobilità sostenibile." L'investimento 2.1, con un budget **di €3,61 miliardi, è mirato al potenziamento delle "reti intelligenti"**.

La Missione 3 del PNRR, "Infrastrutture per una mobilità sostenibile," concentra la sua attenzione sulla transizione ecologica, in particolare sull'ammodernamento della rete ferroviaria, includendo interventi di **digitalizzazione dei sistemi logistici**. Le risorse destinate alla trasformazione digitale in questa Missione ammontano a €3,3 miliardi, pari a circa il 13% dei suoi €25,40 miliardi.

La Missione 4, denominata "Istruzione e ricerca," presenta una notevole sinergia con la transizione digitale, con il 24% delle risorse, ovvero €7,48 miliardi, destinate a interventi e misure riguardanti la digitalizzazione. Gli investimenti più rilevanti sono concentrati nella prima componente (M4.C1), "Potenziamento dell'offerta dei servizi di istruzione: dagli asili nido alle università".

La Missione 5 riguarda il rilancio del mercato del lavoro. Essa dedica il 14% delle risorse, pari a €2,70 miliardi su un totale di €19,85 miliardi, alla digitalizzazione. Le misure principali comprendono politiche attive del lavoro, investimenti nel servizio civile universale per promuovere la formazione digitale, ed interventi nel settore dello sport e dell'inclusione sociale.

In conclusione, anche la Missione 6 del PNRR intitolata "Salute" prevede risorse significative per la **transizione digitale del settore sanitario**, pari a €4,40

Tab. 7.2: Le risorse con tag digitale nel PNRR

Fonte: PNRR, Italia Domani[35]

Titolo	Risorse (€ mld)	Tag digitale (€ mld)	Quota digitale
Missione 1 – Digitalizzazione, innovazione, competitività, cultura e turismo	40,29	28,28	70%
Missione 2 – Rivoluzione verde e transizione ecologica	59,46	1,91	3%
Missione 3 – Infrastrutture per una mobilità sostenibile	25,40	3,33	13%
Missione 4 – Istruzione e ricerca	30,88	7,48	24%
Missione 5 – Inclusione e coesione	19,85	2,70	14%
Missione 6 – Salute	15,63	4,40	28%
Totale	191,50	48,09	25%

35 Dati aggiornati a marzo 2023

miliardi (28% delle risorse totali). Le misure principali sono presenti nella seconda componente, miranti all'ammodernamento delle infrastrutture tecnologiche ospedaliere e sulla **creazione di una solida infrastruttura per la raccolta, l'elaborazione e l'analisi dei dati sanitari**. In particolare, sono previsti investimenti nella creazione di un ***National Health Prevention Hub*** per affrontare eventuali nuove pandemie.

7.2. LO STATO DI AVANZAMENTO DEI PROGETTI

7.2.1. In attesa di Transizione 5.0

La transizione digitale delle imprese è senza dubbio uno degli obiettivi più importanti e sfidanti in chiave competitività del sistema paese.

In tale logica, nel 2016 è stato lanciato il Piano Nazionale Industria 4.0, con il quale si mirava, appunto, a **sostenere ed incentivare l'innovazione tecnologica del tessuto imprenditoriale italiano**, caratterizzato per la maggior parte da **piccole e medie imprese** operanti nel settore manifatturiero e da una bassa crescita della produttività, seguendo tre linee guida principali che prevedevano azioni orizzontali volte ad agire sui fattori abilitanti secondo una logica di neutralità tecnologica. Gli strumenti previsti, in particolare, erano:

- **iper e superammortamento:** iperammortamento del 250% nel caso di acquisto di beni materiali nuovi, dispositivi e tecnologie abilitanti la trasformazione in chiave 4.0, inseriti nell'Allegato A della Legge di Stabilità 2017 – Legge n. 232/2016 (inclusi i beni che già comprendono un software necessario per il loro funzionamento) e superammortamento del 140% per l'acquisto di beni immateriali (software, sistemi e *system integration*, piattaforme e applicazioni) inseriti nell'All. B alla stessa legge, compiuti da imprese che già hanno beneficiato dell'iperammortamento.
- **Beni Strumentali (Nuova Sabatini)**: finalizzata a migliorare l'accesso al credito delle micro, piccole e medie imprese per l'acquisto di nuovi macchinari, impianti e attrezzature, consente alle imprese di ottenere un contributo a parziale copertura degli interessi su finanziamenti bancari di importo compreso tra €20 mila e €2 milioni, concessi da istituti bancari convenzionati con il MISE. Il contributo era calcolato sulla base di un piano di ammortamento convenzionale di 5 anni con un tasso d'interesse del 2,75% annuo ed era maggiorato del 30% per investimenti in tecnologie Industria 4.0.
- **Credito d'imposta R&D**: credito d'imposta del 50% su spese incrementali in Ricerca e Sviluppo. È riconosciuto fino a un massimo annuale di 20 mln di €/anno per beneficiario e computato su una base fissa data dalla media delle spese in Ricerca e Sviluppo negli anni 2012-2014. Rientrano nel beneficio tutte le spese relative a ricerca fondamentale, ricerca industriale e sviluppo sperimentale e, dunque, quelle relative all'assunzione di personale altamente qualificato e tecnico, contratti di ricerca con università, enti di ricerca, imprese, startup e PMI innovative, quote di ammortamento di strumenti e attrezzature di laboratorio, privative industriali, ecc.
- **Patent Box**: riduzione delle aliquote IRES e IRAP del 50% dal 2017 in poi, sui redditi d'impresa connessi all'uso diretto o indiretto (ovvero in licenza d'uso) di beni immateriali sia nei confronti di controparti terze che di controparti correlate (società infragruppo) a patto che il contribuente conduca attività di R&S connesse allo sviluppo e al mantenimento dei beni immateriali;
- **Misure a favore di Startup e PMI innovative**: previsione di una serie di vantaggi in modo da

sostenere le imprese innovative in tutte le fasi del loro ciclo di vita (es. nuova modalità di costituzione digitale e gratuita, *Equity crowdfunding* per la raccolta di nuovi capitali di rischio, esonero dalla disciplina fallimentare ordinaria, incentivi agli investimenti in capitale di rischio quali detrazione IRPEF – per investimenti fino a €1 milione – o deduzione dell'imponibile IRES – fino a €1,8 milioni – pari al 30%).

Se questo era il punto di partenza, sono ampie e numerose le modifiche intervenute nel tempo e che hanno condotto al superamento del Piano Nazionale Industria 4.0, dapprima in favore del Piano Nazionale Impresa 4.0 (ad opera della legge di bilancio 2018) e, infine, del Piano Transizione 4.0, che da ultimo è stato rimodulato ad opera del PNRR. Come anticipato nel paragrafo precedente, nell'ambito della Missione 1 – Componente 2 "Digitalizzazione, innovazione e competitività del sistema produttivo", è stato previsto l'Investimento 1 **"Transizione 4.0"** che, con una dotazione finanziaria di €13,381 miliardi (a cui si aggiungono €5,08 miliardi del Fondo complementare), persegue l'obiettivo di sostenere la trasformazione digitale delle imprese.

Rispetto alle modifiche normative introdotte, la legge di bilancio 2020 ha disposto il superamento del sistema dell'iperammortamento e del superammortamento, in favore di un **credito d'imposta**, su cui è intervenuta in ultimo la legge di bilancio 2022 (così come modificata dal decreto Milleproroghe) per il triennio 2023-2025, la quale ha inserito una serie di correttivi anche alla luce degli obiettivi del PNRR, includendo la scadenza del regime di favore per l'acquisto di beni materiali e immateriali tradizionali e le attività di formazione 4.0. In particolare, per i beni materiali 4.0[36] è stato stabilito un dimezzamento per tutte le classi di investimento: dal 40% al 20% fino a €2,5 milioni; dal 20% al 10% da €2,5 a 10 milioni; dal 10% al 5% da €10 a 20 milioni. Per quanto riguarda i beni immateriali 4.0[37], dal 50 al 20% (fino a un tetto di €1 milione). Mentre vale ancora la regola del dimezzamento (dal 20 al 10%) per le attività di ricerca di base, industriale e sperimentale.

Oltre al superamento dell'iperammortamento e del superammortamento, anche la misura Beni Strumentali (c.d. Nuova Sabatini) è stata oggetto di modifica nel corso degli anni. In particolare, si tratta di un'agevolazione che sostiene gli investimenti di micro, piccole e medie imprese (PMI) attive in ogni settore produttivo – eccetto attività finanziarie e assicurative ed attività connesse all'esportazione e per gli interventi subordinati all'impiego preferenziale di prodotti interni rispetto ai prodotti di importazione – per acquistare o acquisire in leasing

36 Beni ricompresi nell'Allegato A alla legge di bilancio 2017, ossia: i) i) beni strumentali il cui funzionamento è controllato da sistemi computerizzati o gestito tramite opportuni sensori e azionamenti (che comprendono numerose tipologie di macchine utensili, robot, robot collaborativi e sistemi multi-robot) di cui lo stesso allegato descrive le caratteristiche indispensabili; ii) sistemi per l'assicurazione della qualità e della sostenibilità, tra cui rientrano sistemi di monitoraggio in process, per l'ispezione e la caratterizzazione dei materiali, sistemi intelligenti e connessi di marcatura e tracciabilità dei lotti produttivi e/o dei singoli prodotti, di monitoraggio e controllo delle condizioni di lavoro delle macchine; iii) dispositivi per l'interazione uomo macchina e per il miglioramento dell'ergonomia e della sicurezza del posto di lavoro in logica «4.0» ed in particolare banchi e postazioni di lavoro dotati di soluzioni ergonomiche in grado di adattarli in maniera automatizzata alle caratteristiche fisiche degli operatori, sistemi per il sollevamento/traslazione di parti pesanti o oggetti esposti ad alte temperature, dispositivi wearable, apparecchiature di comunicazione tra operatore/ operatori e sistema produttivo, dispositivi di realtà aumentata e virtual reality ed interfacce uomo-macchina (HMI) intelligenti che coadiuvano l'operatore a fini di sicurezza ed efficienza delle operazioni di lavorazione, manutenzione, logistica.

37 Beni ricompresi nell'Allegato B alla legge di bilancio 2017, tra cui beni immateriali (software, sistemi e system integration, piattaforme e applicazioni) connessi a investimenti in beni materiali «Industria 4.0» come ad es. software, sistemi, piattaforme e applicazioni di artificial intelligence & machine learning, per la produzione automatizzata e intelligente, software, sistemi, piattaforme e applicazioni in grado di comunicare e condividere dati e informazioni sia tra loro che con l'ambiente e gli attori circostanti (Industrial internet of Things) grazie ad una rete di sensori intelligenti interconnessi, ecc.

macchinari, attrezzature, impianti, beni strumentali ad uso produttivo e hardware, nonché software e tecnologie digitali.

Il finanziamento è un altro strumento di sostegno straordinariamente rilevante, date le seguenti caratteristiche: deve avere durata non superiore a 5 anni, di importo compreso tra €20 mila e €4 milioni e interamente utilizzato per coprire gli investimenti ammissibili. Esso viene concesso da parte di banche e intermediari finanziari – può essere assistito dalla garanzia del "Fondo di garanzia per le piccole e medie imprese" fino all'80% dell'ammontare del finanziamento stesso – a cui si affianca un contributo da parte del Ministero delle Imprese e del Made in Italy, il quale viene rapportato agli interessi sui predetti finanziamenti. Più in dettaglio, il contributo è erogato dal Ministero alle PMI beneficiarie in quote annuali, così come riportato nel relativo provvedimento di concessione, il quale si esaurisce entro il sesto anno dalla data di ultimazione dell'investimento. Dal punto di vista delle risorse, dopo una serie di rifinanziamenti si è visto allocare, dalla legge di bilancio 2022, €240 milioni per ciascuno degli anni 2022 e 2023, €120 milioni per ciascuno degli anni dal 2024 al 2026, €60 milioni per il 2027.

Partendo dal monitoraggio sull'efficacia delle misure fiscali ed al fine di focalizzare l'attenzione e la trasformazione digitale anche in chiave di sostenibilità ambientale la legge di bilancio 2020 e, successivamente, le leggi di bilancio 2021 e 2022, hanno prorogato e rimodulato anche il credito di imposta R&D**.** Nello specifico, tale credito è riconosciuto:

a. per investimenti in **ricerca e sviluppo**:
   i. fino al periodo di imposta in corso al 31 dicembre 2022, in misura pari al 20% della relativa base di calcolo e nel limite di €4 milioni;
   ii. per i successivi periodi d'imposta, fino al 2031, in misura pari al 10% della relativa base di calcolo, assunta al netto delle altre sovvenzioni o dei contributi a qualunque titolo ricevuti per le stesse spese, e nel limite di €5 milioni;
b. per le attività di **innovazione tecnologica e di design e ideazione estetica** (prorogato fino al periodo d'imposta 2025):
   i. per i periodi d'imposta 2022 e 2023, nella misura del 10% nel limite annuo di €2 milioni;
   ii. per i periodi d'imposta 2024 e 2025, nella misura del 5%, nel limite annuo di €2 milioni;
c. per le attività di **innovazione tecnologica finalizzate alla realizzazione di prodotti o processi di produzione nuovi o sostanzialmente migliorati per il raggiungimento di un obiettivo di transizione ecologica o di innovazione digitale 4.0**, il credito d'imposta è prorogato sino al periodo d'imposta 2025 ed è riconosciuto, per il periodo d'imposta 2022, nella misura del 15% nel limite di €2 milioni. Per il periodo di imposta 2023 è riconosciuto in misura del 10% nel limite massimo annuo di €4 milioni e, per i periodi d'imposta 2024 e 2025, nella misura del 5% sempre nel limite di €4 milioni.

Rispetto a ricerca ed innovazione, con decreto del 14 novembre 2022, il Ministero delle imprese e made in Italy (MIMIT) ha sbloccato €500 milioni, a valere sul Fondo nazionale complementare al PNRR, per finanziare progetti di ricerca e sviluppo nell'ambito del secondo sportello dedicato agli Accordi per l'innovazione, la cui graduatoria finale è stata pubblicata il 17 febbraio scorso. Si tratta di benefici rivolti alle imprese di qualsiasi dimensione, anche in forma congiunta, che esercitano attività industriali, agroindustriali, artigiane o di servizi all'industria nonché attività di ricerca (mentre per le imprese agricole è prevista la possibilità di partecipare nell'ambito di progetti congiunti). I

progetti di ricerca e sviluppo, che devono rientrare nelle aree di intervento[38] riconducibili al secondo Pilastro del Programma quadro di ricerca e innovazione "Orizzonte Europa", di cui al Regolamento (UE) 2021/695 del Parlamento europeo e del Consiglio del 28 aprile 2021, devono prevedere spese e costi ammissibili non inferiori a €5 milioni, avere una durata non superiore a 36 mesi ed essere avviati successivamente alla presentazione della domanda di agevolazioni al Ministero.

Anche la disciplina del **Patent Box**, ossia il regime opzionale con tassazione agevolata sui redditi derivanti dall'utilizzo di taluni beni immateriali introdotto nel 2015, ha subito una vera e propria rivoluzione. Se fino al 2019 al contribuente era richiesta la preventiva sottoscrizione di un accordo con l'Agenzia delle entrate (c.d. ruling obbligatorio che diventava facoltativo nel caso di concessione in uso del bene o di plusvalenze realizzate in ambito infragruppo), successivamente si è passati al sistema dell'autoliquidazione del relativo beneficio fino a quando, nel 2021, il decreto fiscale 2021 (articolo 6 del decreto-legge n. 146 del 2021) ne ha completamente ridisegnato la disciplina sostituendo l'originaria misura, con un'agevolazione che consente di maggiorare (in origine del 90%, poi del 110% a seguito dell'innalzamento disposto dalla legge di bilancio 2022), ai fini delle imposte sui redditi e dell'imposta regionale sulle attività produttive, le spese sostenute dall'impresa in relazione a software protetto da copyright, brevetti industriali, disegni e modelli, che siano utilizzati dagli stessi soggetti direttamente o indirettamente nello svolgimento della propria attività di impresa.

Nonostante le importanti modifiche ed innovazioni introdotte nel corso degli anni, non può non segnalarsi come **l'Allegato A continui a non comprendere gli elementi abilitanti le comunicazioni tra dispositivi**. Si tratta di un vulnus importante ove si consideri la crescente importanza assunta da nuove tecnologie come IoT, intelligenza artificiale (IA), realtà virtuale (VR) e realtà aumentata (AR), in grado di promuovere l'efficienza operativa e ottimizzare i processi attraverso i trasporti, la logistica, la catena di approvvigionamento e le spedizioni, che impone, evidentemente, l'accesso ad infrastrutture di connettività all'avanguardia comprese reti 5G private.

Il ministro delle Imprese e del Made in Italy, Adolfo Urso, già da diversi mesi ha annunciato l'intenzione del Governo di inaugurare un nuovo piano che potrebbe essere denominato Transizione 5.0, la cui fonte di finanziamento, per 4,04 mld di euro, è stata individuata nel piano RePower EU. Nel mese di agosto è stata dunque inviata dall'Italia alla Commissione Europea una proposta in tal senso in attesa di essere approvata.

Sebbene sia la presentazione della legge di bilancio la sede deputata alla definizione della cornice normativa del nuovo piano, secondo le notizie informalmente circolate, il Piano Transizione 5.0 dovrebbe confermare le aliquote attualmente previste fino al 2025 per gli investimenti in beni strumentali 4.0 sopra descritte, con la speranza che vada in qualche modo ad includere anche le infrastrutture di rete, ma dovrebbe al contempo disporre un'importante novità, ossia la previsione di premialità – che potrebbero addirittura raddoppiare le aliquote – nel caso in cui gli investimenti, oltre a rispondere ai requisiti previsti dalla normativa per i beni 4.0, offrano benefici tangibili in ottica green. Sembrerebbe anche in discussione la necessità di

38 Tecnologie di fabbricazione, tecnologie digitali fondamentali, comprese le tecnologie quantistiche, tecnologie abilitanti emergenti, materiali avanzati, Intelligenza artificiale e robotica, industrie circolari, industria pulita a basse emissioni di carbonio, malattie rare e non trasmissibili, impianti industriali nella transizione energetica, competitività industriale nel settore dei trasporti, mobilità e trasporti puliti, sicuri e accessibili, mobilità intelligente, stoccaggio dell'energia, sistemi alimentari, sistemi di bioinnovazione nella bioeconomia dell'Unione e sistemi circolari.

dimostrare i requisiti attraverso una perizia nonché la possibilità, per le aziende, di ottenere una certificazione che metta al riparo da imprevedibili criticità in sede di verifiche fiscali.

7.2.2. Sanità digitale – Telemedicina

La digitalizzazione della sanità, in linea con il Piano Nazionale di Ripresa e Resilienza (PNRR), riveste un ruolo cruciale nel rendere più efficiente, moderno e inclusivo il Servizio Sanitario Nazionale. La pandemia da Covid-19 ha reso evidente, fra i diversi aspetti critici di natura strutturale, un'inadeguata integrazione dei servizi ospedalieri e territoriali. Tale esperienza ha però al contempo evidenziato le grandissime potenzialità offerte dalle nuove tecnologie nell'erogazione delle prestazioni mediche e del monitoraggio dei pazienti per via telematica.

I servizi della sanità digitale costituiscono un prezioso strumento per affrontare le sfide principali del Sistema Sanitario Nazionale. Questi danno la possibilità di ridurre le disparità geografiche e territoriali nell'accesso alle cure, garantendo un livello uniforme di assistenza grazie all'adozione di tecnologie innovative. Parallelamente possono migliorare l'esperienza di cura per i pazienti, rendendo l'assistenza medica più accessibile. Infine, contribuiscono a potenziare l'efficienza dei sistemi sanitari regionali promuovendo la possibilità di fornire assistenza a domicilio e di monitorare i pazienti da remoto.

Come già sottolineato il PNRR dedica al comparto della sanità l'intera Missione 6 – "Salute" e si divide in due componenti:

- **M6C1 – Reti di prossimità, strutture e telemedicina per l'assistenza sanitaria territoriale**, per cui sono stanziate risorse per un totale di 7 miliardi di euro. Questa componente si suddivide in una riforma "Reti di prossimità, strutture e telemedicina per l'assistenza sanitaria territoriale e rete nazionale della salute, ambiente e clima" e tre investimenti: "Case della Comunità e presa in carico della persona" (2 miliardi di euro); "Casa come primo luogo di cura e telemedicina" (4 miliardi di euro); "Rafforzamento dell'assistenza sanitaria intermedia e delle sue strutture" (un miliardo di euro).
- **M6C2 – Innovazione, ricerca e digitalizzazione del servizio sanitario nazionale**, cui sono dedicati 8,63 miliardi di euro. Questa si suddivide nella riforma utile a "riorganizzare gli Istituti di Ricovero e Cura a Carattere Scientifico" e in due subcomponenti (che comprendono 5 investimenti complessivi): "Aggiornamento tecnologico e digitale" (per la quale sono destinati 7,36 miliardi di euro) e "Formazione, ricerca scientifica e trasferimento tecnologico" (cui sono riservati 1,26 miliardi di euro).

Come si evince chiaramente dalle denominazioni delle varie misure descritte, uno degli obiettivi principali dell'intervento è quello di rendere più moderno ed efficace il SSN italiano grazie al ricorso a soluzioni tecnologiche innovative. In sintesi, la prima componente intende rafforzare le prestazioni

Tab. 7.3: L'allocazione delle risorse della Missione 6 del PNRR (€ miliardi)

Fonte: PNRR, Italia Domani

15,63 **Totale Missione 6**	M6C1 – RETI DI PROSSIMITÀ, STRUTTURE E TELEMEDICINA PER L'ASSISTENZA SANITARIA TERRITORIALE	7,00
	M6C2 – INNOVAZIONE, RICERCA E DIGITALIZZAZIONE DEL SERVIZIO SANITARIO NAZIONALE	8,63

Tab. 7.4: Allocazione delle risorse nella componente 1 (€ miliardi)

Fonte: PNRR, Italia Domani

Misure	Risorse
Riforma 1: Reti di prossimità, strutture e telemedicina per l'assistenza sanitaria territoriale e rete nazionale della salute, ambiente e clima	-
Investimento 1: Case della comunità e presa in carico della persona	2
Investimento 2: Casa come primo luogo di cura e telemedicina	4
Investimento 3: Rafforzamento dell'assistenza sanitaria intermedia e delle sue strutture (Ospedali di Comunità)	1
Totale	**7**

erogate sul territorio grazie al potenziamento e alla creazione di strutture e presidi territoriali, al rafforzamento dell'assistenza domiciliare e allo **sviluppo della telemedicina**. La seconda invece mira al **rinnovamento e l'ammodernamento delle strutture tecnologiche e digitali esistenti**, al completamento e diffusione del **Fascicolo Sanitario Elettronico (FSE)** e al miglioramento della capacità di erogazione e monitoraggio dei Livelli Essenziali di Assistenza (LEA) attraverso **più efficaci sistemi informativi**. Rilevanti risorse sono destinate anche alla ricerca scientifica e al **miglioramento delle competenze digitali** del personale attivo nel comparto.

Analizzando nel dettaglio la composizione e lo stato di avanzamento degli interventi previsti, vediamo come l'investimento 1.2 della prima componente è il principale intervento a sostegno della diffusione della telemedicina (con un ammontare di risorse pari a 4 miliardi di euro). Questo mira ad aumentare il volume delle prestazioni rese in assistenza domiciliare fino a prendere in carico, entro la metà del 2026, il 10 percento della popolazione nazionale di età superiore ai 65 anni.

In particolare l'investimento punta a:

- Identificare un modello condiviso per **l'erogazione delle cure domiciliari** che sfrutti al meglio le possibilità offerte dalle nuove tecnologie, specialmente la telemedicina, la domotica e la digitalizzazione in generale;
- Realizzare presso ogni Azienda Sanitaria Locale (ASL) un **sistema informativo in grado di rilevare dati clinici in tempo reale**;
- Attivare 602 Centrali Operative Territoriali (COT), una in ogni distretto, con la funzione di coordinare i servizi domiciliari con gli altri servizi sanitari, assicurando l'interfaccia con gli ospedali e la rete di emergenza-urgenza;
- **Utilizzare la telemedicina per supportare al meglio i pazienti con malattie croniche.**

Quest'intervento si traduce nel finanziamento di progetti di telemedicina proposti dalle Regioni sulla base delle priorità e delle linee guida definite dal Ministero della Salute. Per ottenere i finanziamenti, tuttavia, i progetti dovranno innanzitutto potersi integrare con il Fascicolo Sanitario Elettronico. Riguardo lo stato di avanzamento dell'investimento 1.2, degli 8 target da raggiungere nel 2023 (uno dei quali a dicembre) ne è stato conseguito solo uno[39], va comunque sottolineato che rispetto agli altri le percentuali di completamento sono generalmente elevate.

Passando alla seconda componente della Missione 6, possiamo vedere come all'"Aggiornamento

39 Dai dati del Ministero della salute (che saranno utilizzati per gli stati di avanzamento anche degli altri investimenti e riforme che seguono), delle percentuali di aggiornamento dei target quattro sono state aggiornate a luglio 2023, una a maggio e una a giugno.

Tab. 7.5: Allocazione delle risorse nella componente 2 (€ miliardi)

Fonte: PNRR, Italia Domani

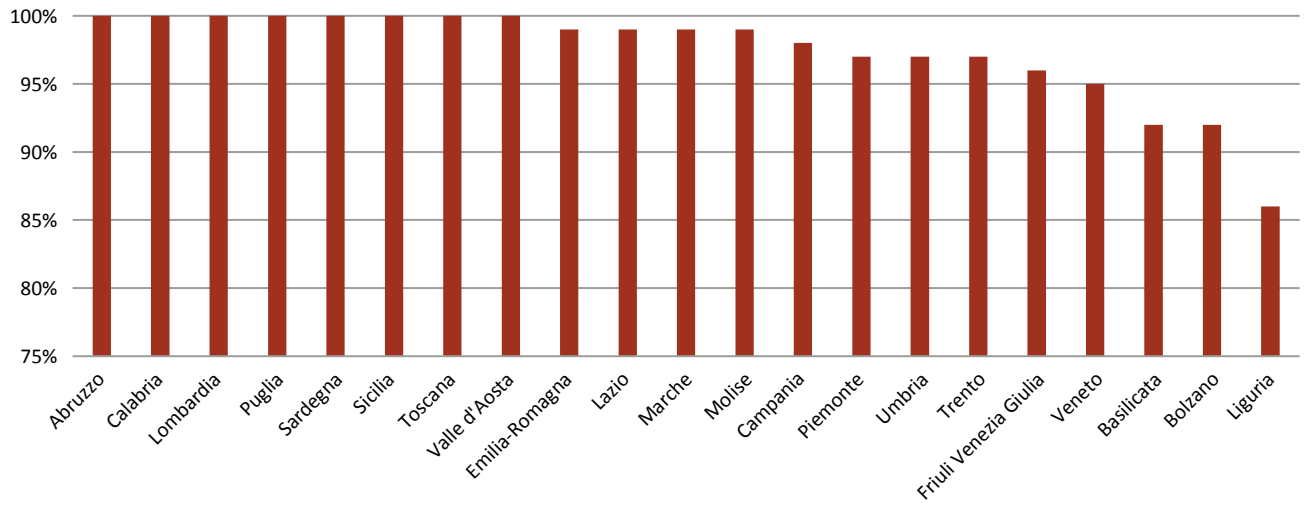
Misure	Risorse
Riforma 1: Riorganizzare la rete degli IRCCS	-
I. Aggiornamento tecnologico e digitale	7,36
Investimento 1.1: Ammodernamento del parco tecnologico e digitale ospedaliero	4,05
Investimento 1.2: Verso un ospedale sicuro e sostenibile	1,64
Investimento 1.3: Rafforzamento dell'infrastruttura tecnologica e degli strumenti per la raccolta, l'elaborazione, l'analisi dei dati e la simulazione	1,67
II. Formazione, ricerca scientifica e trasferimento tecnologico	1,26
Investimento 2.1: Valorizzazione e potenziamento della ricerca biomedica del SSN	0,52
Investimento 2.2: Sviluppo delle competenze tecnico-professionali, digitali e manageriali del personale del sistema sanitario	0,74
Totale	**8,63**

tecnologico e digitale" siano state destinate risorse per €7,36 miliardi. L'investimento 1.1 è il più consistente della missione ed è riservato all'"Ammodernamento del parco tecnologico e digitale ospedaliero". L'importo complessivo (€4,05 miliardi) comprende anche la quota, pari a €1,41 miliardi, relativa a progetti già avviati dal Ministero della Salute relativi al rafforzamento del SSN predisposti per fronteggiare l'emergenza Covid-19. Ad oggi, le infrastrutture tecnologiche e digitali ospedaliere presentano un significativo grado di obsolescenza e risultano carenti in molti ambiti. Ciò rischia di compromettere sia la qualità delle prestazioni che l'efficienza del sistema, generando un effetto negativo sulla fiducia dei cittadini nel sistema sanitario. L'investimento prevede l'ammodernamento digitale del parco tecnologico ospedaliero, tramite l'acquisto di 3.133 nuove grandi apparecchiature ad alto contenuto tecnologico, per una spesa totale di 1,19 miliardi. Inoltre, sono presenti interventi finalizzati al potenziamento del livello di digitalizzazione dei Dipartimenti di emergenza e accettazione (DEA) di I e II livello, al costo di 1,45 miliardi di euro. Infine, una spesa di 1,41 miliardi di euro è destinata alla creazione di posti letto di terapia intensiva e semi-intensiva. In merito allo stato di avanzamento sono stati raggiunti tutti i 4 milestone da conseguire fra il 2021 e il 2022; restano da raggiungere altri 4 milestone, il primo dei quali entro fine 2024.

L'investimento 1.3 mira a rafforzare l'infrastruttura tecnologica e migliorare la capacità di raccolta ed elaborazione dei dati, ad esso sono destinati €1,67 miliardi. L'obiettivo è il potenziamento del Fascicolo Sanitario Elettronico al fine di garantirne la diffusione, l'omogeneità e l'accessibilità su tutto il territorio nazionale. Il progetto prevede innanzitutto l'integrazione completa dei dati sanitari attraverso la creazione di un archivio centrale e la promozione dell'interoperabilità. In aggiunta, l'investimento sostiene finanziariamente e fornisce supporto tecnico alle Regioni e ai fornitori di servizi sanitari per l'adozione del FSE, compreso l'aggiornamento delle infrastrutture tecnologiche e la compatibilità dei dati. Il progetto include iniziative già avviate per la realizzazione del Sistema di Tessera sanitaria elettronica. Quest'iniziativa assorbe gran parte delle risorse, ovvero 1,38 miliardi di euro.

Fig. 7.2: La percentuale di completamento del progetto FSE nelle regioni italiane

Fonte: Fascicolo sanitario elettronico



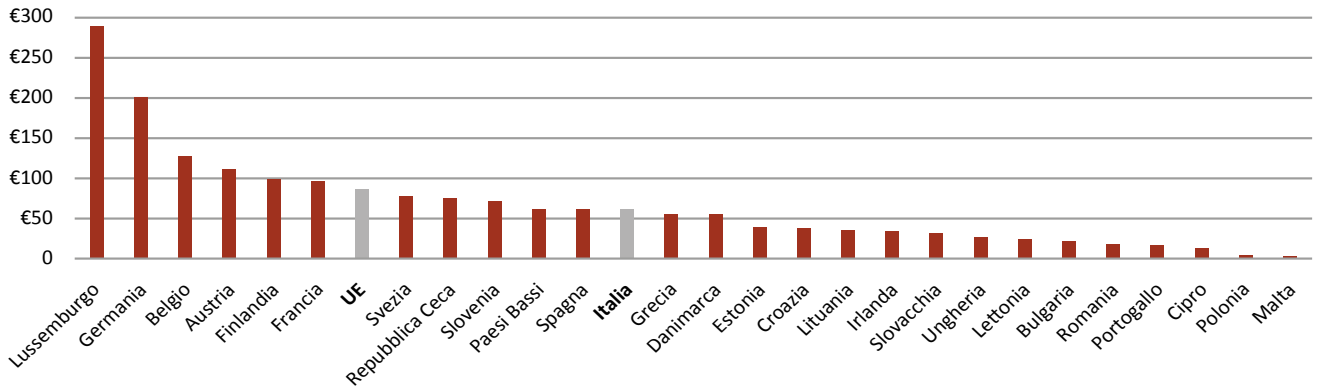
Ad oggi, **le percentuali di attuazione sono vicine al 100% nella quasi totalità delle regioni**: infatti, ben diciassette regioni presentano valori superiori al 95% (Fig. 7.2). Solamente la Liguria registra un ritardo significativo rispetto alle altre regioni italiane, attestandosi a un grado di completamento dell'86%.

Un secondo progetto, cui sono destinati i restanti 290 milioni di euro, è relativo al rafforzamento del Nuovo Sistema Informativo Sanitario (NSIS), ossia l'infrastruttura tecnologica del Ministero della salute per il monitoraggio dei LEA e la programmazione di servizi di assistenza. Una più attenta e completa analisi dei bisogni sanitari può infatti trasformarsi in un utile strumento per la quantificazione e qualificazione dell'offerta sanitaria. Stando agli ultimi dati del Ministero della salute, aggiornati a giugno scorso, non è stato ancora raggiunto l'unico target da conseguire nel 2023.

La seconda parte della M6C2 è dedicata alla **formazione** e alla **ricerca scientifica** con una dotazione complessiva di 1,26 miliardi articolati in 2 investimenti. Relativamente al primo, vi è l'intento di potenziare la ricerca biomedica in Italia, con particolare focus alle malattie rare o altamente invalidanti, e favorire il trasferimento tecnologico fra ricerca e imprese, riducendo il divario fra i risultati del settore della ricerca scientifica e quello dell'applicazione per scopi industriali. I dati Eurostat (Fig. 7.3), mostrano come l'Italia sia al di sotto della media UE relativamente alla spesa pubblica pro-capite in R&S (€61 contro €86). Dall'osservazione delle analisi dell'Istituto di statistica europeo, a saltare all'occhio è però, in particolare, l'enorme differenza con altri paesi particolarmente attivi nell'ambito della produzione farmaceutica e biomedicale e quindi i competitor più diretti del nostro Paese. La spesa pro-capite dell'Italia è soltanto un terzo di quella tedesca (€251,6), meno della metà rispetto al Belgio (€127,6) e circa il 50% inferiore alla francese (€96,1). In generale tutte le economie dell'Europa centro-occidentale, con le sole eccezioni rappresentate da Danimarca, Portogallo e Irlanda, spendono di più pro-capite in ricerca di quanto fa lo Stato italiano.

Fig. 7.3: Spesa pubblica in ricerca e sviluppo pro-capite, per Stato membro UE (2021)

Fonte: Eurostat



L'investimento 2.2 invece mira direttamente allo sviluppo delle competenze tecniche sia degli operatori già attivi nel comparto che dei nuovi entranti. Per poter stare al passo con il progresso scientifico e la continua innovazione tecnologica, **gli operatori sanitari necessitano di essere regolarmente aggiornati ed avere un livello elevato di competenze digitali**. L'investimento opererà tramite borse di studio congiuntamente all'avvio di percorsi di formazione professionale. La difficoltà di reperimento dei lavoratori del settore sanitario da parte delle imprese emerge chiaramente dagli ultimi dati sulle entrate programmate nel mercato del lavoro diffusi da Unioncamere-ANPAL. Nel mese di settembre 2023, i tre indirizzi di studio più attinenti al comparo, ovvero sanitario e paramedico, chimico-farmaceutico e medico-odontoiatrico, sono tra quelli a più elevata difficoltà di reperimento (Tab. 7.6). Tuttavia, **l'ostacolo maggiore sembra essere non tanto la preparazione inadeguata, con percentuali prossime allo zero ad eccezione dell'indirizzo chimico-farmaceutico, quanto invece la penuria di candidati**.

Relativamente allo stato di avanzamento, l'investimento 2.1 comprende solamente un target per il 2023 non ancora raggiunto, ma con scadenza a dicembre. Per l'investimento 2.2 invece è stato conseguito in anticipo il target di dicembre 2023 mentre non è stato conseguito quello di giugno.

Tab. 7.6: Lavoratori richiesti dal mercato, per titolo di studio (ingressi programmate nel mese di settembre 2023)

Fonte: Unioncamere-ANPAL, Sistema Informativo Excelsior

Indirizzo	Entrate previste (v.a.)	Di difficile reperimento (%):		
		Totale	Per mancanza di candidati	Per preparazione inadeguata dei candidati
Sanitario e paramedico	8.060	63,4	55,6	1,8
Chimico-farmaceutico	3.540	75,8	52,3	22,5
Medico e odontoiatrico	1.960	46,8	43,3	0,6

icom
istituto per la competitività

CAPITOLO 8

LA NUOVA STRATEGIA ITALIANA PER LA BANDA ULTRA-LARGA. LO STATO DI IMPLEMENTAZIONE DEL PIANO ITALIA 1 GIGA E ITALIA 5G

8.1. DAL PIANO BUL DEL 2015 ALLA NUOVA STRATEGIA

Alla luce degli obiettivi di connettività fissati a livello UE (v. cap. 5), nel marzo 2015 è stata lanciata la **Strategia per la Banda Ultralarga**, con la quale i decisori politici avevano assunto l'impegno, coerentemente con gli obiettivi dell'Agenda digitale UE 2020, di coprire almeno l'85% della popolazione con connettività ≥100 Mbit/s e il 100% con copertura ad almeno 30 Megabit/s. Tale strategia, in particolare, puntava alla copertura delle aree bianche, ossia le aree a fallimento di mercato e prevedeva misure a sostegno della domanda (voucher). L'attuazione del Piano Banda Ultralarga (Piano BUL) è stata affidata ad 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 Mbit/s. I comuni oggetto di intervento sono stati dunque suddivisi in tre diverse gare, aggiudicate tutte ad Open Fiber, parcellizzati in lotti regionali (o relativi alle Provincie Autonome):

- la prima gara prevedeva 5 lotti in 3.031 Comuni di Abruzzo, Molise, Emilia-Romagna, Lombardia, Toscana e Veneto;
- il secondo bando prevedeva 6 lotti comprendenti 3.712 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.

Per quanto concerne, invece, il **Piano Voucher,** esso è stato attivato nel 2020 e prevedeva due distinte linee d'azione: la prima, rivolta alle famiglie con ISEE inferiore a euro 20.000 e consistente in uno sconto del valore massimo di euro 500 sul canone di abbonamento a servizi di connettività internet a banda ultralarga in caso di nuove attivazioni di utenze di rete fissa e nella fornitura di un personal computer o tablet (in quest'ultimo caso il contributo per l'acquisto di personal computer o tablet era subordinato alla contestuale attivazione del servizio di connettività), si è conclusa nel 2021; la seconda, rivolta alle imprese e alle persone fisiche titolari di partita IVA che esercitano, in proprio o in forma associata, una professione intellettuale (articolo 2229 del Codice civile) o una delle professioni non organizzate (legge 14 gennaio 2013, n. 4) presenti su tutto il territorio nazionale e consistente nella possibilità di richiedere un contributo, da un minimo di 300 euro ad un massimo di 2.500 euro (secondo una suddivisione in quattro tipologie di distinti voucher), per servizi di connettività a banda ultralarga da 30 Mbit/s ad 1 Gbit/s (e superiori).

Quanto alla durata dei voucher imprese, nel febbraio scorso è stata effettuata una redistribuzione delle risorse tra le regioni ed è stata disposta una proroga al 31 dicembre 2023, salvo esaurimento delle risorse stanziate, a seguito della decisione della Commissione europea del 6/12/2022. Da ultimo, con decreto del 10 luglio 2023 è stata disposta una ripartizione diversificata delle risorse nella logica di favorire l'accesso a servizi di connettività più performanti ed in particolare quelli con velocità massima in download superiore ad 1 Gbit/s cui sono state destinate il 72,5% delle risorse. Relativamente ai voucher destinati alle famiglie, tra il 27 aprile al 31 maggio 2023 Infratel ha svolto una consultazione ad integrazione di quella già effettuata, utile alla definizione delle modalità di lancio della seconda fase di incentivi. A differenza della prima tornata di voucher, nella seconda non sono previste limitazioni di ISEE ed è prevista la destinazione alle sole famiglie senza un contratto di rete fissa in banda ultralarga.

Al fine di dare attuazione a quanto previsto rispettivamente con la Comunicazione sulla Connettività per un mercato unico digitale europeo (cd. 'Gigabit Society') e la Comunicazione sul decennio digitale (cd. "Digital compass") con cui sono stati presentati

la visione, gli obiettivi e le modalità per conseguire la trasformazione digitale dell'Europa entro il 2030, il 27 maggio 2021 è stata lanciata la **Strategia italiana per la Banda Ultralarga "Verso la Gigabit Society"** con l'obiettivo di portare la connettività a 1 Gbps su tutto il territorio nazionale entro il 2026, con un anticipo di 4 anni rispetto agli obiettivi europei fissati per il 2030. La nuova strategia, in particolare, in attuazione del Piano Nazionale di Ripresa e Resilienza che destina il 27% delle risorse alla transizione digitale, di cui 6,7 miliardi di euro per progetti relativi alla connettività, ha individuato altre 5 azioni da aggiungere alle due già in atto e da completare (il Piano aree bianche appena descritto e il Piano voucher) e, nello specifico, il Piano "Italia a 1 Giga", il Piano "Italia 5G", il Piano "Scuole connesse", il Piano "Sanità connessa" e il Piano "Isole Minori".

Il Piano "**Italia a 1 Giga**" mira ad intervenire fornendo una connessione ad almeno 1 Gbps in download e 200 Mbit/s in upload alle unità immobiliari presenti nelle aree grigie e nere NGA che, a seguito della mappatura delle infrastrutture presenti effettuata nel 2021 e degli interventi già pianificati dalle aziende operanti nel mercato entro il 2026, sono risultate non coperte da almeno una rete in grado di fornire in maniera affidabile velocità di connessione in download ≥ 300 Mbit/s.

Specifica attenzione e risorse dedicate (oltre 45 mln di euro assegnati ad un operatore aggiudicatario) sono rivolte alle isole minori italiane attraverso il Piano **Isole Connesse** che punta a portare la connessione internet ultraveloce, prevedendo la progettazione, la fornitura e posa in opera dei cavi sottomarini in fibra ottica e relativa manutenzione per complessive 21 tratte.

Sempre al tema connettività è dedicato il Piano **Scuole Connesse,** che prevede interventi per connettere, con velocità simmetriche di almeno 1 Gbps, quasi 10 mila sedi scolastiche di tutto il territorio italiano ed è stato assegnato, a seguito di un bando pubblico, a tre operatori aggiudicatari per un totale di circa 165 milioni di euro.

Il Piano **Sanità Connessa** mira invece a garantire la connettività con velocità simmetriche di almeno 1 Gbps e fino a 10 Gbps alle strutture del servizio sanitario pubblico, dagli ambulatori agli ospedali, per un totale di circa 12 mila strutture. Tale Piano è stato suddiviso in 8 lotti ed è stato assegnato, a seguito di un bando pubblico, a tre operatori aggiudicatari per un totale di circa 315 milioni di euro.

Con il Piano **Italia 5G**, invece, si punta ad incentivare la realizzazione delle infrastrutture di rete per lo sviluppo e la diffusione di reti mobili 5G nelle aree a fallimento di mercato su tutto il territorio nazionale. Esso, in particolare, persegue l'obiettivo di incentivare la diffusione di reti mobili 5G in grado di assicurare un significativo salto di qualità della connettività radiomobile mediante rilegamenti in fibra ottica delle stazioni radio base (SRB) e la densificazione delle infrastrutture di rete, al fine di garantire la velocità ad almeno 150 Mbit/s in downlink e 30 Mbit/s in uplink, in aree in cui non è presente, né lo sarà nei prossimi cinque anni, alcuna rete idonea a fornire connettività a 30 Mbit/s in tipiche condizioni di punta del traffico.

Partendo dalla constatazione delle criticità registrate nella fase di implementazione dei Piani sopra descritti, nel mese di agosto è stata lanciata la **Strategia italiana per la Banda Ultra Larga 2023-2026** che, sulla base dell'analisi dei gap attualmente presenti lungo la "catena del valore" della BUL, ovvero degli interventi attualmente in essere per la creazione e diffusione delle reti ad altissima capacità in Italia, declina un insieme di azioni tese a traguardare gli obiettivi fissati al 2026. Nello specifico, la strategia si articola in una serie di iniziative sussumibili in 5 macro-finalità: 1) incremento competenze della PA e potenziamento R&S del settore; 2) rafforzamento delle attività di monitoraggio, programmazione e pianificazione degli interventi; 3) realizzazione e potenziamento delle infrastrutture di rete; 4) aumento di efficienza e resilienza

delle reti; 5) supporto alla domanda e all'aumento del take up.

Le linee di intervento individuate puntano al raggiungimento di 4 obiettivi primari: a) la **copertura della rete fissa** con velocità (capacità trasmissiva nell'ora di picco e per ogni cliente attivo) pari o superiore a 1 Gigabit/s per tutti i numeri civici/unità immobiliari e copertura FWA (Fixed Wireless Access) nelle aree più remote con velocità minima di 100 Megabit/s per ogni cliente attivo nell'ora di punta; b) **la copertura per la rete mobile 5G stand alone** dell'intero territorio italiano; c) **take up di almeno il 50% della rete fissa** con velocità pari o superiore a 1 Gigabit/s entro il 2026; d) **supporto alla creazione di una rete Edge Cloud Computing** per garantire migliore qualità dei servizi applicativi e significativi risparmi (fino al 60%) per gli operatori di telecomunicazioni italiani. Questa soluzione innovativa è anche in grado di garantire maggiori ricavi agli operatori.

Si tratta di una strategia realista che parte dalla constatazione dell'esistenza di una serie di criticità legate a ritardi di nell'esecuzione dei lavori nelle Aree Bianche dove si registra inoltre una bassa adesione della popolazione, lunghi tempi di attivazione e performance dell'FWA non in linea con i target della Gigabit Society (l'FWA in queste aree assicura solo 100 Mbit/s), ritardi nel rilascio dei permessi, carenza di manodopera specializzata, mancanza di strumenti adeguati alla progettazione (ci si riferisce in particolare alla mancanza di una banca dati nazionale aggiornata e completa relativa ai civici presenti sul territorio ed alle unità immobiliari ad essi associate e relativa destinazione d'uso) ed una bassa adesione ai Piani Voucher per poi prevedere correttivi specifici non solo per lo sviluppo della connettività fissa e mobile e il sostegno alla domanda, ma anche azioni trasversali tese a favorire l'intero sistema Telco. Tali azioni trasversali, in particolare, mirano a:

A. **migliorare ed uniformare i processi locali inerenti alla gestione della permessistica** attraverso una serie di possibili interventi che riguardano la strutturazione di meccanismi di comunicazione preventiva che permetta ai Comuni di conoscere con congruo anticipo quando sarà presentata la richiesta di autorizzazione da parte degli operatori, la creazione di percorsi formativi per gli Enti interessati sui procedimenti autorizzatori per la realizzazione di reti di comunicazione elettronica, lo sviluppo di sistemi di supporto ai piccoli Comuni nella gestione dei procedimenti e per favorire la collaborazione tra i Comuni e gli operatori nella localizzazione degli impianti e la promozione dell'adozione di iniziative di regia regionale delle Conferenze di Servizi per la BUL, a partire da un'analisi delle best practice regionali, l'implementazione di modulistica standardizzata a livello nazionale e l'organizzazione di un tavolo specifico con gli enti per risolvere le problematiche applicative della norma sull'utilizzo delle mini-trincee;
B. **favorire il re-skilling del personale e il reperimento competenze in ambito europeo;**
C. **implementare una piattaforma numeri civici e unità immobiliari** per risolvere le criticità legate all'inadeguata qualità del data base dei numeri civici utilizzati per la programmazione degli interventi;
D. **rilanciare il Sistema Informativo Nazionale Federato delle Infrastrutture (SINFI) per gestione permessistica** con l'obiettivo di favorire la condivisione delle infrastrutture attraverso una gestione ordinata del sotto e sopra suolo e dei relativi interventi, nonché di offrire un unico cruscotto che gestisca e monitori tutti gli interventi in materia di BUL;
E. **sviluppare una piattaforma per favorire l'incontro domanda-offerta per la filiera Telco** al fine di agevolare Telco e PA nell'individuazione sul mercato di professionisti ed aziende specializzate con cui collaborare;

F. **costituire un fondo capitale di rischio per start-up e PMI innovative del settore Telco e supportare start-up e Venture Capital per la transizione ecologica del settore Telco;**
G. **potenziare i Centri di Trasferimento Tecnologico per il supporto all'innovazione del settore Telco;**
H. **aderire a progetti multi-Paese per lo sviluppo di iniziative transnazionali** come, ad esempio, i corridoi 5G;
I. **realizzare un backhauling in fibra ottica di proprietà pubblica lungo il sedime ferroviario, utilizzando anche l'infrastruttura fisica esistente o in corso di realizzazione**.

Per quanto riguarda, invece, gli interventi per lo sviluppo della **connettività fissa**, la nuova strategia individua una fase 3 del Piano Scuola Connessa, con estensione della gratuità del servizio di connettività e della relativa manutenzione fino al 2035 per tutte le scuole pubbliche nazionali, prevede l'offerta di servizi di connettività ad almeno 1 Gigabit/s, oltre ad assistenza tecnica e servizi di manutenzione per 5 anni a 3.000 Comuni per favorire la transizione digitale delle sedi comunali più piccole, annuncia una consultazione pubblica tesa a valutare l'estensione del piano Isole Minori ad ulteriori 10 isole circa, propone l'adeguamento della connettività delle strutture sanitarie pubbliche territoriali, anche aderenti al piano "Sanità connessa", prevedendo prestazioni minime di 10 Gigabit/s gratuite, sostiene l'adeguamento connettività progetto "Polis" per l'accesso ai servizi digitali e connettività ultraveloce in ambito sicurezza e gestione delle emergenze a 10 Gigabit/s Stima costi.

In relazione alla **connettività mobile,** la strategia riprende un annoso tema, ossia quello dei limiti elettromagnetici, proponendo l'avvio di un dialogo istituzionale a vari livelli teso a verificare la congruenza delle attuali modalità di rilevazione dei dati nazionali rispetto a quelle europee, l'adozione di interventi che favoriscano un utilizzo più efficiente dello spettro radio e supportare soprattutto i territori e le amministrazioni locali, anche attraverso una comunicazione mirata, adeguata e supportata da evidenze tecnico-scientifiche, prevede il potenziamento e rilascio in operatività del Catasto Elettromagnetico Nazionale attraverso interventi tesi a favorire il popolamento dei catasti regionali. Nel cluster sviluppo di reti 5G di nuova generazione e servizi innovativi si colloca, invece, l'iniziativa di realizzare, in collaborazione con Ferrovie dello Stato, un'infrastruttura radio mobile multi operatore 5G di proprietà pubblica con priorità lungo le tratte ad alta velocità, di garantire copertura e connettività mobili (4G e/o 5G) lungo la rete stradale, incluse le tratte in galleria, per tutte le linee di comunicazione principali verso le sedi di svolgimento degli eventi olimpici relativi a "Milano – Cortina 2026" ed infine di finanziare progetti per la realizzazione da parte di Enti pubblici (grandi strutture ospedaliere, campus universitari, edifici pubblici di particolare interesse per il pubblico) e da parte di distretti industriali, aree portuali, poli di alta specializzazione e aree agricole (ad esempio, per applicazioni di agricoltura 4.0, la cosiddetta "Agritech") di servizi innovativi basati sul 5G anche mediante sistemi DAS ("Distributed Antenna System") indoor e outdoor e su accesso fisso ultra broadband e VHCN, dove alle infrastrutture si affianchi, con un importo di altri 400 milioni, lo sviluppo e la sperimentazione di servizi innovativi (con applicazioni di realtà virtuale/aumentata, intelligenza artificiale) basati appunto sull'uso di Edge Cloud Computing destinato a reti fisse e mobili che consentano la sperimentazione di tali servizi innovativi.

Per quanto riguarda, infine, le **iniziative a sostegno della domanda**, da un lato si prevede una revisione del piano Voucher Famiglie mediante la previsione di un voucher dedicato alle nuove attivazioni per collegamenti in Banda Ultra Larga; dall'altro, è annunciata l'individuazione, di concerto con la Commissione europea, di forme di incentivazione alle imprese per l'attivazione di servizi dedicati (es. cloud computing, cyber security, ecc.).

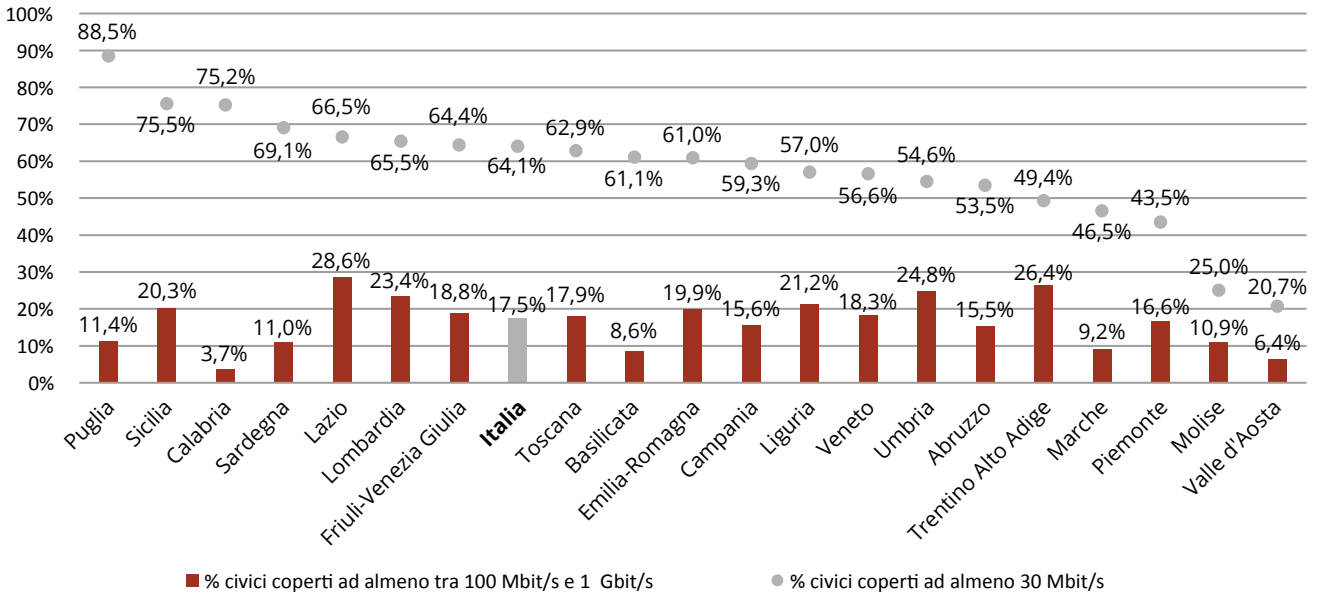
8.2. LA COPERTURA DI RETE FISSA IN ITALIA E LO STATO DI AVANZAMENTO DEL PIANI BUL E ITALIA A 1 GIGA

Gli ultimi dati ufficiali relativi allo stato della copertura del territorio italiano in rete fissa risalgono alle mappature condotte da Infratel Italia nel 2021. Lo scopo dell'iniziativa, in particolare, consisteva **nell'identificare i numeri civici che non sarebbero stati coperti dalle normali dinamiche di mercato ad almeno 300 Mbit/s entro il 2026**, andando a finanziare dunque la connettività nelle aree in cui tale velocità non sarebbe stata garantita. Il primo dato interessante emerso dal monitoraggio consisteva nel grado di copertura dei numeri civici in rete fissa con una velocità di download di almeno 30 Mbit/s al 2021. Tale dato si attestava **al 64,1% dei numeri civici presenti a livello nazionale**. Nel dettaglio, il 22,8% dei civici italiani risultava coperto con tecnologia capace di garantire connettività tra 30 Mbit/s e 100 Mbit/s ; il 23,8% era dotato di una velocità di connessione tra i 100 e i 300 Mbit/s; e, infine**, il 17,5% dei civici poteva contare su una connettività superiore a 300 Mbit/s**, quindi già in linea con gli obiettivi del Piano Italia 1 Giga.

Analizzando la scomposizione territoriale della copertura, **i risultati registrati a livello locale evidenziano notevoli differenze tra regioni**. Per quanto concerne il tasso di civici coperti ad una velocità di connessione di almeno 30 Mbit/s (Fig. 8.1), i dati mostrano come a primeggiare fossero quattro regioni meridionali, ovvero Puglia (88,5%), Sicilia (75,5%), Calabria (75,2%) e Sardegna (69,1%). **Questi risultati sono dovuti ai precedenti interventi di infrastrutturazione a banda larga, storicamente concentrati prevalentemente nel Sud Italia**. Dal lato opposto, si osserva come nelle ultime posizioni figurino in particolare Valle d'Aosta, che vedeva coperto in rete fissa solo il 20,7% del proprio territorio, e il Molise (25%).

Fig. 8.1: Civici coperti in rete fissa per velocità di connessione (%, 2021)

Fonte: elaborazioni I-Com su dati Infratel Italia

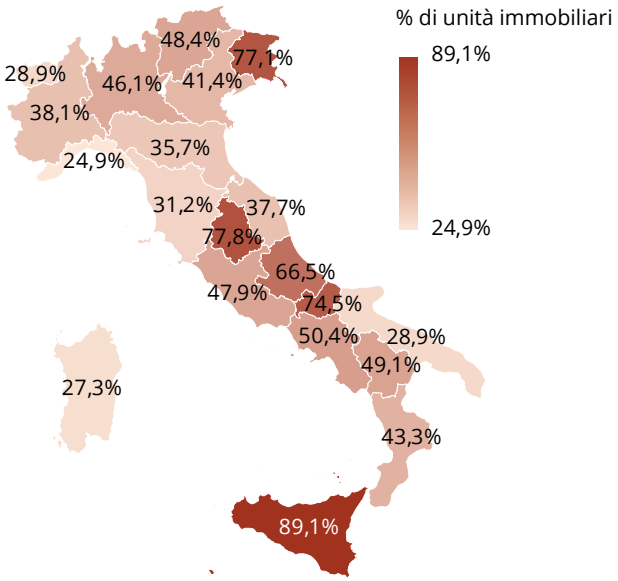


Lo scenario cambia notevolmente analizzando i soli civici coperti con tecnologie che forniscono una velocità di connessione tra i 300 Mbit/s e 1 Giga (2021). In questo caso la classifica delle regioni maggiormente coperte si ribalta, mostrando **una netta prevalenza di regioni centro-settentrionali**. A primeggiare con una copertura del 28,6% dei civici era il Lazio, seguito dal Trentino con il 26,4% e dall'Umbria con il 24,8%. Di contro, all'ultimo posto si è classificata la Calabria, che pure spiccava per copertura ad almeno 30 Mbit/s, la quale può contare su appena il 3,7% dei civici raggiunti ad una velocità di almeno 300 Mbit/s. Come anticipato nel paragrafo precedente, sono due le pianificazioni attivate negli ultimi anni per coprire il territorio il con reti fisse di ultima generazione, **il Piano Piano Banda Ultralarga (Piano BUL) e il Piano Italia a 1 giga**. Relativamente al Piano BUL, al 31 agosto 2023, dal punto di vista progettuale **risultavano 10.033 progetti approvati su 11.346 previsti in *Fiber to the home* e 6.826 approvati su 7.116 previsti in Fixed Wireless Access** (Tab. 8.1).

A livello realizzativo, per le infrastrutturazioni in fibra sono stati emessi 9.991 ordini di esecuzione, di cui 7.444 risultano chiusi, ovvero con CUIR (Comunicazione Ultimazione Impianto di Rete), a fronte di 5.576 collaudi positivi. Per i cantieri FWA si osservano 3.182 ordini emessi, di cui 3.074 con CUIR e 1.336 siti già collaudati positivamente. Analizzando la situazione territoriale, possiamo vedere come **la regione che presenta la percentuale di unità immobiliari collaudate sul totale dei quelle pianificate (Fig. 8.2), è la Sicilia (89,1%), seguita dall'Umbria (77,8%) e dal Friuli-Venezia Giulia (77,1**%). Di converso, **quelle che risultano più indietro relativamente allo stato di avanzamento sono Liguria (24,9%), Sardegna (27,3%) e Puglia (28,9%).**

Fig. 8.2: Piano BUL – % unità immobiliari collaudate sul totale di quelle pianificate (al 31 agosto 2023)

Fonte: elaborazioni I-Com su dati Infratel Italia



Se questo è lo stato di attuazione del Piano BUL, grazie al Piano "**Italia a 1 Giga**", secondo gli ultimi dati pubblicati sul portale *connetti.italia.it*[40] (aggiornati ad agosto 2023)*,* **sono stati già connessi oltre 234 mila**

Tab. 8.1: Progettazione ed esecuzione cantieri Piano BUL

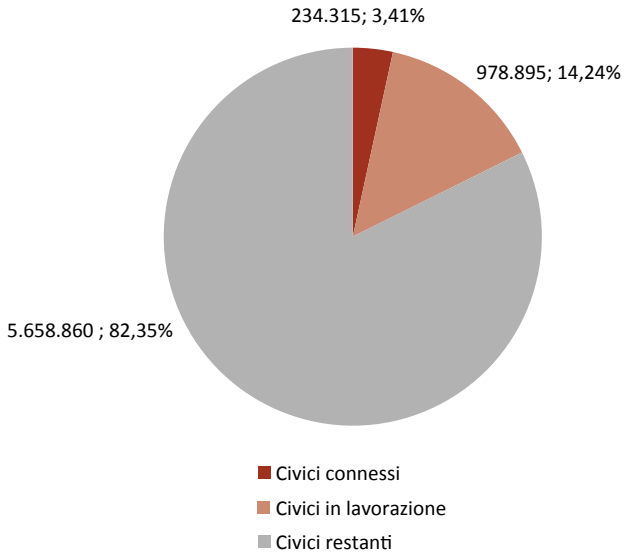
Fonte: Infratel (Relazione sullo stato di avanzamento al 30 aprile 2023) – bandaultralarga.italia.it

	Progetti previsti	Progetti approvati	Ordini emessi	Cantieri con CUIR	Collaudi positivi/ Siti collaudati positivamente
FTTH	11.346	10.033	9.991	7.444	5.576
FWA	7.116	6.826	3.182	3.074	1.336

40 Estratti il 13-10-2023

Fig. 8.3: Tasso di avanzamento del Piano Italia a 1 Giga (agosto 2023)

Fonte: Portale Connetti Italia



civici, ovvero il 3,4% di quelli previsti dall'intervento (Fig. 8.3). Inoltre, sono stati già attivati i lavori di copertura per altri 978.895 civici, che corrispondono al 14,24 del totale da raggiungere.

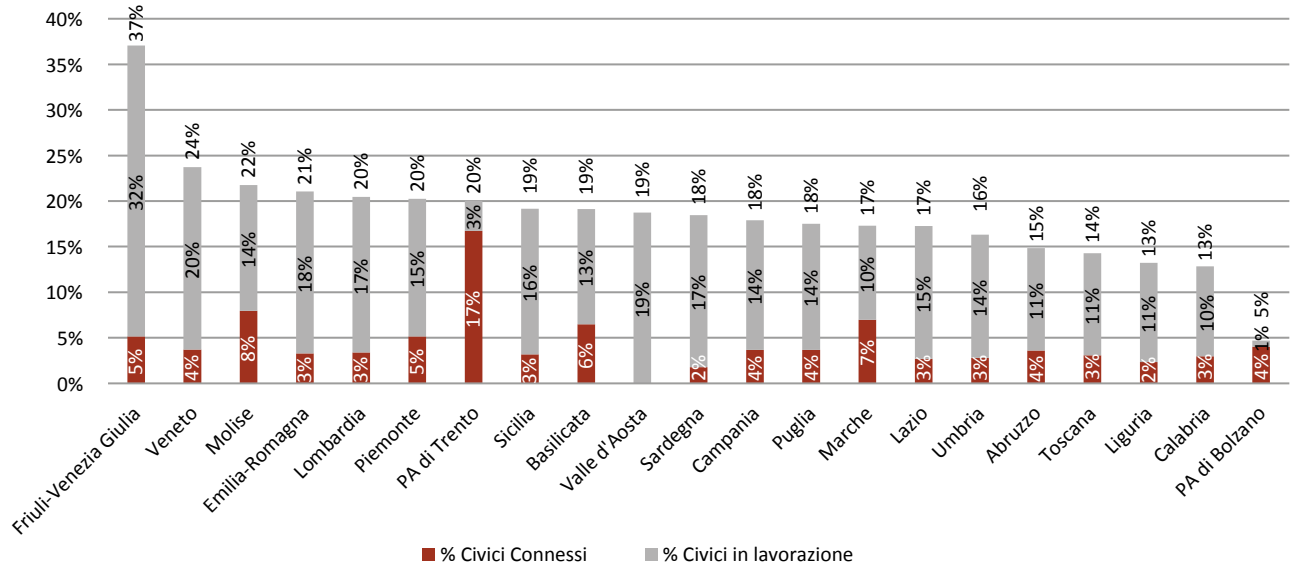
Dall'analisi dello spaccato territoriale (Fig. 8.4), emerge come **l'area geografica che fa registrare la quota più elevata di civici completati è la Provincia Autonoma di Trento (17%),** seguita dalle Marche (7%). Considerando invece sia i civici connessi che quelli già in fase di lavorazione a spiccare e il Friuli-Venezia Giulia (37%), seguito a notevole distanza dal Veneto (24%). Di converso, **le aree del Paese più indietro con gli interventi risultano la PA di Bolzano (5%), la Calabria (13%) e la Liguria (13%).**

8.2.1. Il ruolo del Fixed Wireless Access

Il **Fixed Wireless Access** (FWA) è una tecnologia che utilizza un sistema ibrido di collegamenti via cavo e senza fili per offrire servizi di connettività in banda larga e ultralarga. Il cavo, in fibra ottica, arriva fino

Fig. 8.4: Tasso di avanzamento del Piano Italia a 1 Giga (agosto 2023)

Fonte: Portale Connetti Italia



alla stazione radio base (anche detta BTS dall'inglese *Base Transceiver Station*) la quale emette un segnale radio per raggiungere il terminale ricevente (un'antenna posta al domicilio dell'utente) che a sua volta lo distribuirà all'interno dell'abitazione. A livello tecnico, le reti fixed wireless offrono un livello di qualità del servizio superiore rispetto ai sistemi mobile wireless dal momento che non deve essere gestita la mobilità del cliente e la capacità trasmissiva messa a disposizione dalla stazione radio base è condivisa da un numero di clienti determinato a priori e non variabile[41].

Nelle zone montane e rurali, la rete mista fibra/radio **costituisce un'alternativa più economica e flessibile rispetto a soluzioni via cavo in cui non sarebbe tecnicamente o economicamente sostenibile realizzare una rete in fibra fino alle abitazioni**. La tecnologia FWA nel corso degli anni ha avuto un ruolo chiave nel contribuire a colmare il problema del *digital divide* e rappresenta oggi una realtà in forte crescita[42]. Inoltre, la natura del FWA rende questa tecnologia complementare all'FTTH nel fornire connettività alle aree a bassa densità abitativa del Paese che rientrano nel Piano Italia 1 Giga e nella nuova Strategia BUL 2023-2026.

A livello di copertura, in base ai dati forniti ad I-Com da Infratel Italia, al **2021 i civici raggiunti in FWA *passed* sul territorio nazionale risultano essere il 5,7% a velocità compresa tra i 30 e i 100 Mbit/s e il 14,8% con velocità di connessione compresa tra i 100 e i 300 Mbit/s**. Analizzando la situazione a livello territoriale si osserva come, per quanto riguarda la copertura potenziale in FWA fino a 100 Mbit/s (Fig. 8.5), la regione maggiormente servita è il Molise (14,8%), seguito dall'Abruzzo (13,6%) e dal Trentino (9,9%). Tra le province spiccano Bolzano (27%), Lodi (24,8%), Isernia (19,3%) e Chieti (18,3%).

Riguardo alla copertura a velocità tra i 100 e i 300 Mbit/s, la regione che primeggia in termini di civici coperti in FWA è il Piemonte (53%), seguito dalla Valle d'Aosta (39,6%) e dalla Liguria (38,7%). La netta preponderanza del Piemonte nella copertura di FWA tra 100 e 300 Mbit/s traspare anche dai dati provinciali. Infatti, nelle prime sei posizioni tra le province più coperte, figurano tutte località di questa regione, ovvero Asti (70%), Cusio-Ossola (69%), Biella (63,8%), Cuneo (63,7%), Alessandria (60,4%) e Novara (48,9%). La stessa città metropolitana di Torino presenta un valore di copertura (pari al 41,2% dei civici) notevolmente più alto di quello fatto registrare da altre grandi città quali Bologna (11,1%), Milano (9,2%), Roma (7,1%) e Napoli (4,9%).

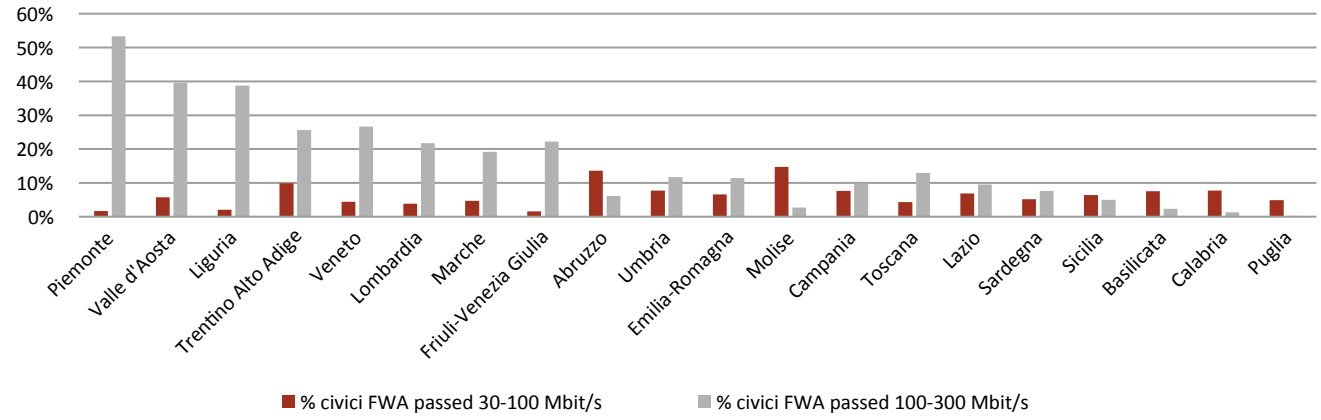
La tecnologia FWA appare in crescita anche dal punto di vista prestazionale. Negli ultimi anni sono diversi gli operatori che, oltre ad offrire connettività fixed-wireless a 300 Mbit/s, stanno lavorando per raggiungere prestazioni fino ad 1 Gbps grazie alle onde millimetriche e all'utilizzo del 5G in ambito fisso. A tal proposito è opportuno osservare come il costo unitario per la connessione di ogni singola abitazione in fibra FTTH cresca al diminuire della densità abitativa, rendendo quindi particolarmente dispendioso e complicato coprire le aree più remote del Paese con tale tecnologia. Per converso, il vantaggio del *Fixed Wireless* risiede proprio nella capacità di connettere ogni abitazione ad un costo che rimane pressoché invariato anche di fronte alla diminuzione – anche drastica – della densità abitativa. Per tali ragioni, la connettività *fixed wireless* appare come un possibile complemento alla copertura in fibra prevista dal Piano Italia 1 Giga e ribadita dalla Strategia BUL 2023-2026, in particolare nelle aree rurali del Paese. Infatti, un aumento prestazionale delle connessioni FWA fino

41 Delibera 348/19/CONS, par. 41.

42 Tale ruolo è stato formalmente riconosciuto nel nuovo Codice Europeo delle Comunicazioni Elettroniche e nelle linee guida del BEREC che classificano Very High Capacity Network (VHCN) anche le reti wireless con architettura FTTA (Fiber to the Antenna), tra le quali rientra a pieno titolo l'FWA (BEREC GUIDELINES on Very High Capacity Networks – BoR (20) 165).

Fig. 8.5: Civici coperti in FWA per velocità di connessione (%, 2021)

Fonte: elaborazioni I-Com su dati Infratel Italia



ad un 1 Gbps consentirebbe di coadiuvare la copertura in fibra di tutti i numeri civici in ambito nazionale, riducendo i costi di roll-out delle reti e soprattutto aumentando la velocità di realizzazione della copertura ad 1 Gbps del Paese, in linea con gli obiettivi previsti dal *Digital Compass*.

Oltre ai dati di copertura, per analizzare la diffusione della tecnologia FWA in Italia appare interessante osservare i dati relativi agli accessi, ovvero gli abbonamenti sottoscritti dagli utenti. A dicembre 2022, **la distribuzione territoriale degli accessi mostrava come, in valori assoluti, fosse la Lombardia a primeggiare (circa 300 mila),** seguita dal Piemonte (213 mila) e dal Veneto (160 mila). Rispetto alla percentuale di linee

Fig. 8.6: Accessi broadband in FWA per regione (in migliaia, dicembre 2022)

Fonte: elaborazione su dati Agcom

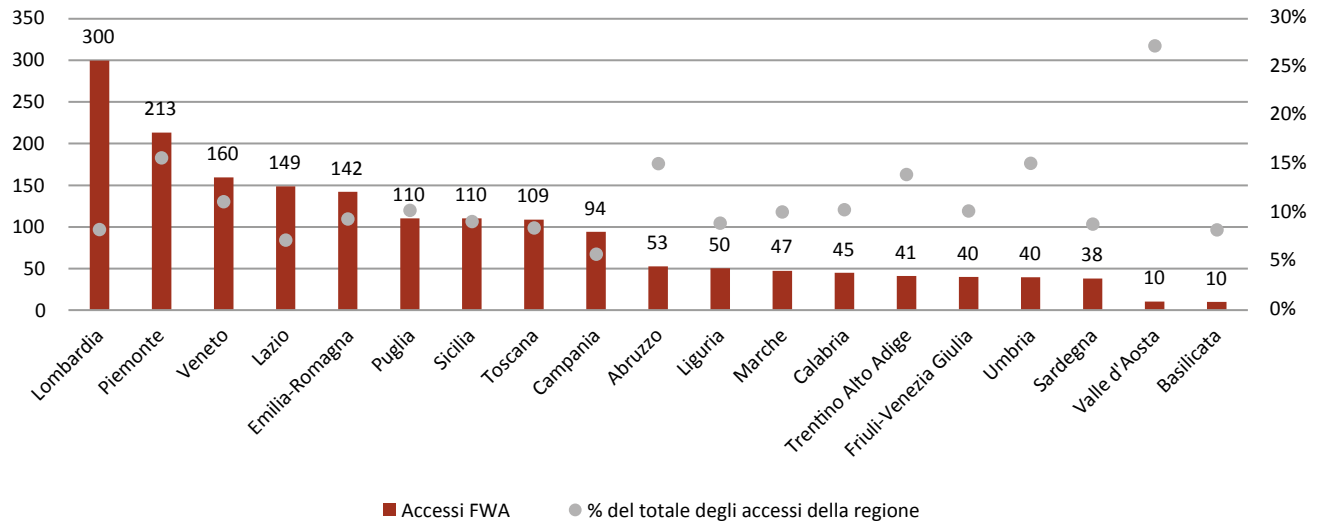
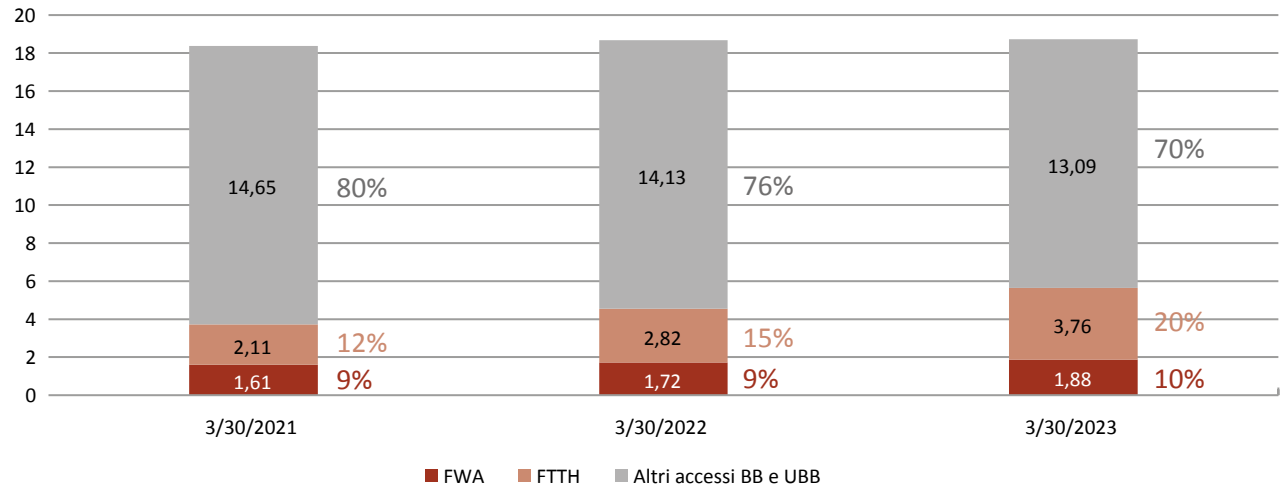


Fig. 8.7: Accessi broadband per anno (in milioni, %)

Fonte: elaborazione su dati Agcom



FWA **sul totale delle linee sottoscritte in ogni regione spicca in maniera evidente la Valle d'Aosta (27%)** che, per conformazione morfologica, appare uno dei territori in cui la copertura in questa tecnologia è maggiormente indicata. Al secondo posto per quota di connessioni in FWA sul totale delle broadband si posiziona il Piemonte (16%), seguito dal duo Umbria e Abruzzo (entrambe al 15%). Le regioni del Paese che, secondo i dati analizzati, risultano affidarsi meno a questa tecnologia, si confermano, come nel 2021, Campania (6%) e Lazio (7%).

Secondo i dati pubblicati nell'ultima versione dell'Osservatorio Trimestrale Agcom (giugno 2023), il numero di abbonamenti complessivi in tecnologia FWA a marzo 2023 ammonta a circa 1,88 milioni di unità, che equivalgono al **10% delle linee broadband totali** (Fig. 8.7). Analizzando l'andamento rispetto allo stesso periodo dei due anni precedenti, appare evidente come questa soluzione di connettività sia valutata positivamente dagli utenti essendo **cresciuta sia in termini assoluti che rispetto alla quota di mercato**.

8.3. LA COPERTURA MOBILE E LO STATO DI ATTUAZIONE DEL PIANO ITALIA 5G

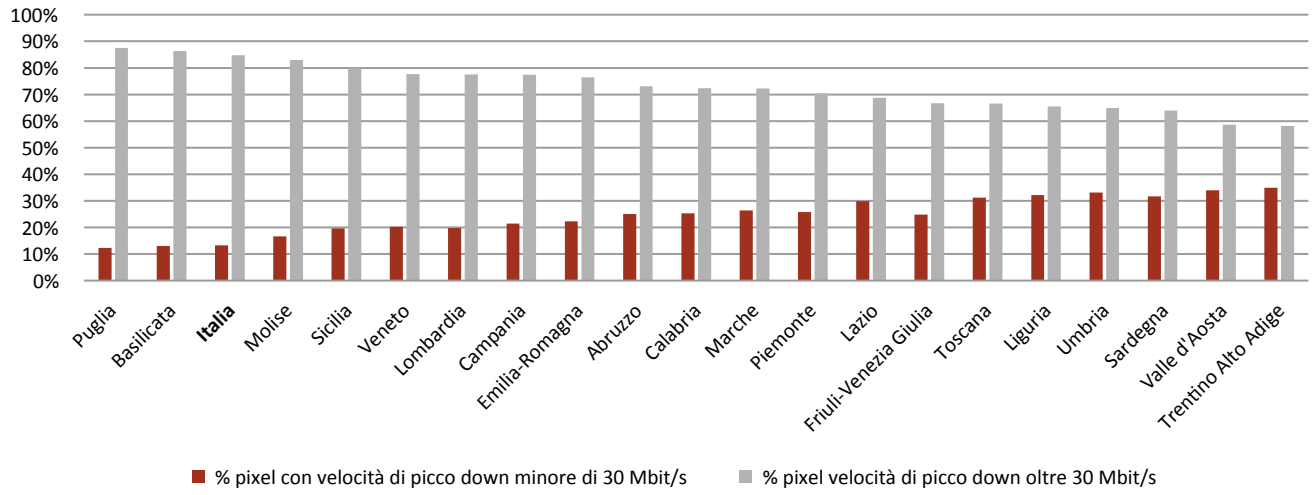
Parimenti a quanto visto per le reti fisse, tra il 10 giugno e il 31 agosto 2021, Infratel ha effettuato una mappatura[43] delle reti mobili che coprono il territorio nazionale. Per effettuare la mappatura, il territorio italiano è stato suddiviso in un reticolato di pixel che corrispondono ad un'area di dimensione di 100mt x 100mt ciascuno.

Va segnalato che, a seguito della mappatura**, è risultato completamente scoperto da rete mobile il 2,4% del territorio nazionale**. A livello regionale si osservava una netta prevalenza di "pixel" scoperti nelle regioni alpine, ovvero Friuli (8,5%), Valle d'Aosta (7,4%) e Trentino (7,1%). Al contrario, le regioni che avevano la percentuale minore di pixel scoperti sono quelle meridionali e in particolare Puglia (0,1%), Molise (0,5%), Sicilia (0,6%), Basilicata (0,7%) e Campania (1,2%).

43 La mappatura è stata realizzata seguendo le disposizioni delle linee guida del BEREC "Guidelines to assist NRAs on the consistent application of Geographical surveys of network deployments" approvate ad ottobre 2020.

Fig. 8.8: Pixel coperti in rete mobile per velocità di connessione (%, 2021)

Fonte: elaborazioni I-Com su dati Infratel Italia



Per quanto concerne la distinzione per velocità, si osservava come, tra le aree con la maggior quota di pixel coperti da rete mobile con velocità di picco minore di 30 Mbit/s in download, al 2021 erano ancora una volta le regioni alpine a presentare i valori più alti, ovvero Trentino (34,9%) e Valle d'Aosta (34%). Al contrario osservando i dati territoriali relativi alle regioni che avevano la maggiore quota di territorio coperto con **velocità di picco oltre i 30 Mbit/s** (Fig. 8.8), si osservava come spiccavano in maniera evidente **Puglia (87,6%) e Basilicata (86,3%).**

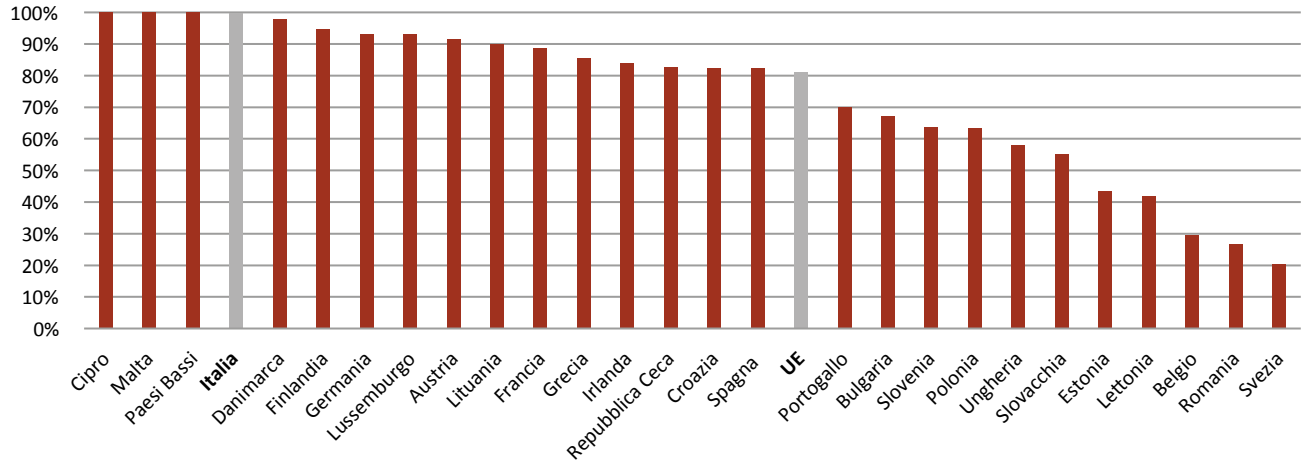
Relativamente alle reti mobili, l'argomento principale è certamente **lo stato della copertura del Paese in rete 5G**. Gli ultimi dati pubblicati dal 5G Observatory (Fig. 8.9) indicano come, nel primo trimestre del 2023, **gli operatori italiani abbiano dichiarato una copertura della popolazione pari al 99,7%**, il quarto valore più alto tra quelli pubblicati a livello europeo. Peraltro, è interessante notare come la percentuale di popolazione coperta dalla rete 5G in Italia risulti nettamente superiore sia alla media europea (81%) che rispetto alle altre principali economie UE, come Francia (84%), Germania (91%) e Spagna (80%).

Nonostante l'ottima performance registrata dal nostro Paese, ad un'analisi più attenta emerge chiaramente come **tale livello sia stato ad oggi raggiunto almeno in parte grazie all'eredità storica della buona copertura 4G e dell'utilizzo della tecnologia DSS (Dynamic Spectrum Sharing)** che abilita sulla medesima banda (in particolare le frequenze 1800 Mhz e 2600 MHz) sia l'LTE 4G che il 5G FDD, gestendo attraverso una singola antenna in maniera dinamica ed intelligente l'allocazione di banda che è necessario mettere a disposizione delle due tecnologie. In altre parole, la rete sceglie automaticamente sullo stesso spettro FDD tra connessione 4G e 5G in base al tipo di terminale e all'offerta sottoscritta dal cliente.

Osservando la composizione del mix tecnologico emerso dalla mappatura effettuata nel 2021 da Infratel è possibile vedere come la quota maggioritaria del territorio italiano, **ovvero il 72%** (Fig. 8.10), risultasse coperta proprio attraverso il DSS che per le sue caratteristiche tecniche rappresenta la migliore soluzione tecnologica disponibile per far convivere i due standard di comunicazione in questo periodo di transizione.

Fig. 8.9: Copertura della popolazione con rete 5G (%, marzo 2023)

Fonte: Commissione Europea



Se consideriamo esclusivamente **il 5G standalone** risultava coperto solo il **7,3% del territorio nazionale** (Fig. 8.11). Tra le regioni più avanti nella copertura 5G SA troviamo l'Emilia Romagna (14,9%), il Lazio (14,7%) e il Veneto (11,7%). Al contrario, quelle più indietro nel percorso di copertura del territorio il reti di quinta generazione SA sono la Basilicata (0,5%), il Trentino (1,3%) e la Valle d'Aosta (1,4%).

Relativamente allo stato di avanzamento del **Piano Italia 5G** (aggiornamento ad agosto 2023), dal punto di vista del ***backhauling*** – ovvero della rilegatura in fibra delle Stazioni Radio Base (SRB) che, secondo quanto emerso dalla mappatura, non verranno coperte dai soli operatori entro il 2026 – risultano completati oltre il 10% dei siti oggetto di intervento, mentre un ulteriore 15% è in lavorazione (Fig. 8.13).

Fig. 8.10: % di pixel coperti in DSS (2021)

Fonte: elaborazioni I-Com su dati Infratel Italia

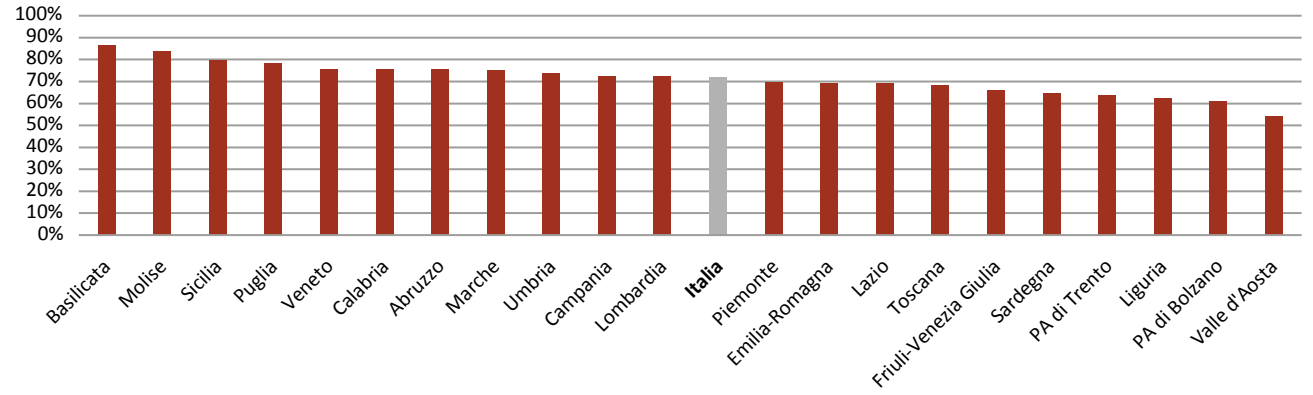
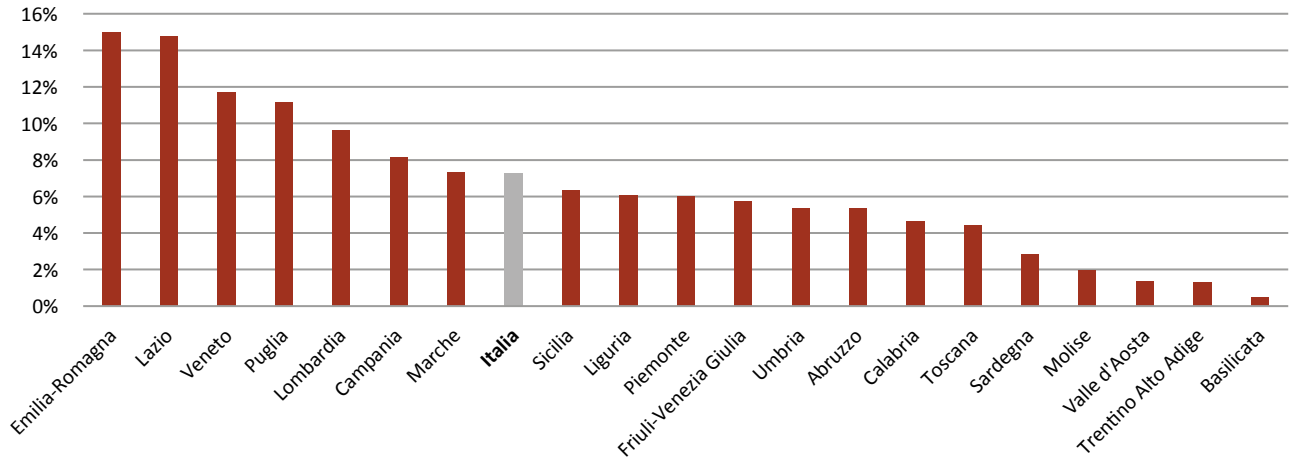


Fig. 8.11: % di pixel coperti da rete mobile 5G *Stand Alone* (2021)

Fonte: elaborazioni I-Com su dati Infratel Italia



Sul versante della **densificazione,** la situazione sembrerebbe **procedere un po' più a rilento con solo il 3,26% degli interventi completati e il 13,95% in lavorazione** (Fig. 8.12).

Fig. 8.12: Stato di avanzamento del Piano Italia 5G – *backhauling* (%, agosto 2023)

Fonte: Portale Connetti Italia

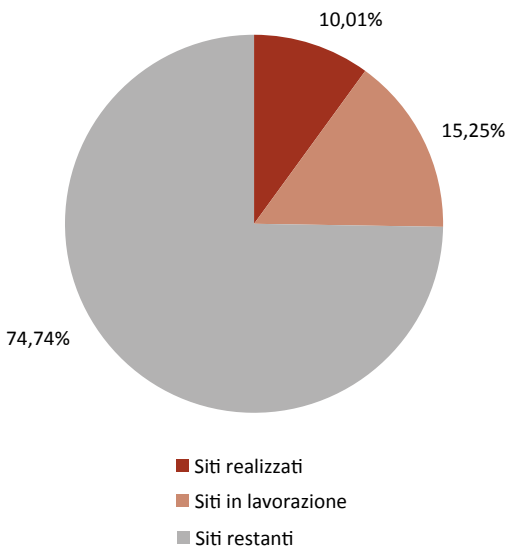
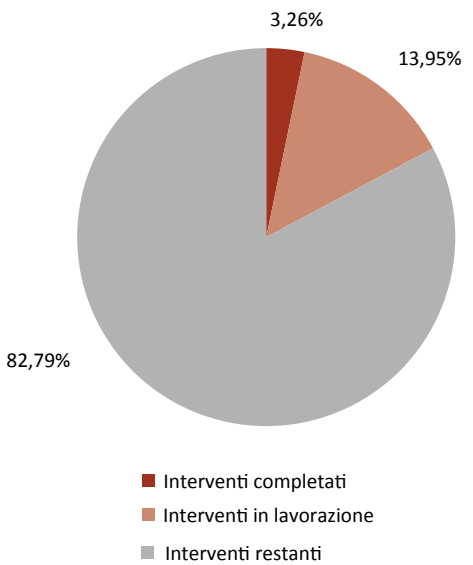


Fig.8.13: Stato di avanzamento del Piano Italia 5G – densificazione (%, agosto 2023)

Fonte: Portale Connetti Italia



8.4. GLI OSTACOLI ALLO SVILUPPO DELLE RETI. DALLE PROCEDURE AUTORIZZATIVE ALLA DISCIPLINA SUI LIMITI ELETTROMAGNETICI

Uno degli ostacoli principali allo sviluppo delle infrastrutture di TLC nel contesto nazionale è rappresentato dalle procedure autorizzative, notoriamente caratterizzate da lungaggini, eterogeneità applicativa, elusione finanche violazione delle norme. Partendo da tali constatazioni, sulla scia delle indicazioni provenienti dall'Europa ed al fine di imprimere un'accelerazione allo sviluppo delle reti di TLC necessario per centrare gli obiettivi di connettività fissati, l'ultimo quinquennio si è caratterizzato per l'adozione di una serie di importanti **interventi di semplificazione** attraverso i quali si è cercato di ridurre le tempistiche delle procedure di autorizzazione e chiarire le competenze ed il ruolo degli enti a vario titolo coinvolti nelle procedure di autorizzazione.

Ci si riferisce, in particolare, ai decreti-legge n. 76/2020 e n. 77/2021, convertiti, rispettivamente, con L. n. 120/2010 e L. n. 108/2021, al D.Lgs. n. 207/2021 con il quale è stata recepita la direttiva 2018/1972 che istituisce il Codice europeo delle comunicazioni elettroniche, alla legge annuale per il mercato e la concorrenza 2021 (Legge n. 118/2022) nonché al D.L. n. 13/2023 convertito con legge n. 41 del 21 aprile 2023. Attraverso tali interventi si è tentato di ridurre gli oneri a carico degli operatori, semplificare e tagliare le tempistiche delle procedure autorizzative, valorizzando strumenti funzionali a tale scopo come la Conferenza di servizi, fissare termini chiari ad ENAC ed ENAV per il rilascio dei relativi pareri e nullaosta, prescrivere l'impiego di procedure digitali per gli invii documentali finanche, con il D.L. n. 13/23, prevedere l'esercizio di poteri sostitutivi da parte di soggetti individuati dal Governo nel caso di mancata adozione da parte dell'amministrazione competente, di atti o provvedimenti finalizzati all'attuazione dei progetti del PNRR (nel caso di inosservanza del termine di 15 gg assegnato dal Governo). Si tratta di un corposo apparato di norme che va ad incidere su un insieme complesso ed articolato di procedure, nel tentativo, ancora in progress alla luce delle persistenti difficoltà applicative, di ridurre gli ostacoli alla realizzazione di reti moderne e performanti, tra cui quelle 5G che, insieme alla fibra, rappresenteranno per il Paese leve di competitività importanti.

A tali complessità si aggiunge, rispetto alle reti 5G, la **disciplina sul golden power** (così come integrata dal D.L. 25 marzo 2019, n. 22 – c.d. Decreto Brexit, convertito con modificazioni dalla Legge 20 maggio 2019, n. 41 e successivamente modificato dal D.L. 21/2022), che, fermi restando gli obblighi previsti dalla normativa sul perimetro di sicurezza nazionale cibernetica, prescrive la notifica alla Presidenza del Consiglio dei ministri di un piano annuale, modificabile con cadenza quadrimestrale, alle imprese che, anche attraverso contratti o accordi, intendano acquisire, a qualsiasi titolo, beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione di componenti ad alta intensità tecnologica funzionali alla realizzazione o gestione di reti 5G. Tale piano, in particolare, deve indicare il programma di acquisti, fornire dati dettagliati identificativi dei relativi, anche potenziali, fornitori, la descrizione dei beni, dei servizi e delle componenti ad alta intensità tecnologica funzionali alla progettazione, alla realizzazione ed alla manutenzione, un'informativa completa sui contratti in corso e sulle prospettive di sviluppo della rete 5G, ogni ulteriore informazione funzionale a fornire un dettagliato quadro delle modalità di sviluppo dei sistemi di digitalizzazione del notificante, nonché dell'esatto adempimento alle condizioni e alle prescrizioni imposte a seguito di precedenti notifiche, un'informativa completa relativa alle eventuali comunicazioni effettuate al CVCN, inclusiva dell'esito della valutazione, ove disponibile, e delle relative prescrizioni, qualora imposte. Tale pianificazione

deve altresì contenere i contratti o gli accordi relativi ai servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G già autorizzati. Si tratta, evidentemente, di adempimenti che, sebbene perseguano il fine di garantire la sicurezza delle reti 5G e, in ultima battuta, la tutela di interessi primari dello Stato, dall'altro impongono una capacità di progettazione ex ante che spesso si scontra con l'assenza di una pianificazione degli spazi destinati ad accogliere gli impianti di TLC da parte dei Comuni, con la variabilità delle relazioni con i fornitori e con una serie di vincoli progettuali derivanti anche dalla disciplina sui limiti elettromagnetici.

Si tratta di adempimenti che, sebbene perseguano il fine di garantire la sicurezza delle reti 5G e, in ultima battuta, la tutela di interessi primari dello Stato, dall'altro impongono una capacità di progettazione ex ante che spesso si scontra con l'assenza di una pianificazione degli spazi destinati ad accogliere gli impianti di TLC da parte dei Comuni, con la variabilità delle relazioni con i fornitori e con una serie di vincoli progettuali derivanti anche dalla **disciplina sui limiti elettromagnetici**.

Al riguardo il nostro paese ha adottato una disciplina che si caratterizza per essere una delle più restrittive al mondo. Ed infatti, in attuazione della legge 22 febbraio 2001, n. 36 *"Legge quadro sulla protezione dalle esposizioni a campi elettrici, magnetici ed elettromagnetici"* è stato adottato il DPCM dell'8 luglio 2003 (successivamente modificato dal decreto-legge n. 179 del 2012) che ha fissato il valore di attenzione e l'obiettivo di qualità a 6 V/m mentre il limite di esposizione a 60 V/m per frequenze da 0.1 MHz a 3 MHz, a 20 V/m per frequenze da 3MHz a 3 GHz e a 40 V/m per frequenze da 3 a 300 GHZ. Il valore di attenzione di 6 V/m per il campo elettrico, in particolare, è da applicare per esposizioni in luoghi in cui la permanenza di persone è superiore a 4 ore giornaliere mentre l'obiettivo di qualità di 6 V/m per il campo elettrico è da applicare all'aperto in aree e luoghi intensamente frequentati, dunque praticamente in tutti i contesti urbani.

Si tratta di una scelta che, come chiaramente sintetizzato dalla Tab. 8.2, si colloca al di fuori delle indicazioni formulate a livello europeo ed internazionale andando ad impattare direttamente sulla progettazione degli impianti e soprattutto sulla possibilità di utilizzare i siti già esistenti per l'installazione della nuova tecnologia ostacolando, di fatto, il raggiungimento degli obiettivi di connettività fissati.

È fuor di dubbio, infatti, che **la fissazione di limiti di esposizione particolarmente stringenti rende più difficoltosa l'implementazione delle reti 5G su siti già esistenti**, imponendo la proliferazione di impianti

Tab. 8.2: Quadro complessivo sui limiti e sulle relative metodologie di rilevazione

Fonte: ENEA, 2022

Frequenza	Raccomandazione europea 1999/519/CE	Legislazione italiana			ICNIRP 2020
		Limite di esposizione	Valore di attenzione	Obiettivo di qualità	
694-790 MHz	36.2 – 38.6 V/m Mediato su 6 min	20 V/m Mediato su 6 min	6 V/m Mediato su 24 h	6 V/m Mediato su 24 h	36.2 – 38.6 V/m Valori quadratici mediati su 30 min
3.6-3.8 GHz	61 V/m Mediato su 6 min	40 V/m Mediato su 6 min	6 V/m Mediato su 24 h	6 V/m Mediato su 24 h	61 V/m Valori quadratici mediati su 30 min
26.5-27.5 GHz	61 V/m Mediato su 2,2 min	40 V/m Mediato su 6 min	6 V/m Mediato su 24 h	6 V/m Mediato su 24 h	61 V/m Valori quadratici mediati su 30 min

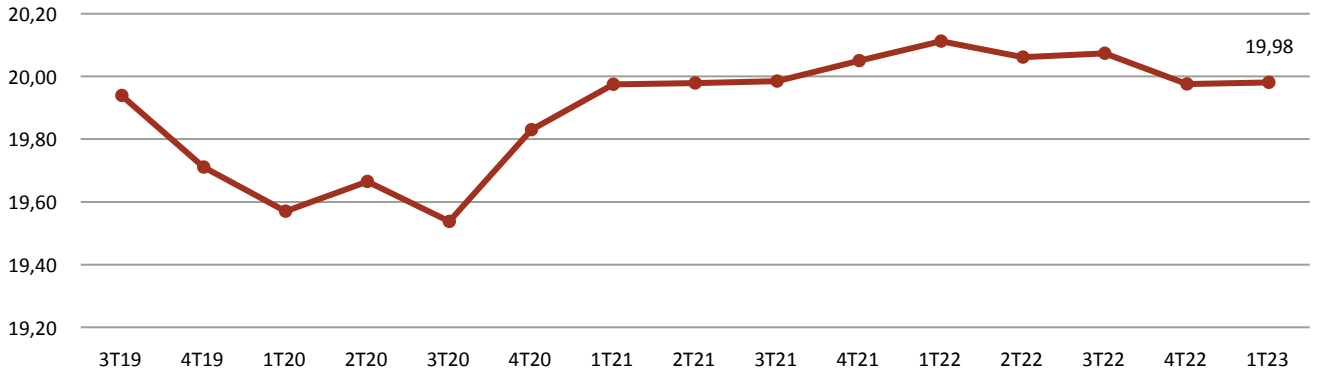
in un contesto in cui l'identificazione di nuovi luoghi dove poter costruire un sito per apparati radiomobili è un processo sempre più difficile e lento a causa del progressivo esaurimento nei centri urbani di luoghi adeguati e della scarsa disponibilità dei proprietari.
Se a ciò si aggiungono i costi realizzativi, uniti all'impatto ambientale conseguente al proliferare degli impianti e dunque all'incremento dei consumi energetici, di spazi e materiali e dei mezzi in circolazione per finalità manutentive ed il tutto si colloca in una cornice che vede l'Italia impegnata nel raggiungimento di obiettivi di copertura assolutamente sfidanti entro il 2026 e nella necessità di non ridurre la competitività delle proprie imprese sia di TLC che, più in generale, delle aziende interessate a beneficiare delle opportunità offerte dal 5G, ben si comprendono le ragioni a sostegno di una riflessione circa l'opportunità, se non addirittura la necessità, di rivedere la disciplina sui limiti elettromagnetici.
Dopo il naufragio del tentativo di innalzamento dei limiti di esposizione ai campi elettromagnetici di questa estate – con il quale si prevedeva l'innalzamento ad un valore di 24 V/m nel caso di mancato raggiungimento di un'intesa entro 120 gg dall'entrata in vigore della legge e si assegnava alla Fondazione Ugo Bordoni un ruolo centrale non solo per l'attività di monitoraggio, da svolgere di concerto con le ARPA, ma anche con riguardo alle attività informative da rivolgere alla cittadinanza – non può dunque che essere condiviso il riferimento espresso a tale tema inserito nella nuova strategia recentemente varata dal Governo.

8.5. LE MISURE A SOSTEGNO DELLA DOMANDA

Oltre che analizzare il lato dell'offerta, per comprendere lo stato delle telecomunicazioni in Italia è interessante andare ad osservare la domanda di connettività nel Paese. Dai dati contenuti nell'ultima relazione dell'Osservatorio Trimestrale sulle Telecomunicazioni realizzata da Agcom (N.2/2023), emerge come **il numero di accessi diretti alla rete**, ovvero il numero di linee attive, nell'ultimo triennio **abbia sperimentato un andamento oscillante** (Fig. 8.14). Analizzando il *breakdown* trimestrale a partire dal T3 2019, è possibile notare come gli accessi siano diminuiti fino a toccare quota 19,54 milioni nel terzo trimestre 2020, per poi tornare lievemente a crescere nel periodo pandemico fino a toccare quota 20,11 milioni nel T1 2022, per poi attestarsi a 19,98 nei primi tre mesi di quest'anno.

Fig. 8.14: Andamento accessi diretti alla rete fissa in Italia (milioni)

Fonte: Osservatorio trimestrale Agcom – N.2/2023



Se il numero degli accessi è lievemente calato, un notevole passo avanti si è fatto sul versante della tecnologia (Fig. 8.15). Analizzando infatti il mix tecnologico nello stesso periodo, appare con evidenza **il calo delle connessioni completamente in rame (-29%)**, che restano comunque il 20,7% del totale, **a fronte di una netta crescita di tutte le altre, in particolare di FTTH (passato dal 5,7% al 18,8%), FTTC (dal 38,1% al 51,1%) e FWA (dal 6,5% al 9,4%).**

Altro dato molto interessante riguarda la distinzione delle linee broadband attive per velocità della connessione. In particolare, possiamo osservare come **quasi il 70% della clientela residenziale sia servita da una linea con velocità uguale o maggiore di 100 Mbit/s**. Tale percentuale è leggermente minore per la clientela business (64%). Di converso, permangono ancora il 18% delle linee broadband residenziali e il 25% di quelle business con una connettività inferiore ai 30 Mbit/s (Fig. 8.16).

Come già descritto nel primo paragrafo, uno degli strumenti attraverso cui si punta per garantire una maggiore diffusione di servizi di connettività a banda ultralarga nel Paese consiste nel Piano voucher connettività. Lanciato dall'allora Ministero dello Sviluppo economico (oggi Ministero delle imprese e del

Fig. 8.16: Linee broadband velocità e tipologia di clientela (%, dicembre 2022)

Fonte: Osservatorio trimestrale Agcom – N.1/2023

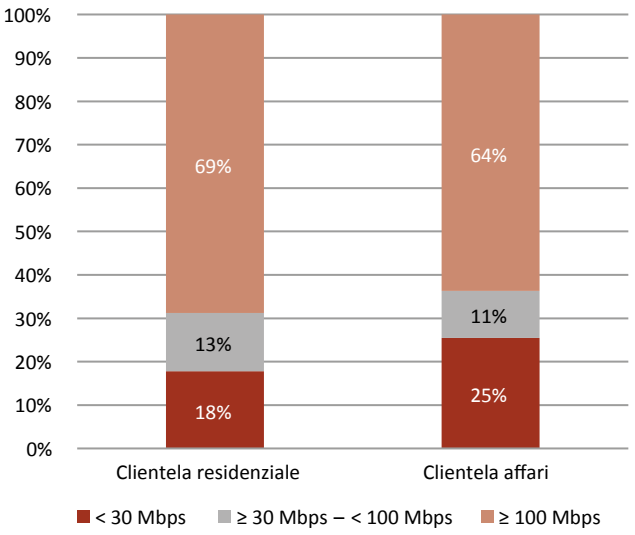


Fig. 8.15: Andamento accessi diretti alla rete per tecnologia in Italia (%)

Fonte: Osservatorio trimestrale Agcom – N.2/2023

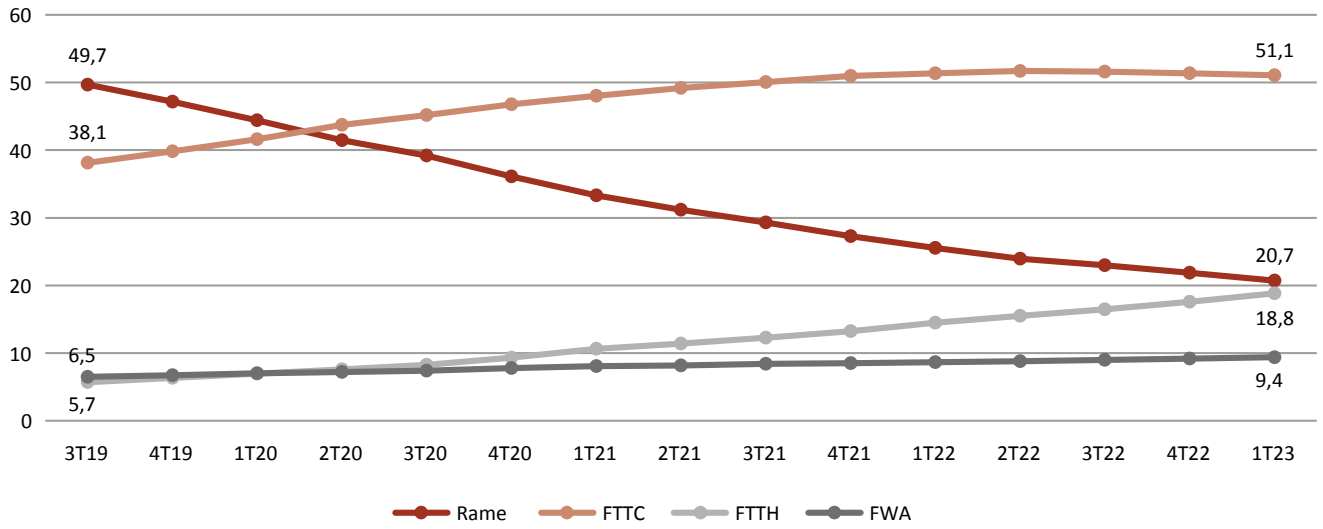
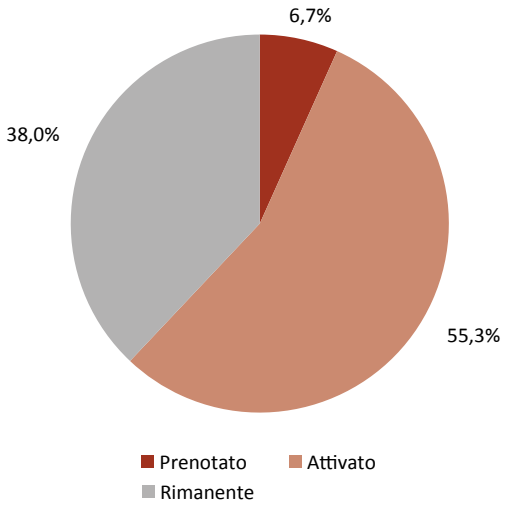


Fig. 8.17: Erogazione voucher imprese

Fonte: Ministero dello Sviluppo Economico (dati estratti il 13-10-2023)

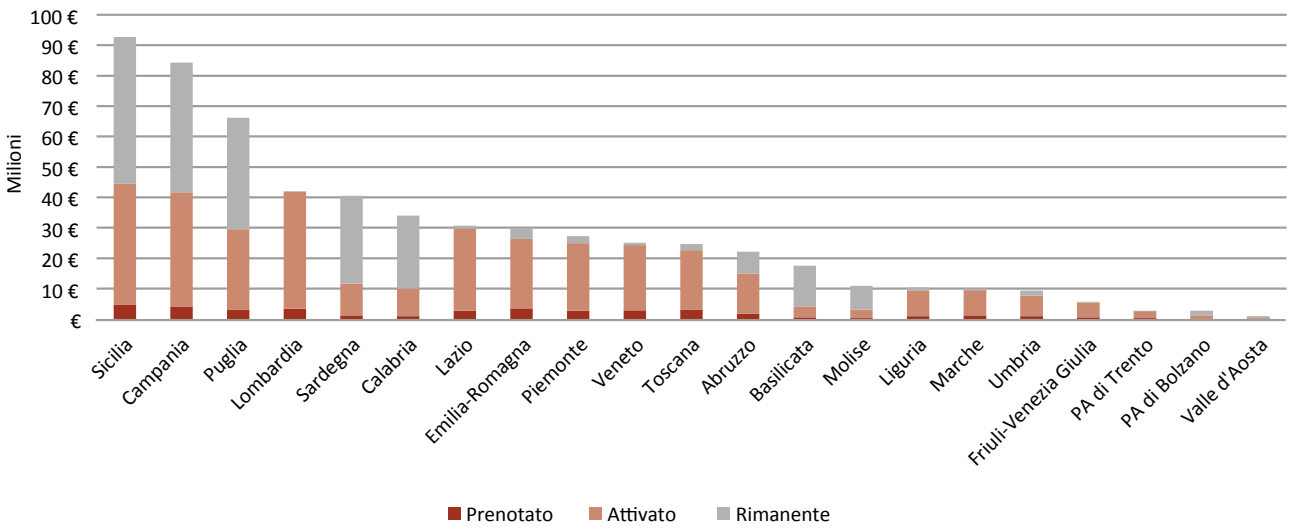


made in Italy)[44], prevede sostegni per la domanda di servizi di connettività sia delle famiglie, sia delle imprese. Nel dettaglio, alle imprese sono stati destinati circa €590 milioni, prevedendo l'erogazione di un contributo compreso tra un minimo di €300 ed un massimo di €2.500 per abbonamenti ad internet a velocità in download da 30 Mbit/s ad 1 Gbps (e superiori), di durata pari a 18 o 24 mesi.

Secondo gli ultimi dati disponibili sul portale web del MIMIT, aggiornati costantemente, a livello nazionale **il 55,3% (€326 milioni) dei fondi destinati alle imprese risulta essere stato attivato, mentre un ulteriore 6,7% (€39,5 milioni) è stato prenotato**. Allo stato attuale restano quindi ancora inutilizzati il 38% dei fondi a disposizione, che equivalgono a circa €223 milioni (Fig. 8.17). Scendendo nell'analisi del breakdown regionale (Fig. 8.18), si osserva come le regioni che, alla data del 13-10-23, **hanno utilizzato la percentuale più elevata**

Fig. 8.18: Dettaglio regionale erogazione Voucher – Imprese

Fonte: Ministero dello Sviluppo Economico (dati estratti il 13-10-2023)



44 Il Piano voucher è stato approvato nel maggio 2020 dal Comitato banda ultralarga (Cobul) e mette a disposizione oltre €1 miliardo per l'erogazione di voucher per la connettività a banda ultralarga destinati, secondo le proiezioni iniziali, a 2,2 milioni di famiglie e a 450.000 imprese attive sul territorio italiano. L'operazione dovrebbe interessare, dunque, l'8,5% delle famiglie italiane e il 9,8% delle imprese.

del budget a propria disposizione sono la Lombardia (91,9%), il Lazio (88,3%) e il Veneto (85,5%). D'altro canto, le regioni che meno hanno utilizzato lo strumento sono la Basilicata (20,9%), il Molise (25,7%) e la Sardegna (25,9%).

Per quel che riguarda i risultati ottenuti dalla **fase I del Voucher Famiglie**, attivata a novembre 2020 e conclusa nel 2021, si osserva come **sui €200 milioni disponibili a livello nazionale, circa il 51% risulta essere stato erogato, mentre il 49% non è stato utilizzato** (Fig. 8.19).

I dati regionali mostrano invece come vi siano state delle notevoli differenze nella risposta della popolazione delle varie aree del Paese. In particolare, **mentre in Lombardia sono quasi andati completamente esauriti i fondi,** essendo stato speso oltre il 99% degli stessi, **in alcune regioni meridionali, tra cui Sicilia e Campania, che erano le principali destinatarie delle risorse in valori assoluti, la percentuale di contributi attivati è inferiore al 60%** (Fig. 8.20).

Fig. 8.19: Dettaglio Fase I Voucher famiglie

Fonte: Ministero dello Sviluppo Economico

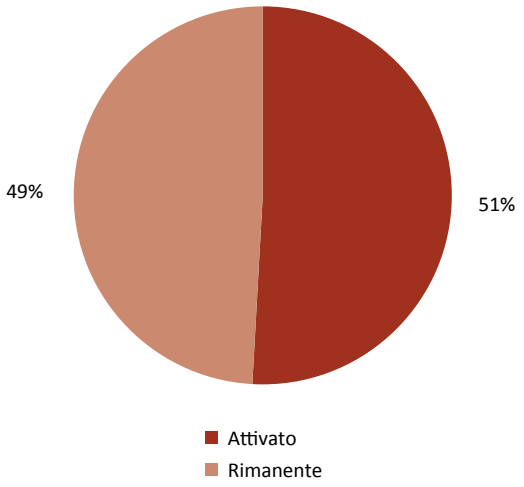
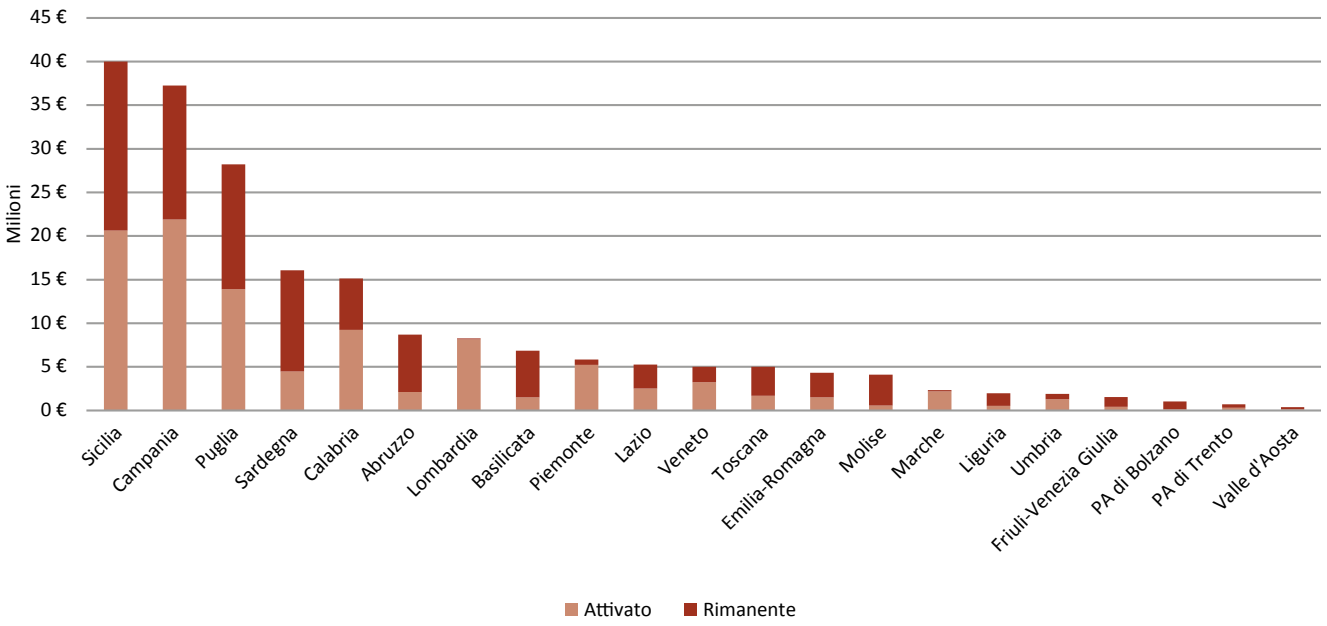


Fig. 8.20: Dettaglio regionale erogazione della Fase I Voucher Famiglie

Fonte: Ministero dello Sviluppo Economico



icom
istituto per la competitività

CAPITOLO 9

LE COMPETENZE DIGITALI NEL CONTESTO NAZIONALE

9.1. LO STATO DELL'ARTE DELLE COMPETENZE DIGITALI IN ITALIA

9.1.1. L'alfabetizzazione digitale dei cittadini

La digitalizzazione è sia una sfida che un'opportunità per l'Italia: affrontarla con successo richiede investimenti nella formazione e nell'aggiornamento delle competenze digitali della popolazione, sia dei giovani che degli adulti. Questo perché **più gli individui hanno competenze digitali avanzate e maggiore è il potenziale di innovazione tecnologica del Paese**. La loro mancanza può ostacolare significativamente la partecipazione attiva nella società e nell'economia digitale. Al contrario, una loro ampia diffusione può innescare un circolo virtuoso: un'utente più competente e consapevole tenderà ad essere più propenso a utilizzare servizi digitali avanzati, generando così una maggiore offerta degli stessi, sia nel pubblico che nel privato.

Nonostante le competenze digitali rappresentino un elemento cardine nel processo di digitalizzazione del nostro Paese, purtroppo gli ultimi dati diffusi da Eurostat mostrano un'**arretratezza generalizzata da parte dell'Italia** in questo ambito. Il nostro Paese si posiziona al **quartultimo posto in UE per quota di popolazione (46%) in possesso di competenze digitali almeno basilari (Fig. 9.1)**. Il dato italiano è distante ben 30 punti percentuali (p.p.) rispetto ai best performer Finlandia e Paesi Bassi, che si attestano al 79%, ed è di 8 p.p. più basso della media UE.

Questo divario rischia di diventare un freno importante per la digitalizzazione e in generale la modernizzazione dell'economia italiana.

Osservando invece i diversi livelli di competenze digitali della popolazione nelle principali economie europee, i cittadini italiani **risultano penultimi per competenze avanzate davanti alla Germania**, che però è lo Stato membro con la maggior quota di competenze di base o scarse. Altro record negativo dell'Italia è relativo alle competenze non misurabili, dove il nostro Paese è primo: Eurostat non ha potuto misurare le competenze perché questa fetta della popolazione non si è avvalsa di internet nei 3 mesi precedenti alla rilevazione (Fig. 9.2). In conclusione in Italia vi è una **diffusa e grave mancanza di competenze digitali** sia avanzate che di base, in particolar modo se la si confronta con le economie dell'Europa occidentale.

Fig. 9.1: Quota della popolazione con competenze digitali almeno basilari per Stato membro UE (%, 2021)

Fonte: DESI, 2023

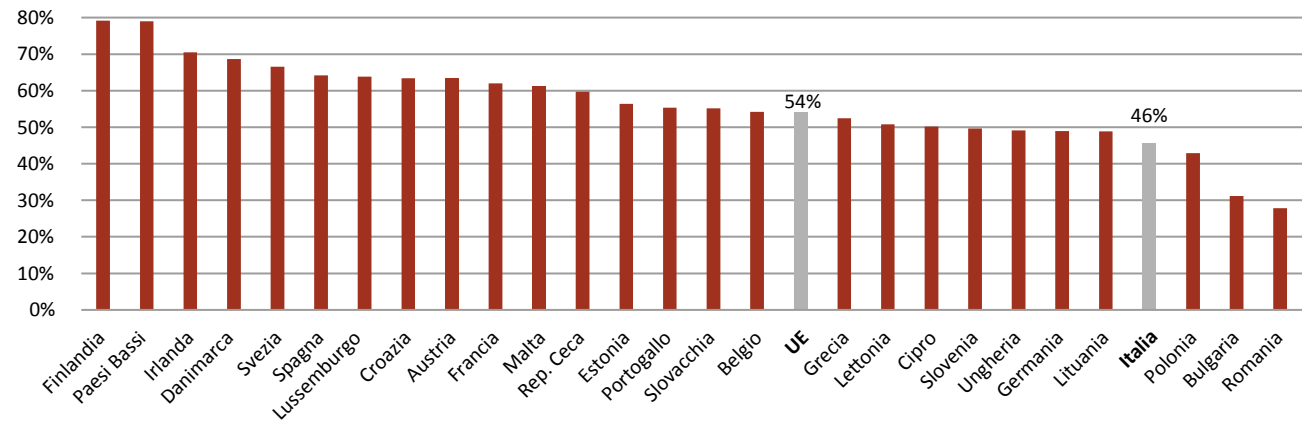
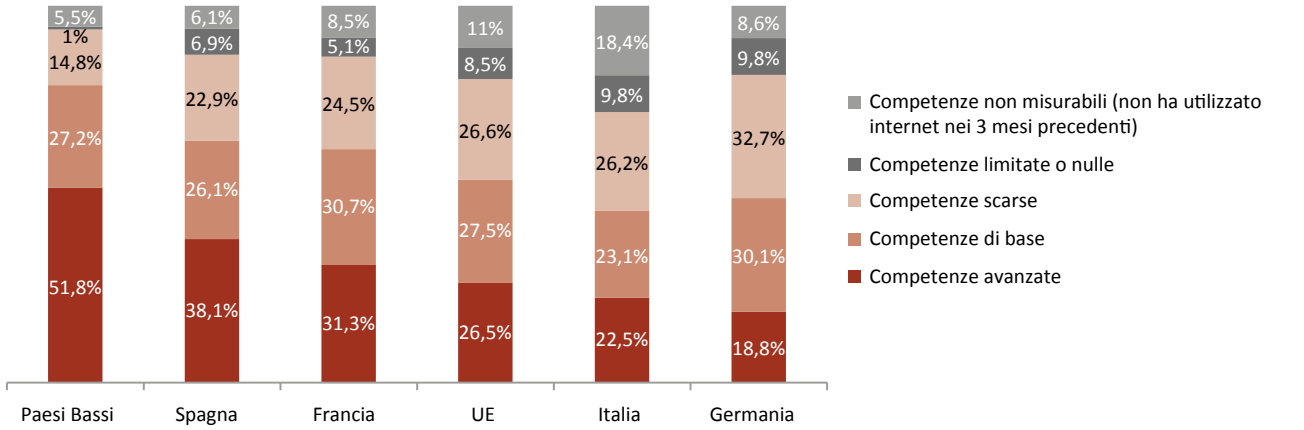


Fig. 9.2: Composizione della popolazione, per livello di competenze digitali (%, 2021)

Fonte: Eurostat

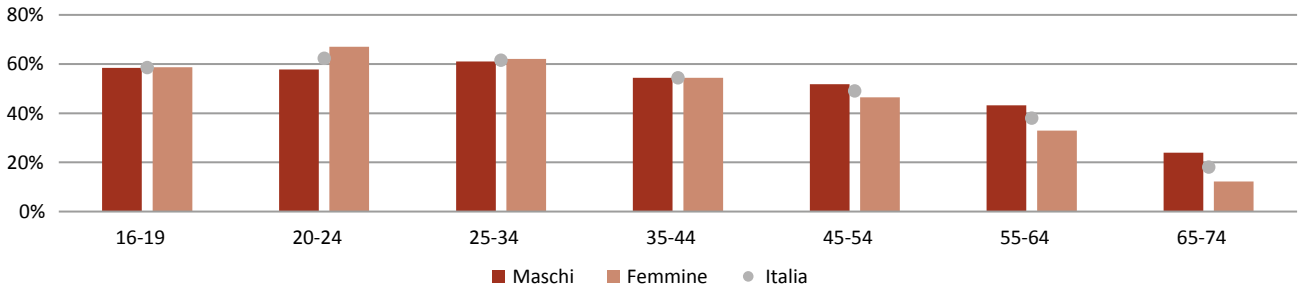


Focalizzando l'attenzione sul contesto nazionale, gli ultimi dati pubblicati dall'Istat[45] a gennaio 2023 (relativi al 2021) evidenziano un interessante cambiamento di tendenza relativamente alle distribuzioni delle competenze digitali tra genere maschile e femminile. Se infatti storicamente il genere maschile era quello più affine all'utilizzo di apparecchiature digitali**, nelle fasce di età che vanno dai 16 ai 34 anni prevale la quota di donne che hanno competenze almeno basilari in quest'ambito.** Il divario di genere torna invece a favorire gli uomini a partire dai 45 anni e si fa via via più elevato con l'aumentare dell'età (Fig. 9.3).

Al pari degli altri paesi europei le competenze digitali sono caratterizzate da forti divari associati ai fenomeni socio-culturali (in questo caso passati) della popolazione. Come ci si aspetterebbe in base all'età anagrafica, le competenze digitali sono via via maggiori nelle generazioni più giovani, ad eccezione della fascia 16-19 anni che probabilmente, data una minore maturità, in media non è ancora pienamente in possesso di competenze sedimentate.

Fig. 9.3: Individui con competenze digitali almeno di base in Italia, per genere e classe di età (2021)

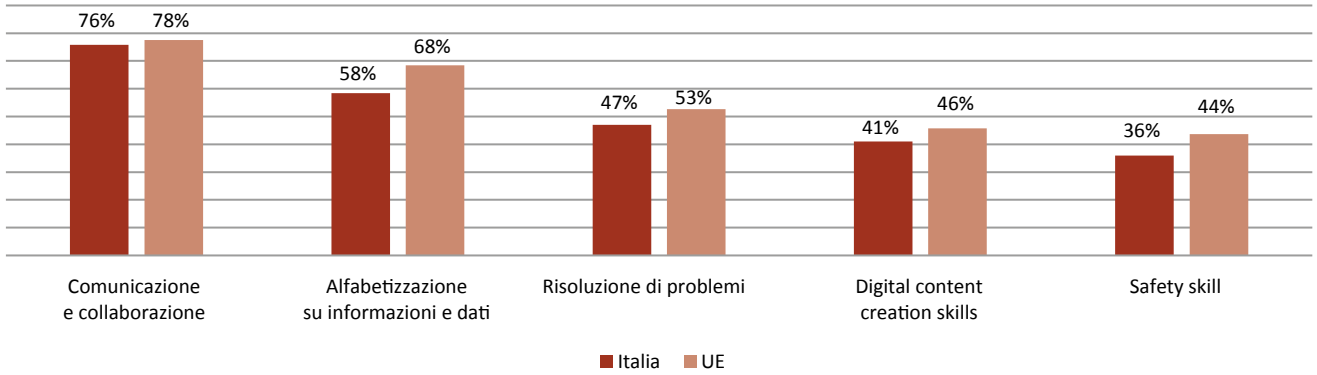
Fonte: Istat, 2023



45 04/01/2023, https://www.istat.it/it/files/2023/06/cs-competenzedigitali.pdf

Fig. 9.4: Quota popolazione con competenze elevate nelle 5 componenti delle competenze digitali (%, 2021)

Fonte: Istat, 2023



Un altro dato interessante che emerge dalle rilevazioni Istat evidenzia come le competenze digitali siano ancora prevalentemente possedute da individui con titoli di studio elevati. Infatti, l'80,3% delle persone di età compresa tra i 25 e i 54 anni con istruzione terziaria ha almeno competenze digitali di base, una percentuale quasi allineata con la media UE. Tuttavia, tale quota scende al 25% per le persone con titoli di studio bassi, fino alla licenza media, presentando un divario di circa l'8% rispetto alla media europea. Queste differenze significative emergono anche considerando la condizione occupazionale. In Italia, **il divario tra gli occupati che** hanno utilizzato internet negli ultimi 3 mesi e **possiedono competenze digitali di base rispetto a chi è alla ricerca di un'occupazione è del 17,8 %**. Inoltre, analizzando la posizione professionale degli occupati, emerge che gli operai presentano i livelli più bassi di competenze digitali, con una differenza di ben il 34,8 % rispetto a direttivi, quadri e impiegati (75,2% contro 36,7%). Questa disparità sottolinea l'importanza di promuovere l'accesso a formazione e strumenti digitali per tutte le categorie professionali, al fine di ridurre il divario esistente e garantire una società più inclusiva e preparata per l'era digitale.

Le competenze digitali possono essere suddivise, secondo le rilevazioni Istat e Eurostat, in cinque diverse dimensioni: comunicazione e collaborazione; alfabetizzazione su informazioni e dati; risoluzione di problemi; capacità di creare contenuti digitali; abilità di sicurezza. Utilizzando queste dimensioni, è possibile tracciare una mappa dei punti di forza e delle carenze nei livelli di preparazione dei cittadini italiani rispetto al panorama europeo. Secondo l'Istat, **i divari rispetto alla media UE sono minimi nel campo della "comunicazione e collaborazione"**, che riguarda l'interazione via internet e l'uso dei social media (75,8% vs 77,5%). Tuttavia diventano significativi nel campo della "creazione di contenuti digitali", che comprende l'utilizzo di applicazioni per creare o modificare contenuti digitali (41% vs 45,2%), e nella "risoluzione di problemi", che coinvolge l'utilizzo di servizi online e alcune abilità di gestione del software (47% vs 52,7%). Infine, emerge un netto ritardo nel campo dell'"alfabetizzazione su informazioni e dati", che riguarda la ricerca e l'interpretazione di informazioni e dati, nonché la capacità di valutarne la fonte (-9,8 p.p. rispetto alla media UE). Segue il dominio della "sicurezza", che si riferisce alla protezione dei dispositivi e dei dati personali negli ambienti digitali

(-7,6% rispetto alla media UE). In Italia, per ciascuna delle cinque dimensioni, i divari registrati per le competenze complessive confermano differenze legate al genere, all'età, al livello di istruzione e all'occupazione. Tuttavia, va segnalato che nel campo della "Comunicazione e collaborazione", le differenze di genere sono quasi inesistenti.

9.1.2. *Le competenze digitali del personale della PA*

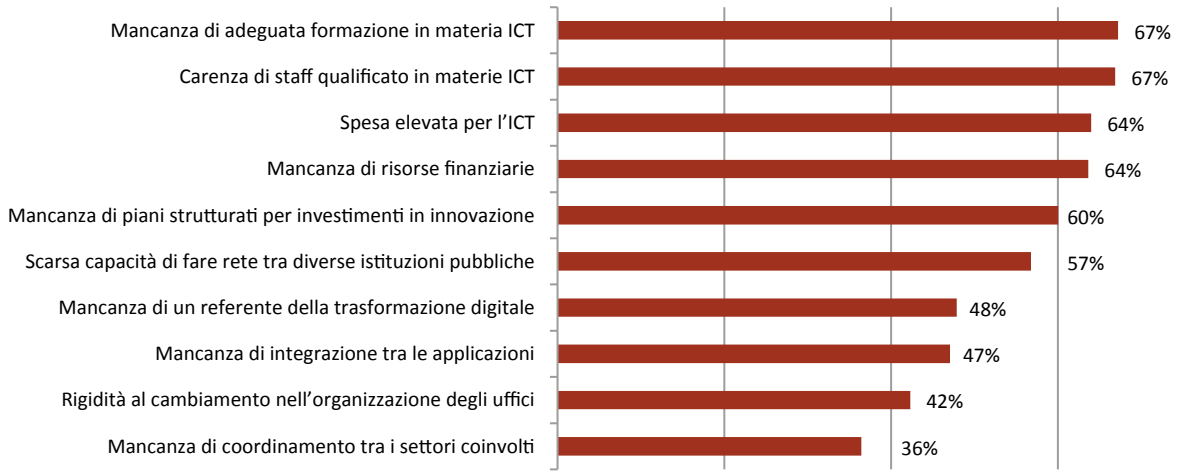
Nel contesto della transizione digitale la pubblica amministrazione assume un ruolo cruciale: il suo processo di digitalizzazione rappresenta una sfida critica e, al tempo stesso, un'importante opportunità. La digitalizzazione dei processi burocratici, mediante l'implementazione di tecnologie innovative e l'adozione di nuovi modelli operativi, conduce a una **significativa ottimizzazione delle risorse economiche e temporali**. Tale trasformazione apporta considerevoli vantaggi sia per le entità amministrative coinvolte, sia per le imprese e i cittadini. Inoltre, essa può segnare una svolta epocale nell'ambito tecnologico e culturale, rappresentando un autentico cambiamento di paradigma.

Il "Censimento permanente Istat delle Istituzioni pubbliche"[46], pubblicato il 28 dicembre 2022 ma contenente dati relativi all'anno 2020, segnala come i problemi più annosi rispetto al processo di digitalizzazione delle stesse siano **la mancanza di adeguata formazione in materia ICT** e **la carenza di personale qualificato** (problema comunque collegato all'insufficienza di competenze digitali)**,** individuate dal 67% dei rispondenti. Al terzo posto, con il 64%, troviamo il costo troppo elevato delle tecnologie ICT, non sempre alla portata dei budget ridotti delle Pubbliche Amministrazioni. Altro dato interessante è quello della **scarsa capacità delle istituzioni di fare rete** insieme alla mancanza di coordinamento dei settori coinvolti, che rappresentano un problema rilevante rispettivamente per il 57% e il 36% delle PA intervistate (Fig. 9.5).

Osservando il dettaglio relativo alle tipologie di enti, vediamo come la situazione più grave dal punto di vista della mancanza di adeguata formazione è

Fig. 9.5: Istituzioni pubbliche per tipologie di ostacoli al processo di digitalizzazione (%, 2020)

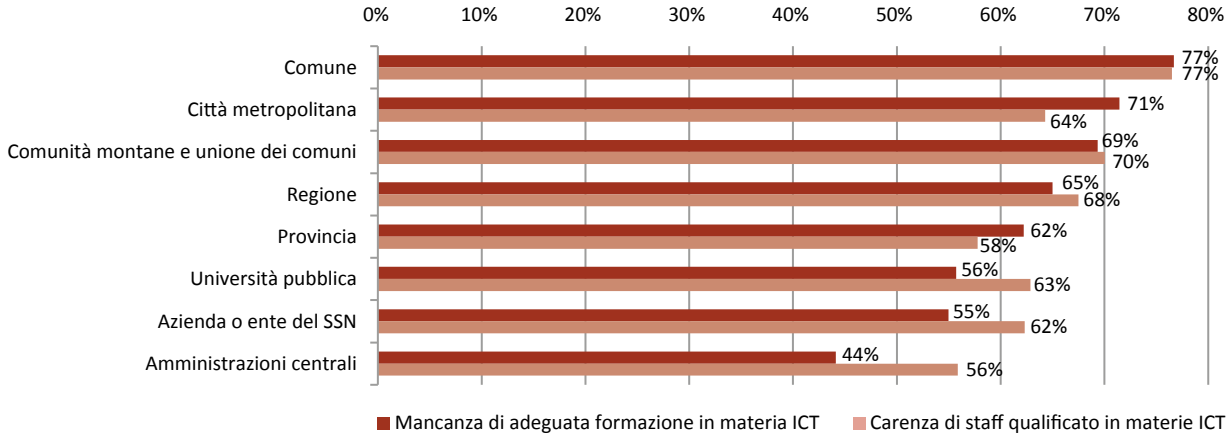
Fonte: Istat, Censimento permanente istituzioni pubbliche, 2022



46 https://www.istat.it/it/archivio/279341

Fig. 9.6: Istituzioni pubbliche per tipologie di ostacoli al processo di digitalizzazione per tipologia (%, 2020)

Fonte: Istat, Censimento permanente istituzioni pubbliche, 2022



segnalata dai **comuni (76,7%) e dalle città metropolitane (71,4%)**. I comuni primeggiano anche per carenza di personale qualificato in ICT (76,5%), ma questa volta il secondo posto è occupato dalle comunità montane e unioni di comuni (70%). In generale, dall'analisi dei dati appare piuttosto evidente come la formazione ICT e la scarsità di competenze tecniche in merito siano il tallone d'Achille di tutte le PA e in particolare degli enti locali (Fig. 9.6).

A conferma della forte necessità di maggiore formazione in materia ICT, **le pubbliche amministrazioni che hanno offerto corsi di formazione rappresentano una quota ridottissima** (Fig. 9.7). In particolare, esclusa l'Emilia-Romagna, in tutte le regioni italiane meno del 40% delle PA ha organizzato dei seminari per la formazione e metà delle regioni è addirittura sotto la quota del 30%. Ciò segnala una necessità di maggiori risorse per le pubbliche amministrazioni italiane, particolarmente di quelle finalizzate alla digitalizzazione e alla formazione del personale.

Fig. 9.7: Istituzioni pubbliche che hanno offerto corsi di formazione, per tipologia di corso (%, 2020)

Fonte: Istat, Censimento permanente istituzioni pubbliche, 2022

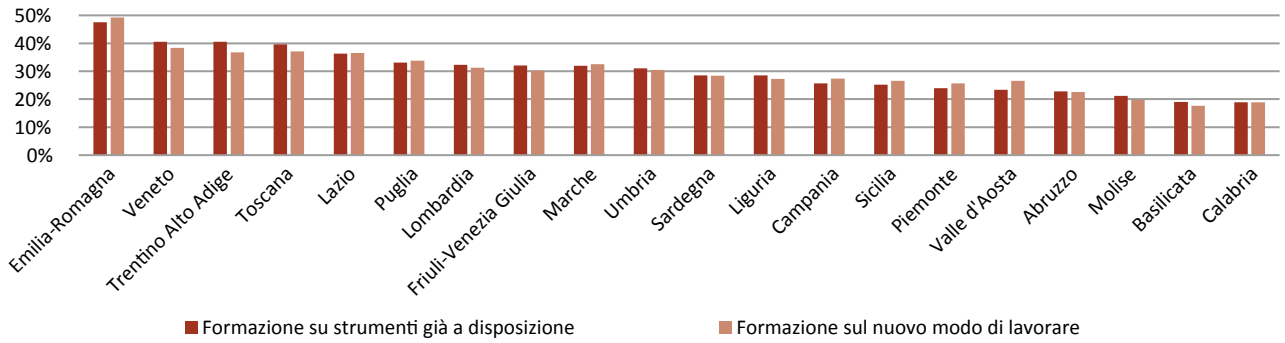
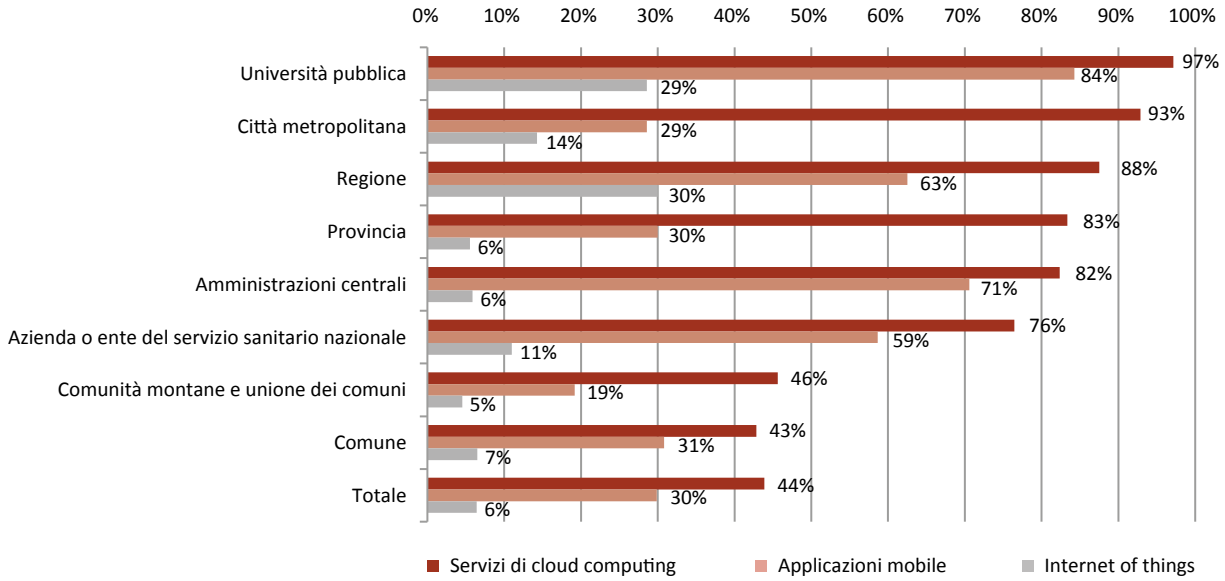


Fig. 9.8: La composizione della PA, per l'utilizzo di tecnologie innovative (%, 2020)

Fonte: Istat, Censimento permanente istituzioni pubbliche, 2022



La mancanza di formazione in ambito ICT influisce negativamente anche **sull'utilizzo di tecnologie innovative da parte delle amministrazioni**. Secondo i dati Istat **solo il 44% delle PA utilizza servizi di cloud computing**, strumento che appare fondamentale nell'efficientamento dei servizi e nella condivisione dei dati tra i vati enti (Fig. 9.8). La situazione appare ancora più critica se si prendono in esame le altre due tecnologie prese in considerazione dell'Istituto di Statistica nazionale, ossia le App mobili e l'IoT. In questo caso le percentuali calano vistosamente scendendo al 30% per le applicazioni per smartphone e addirittura ad appena il 6% per l'IoT.

È importante però considerare che **non tutte le tipologie di enti performano allo stesso modo**. Tra le amministrazioni più virtuose spiccano le Università pubbliche, che fanno registrare i valori più elevati per tutte le tecnologie considerate. Di converso, comuni e comunità montane e unioni di comuni si contendono le ultime posizioni nei tre ambiti analizzati.

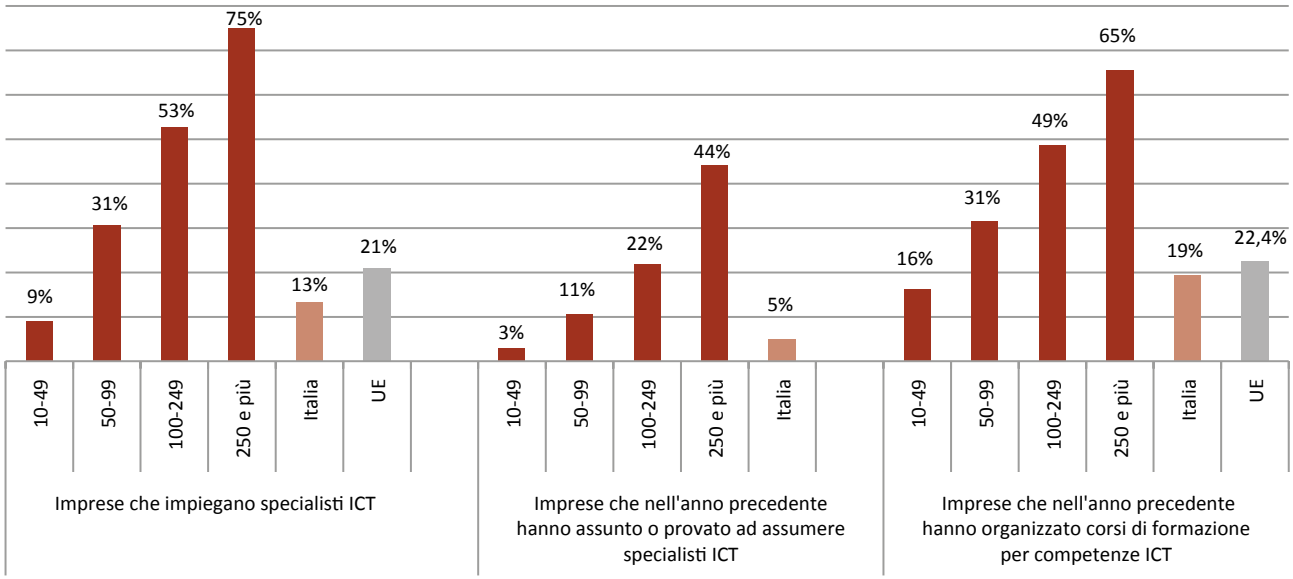
9.1.3. Le competenze digitali nelle imprese

La transizione digitale non può sicuramente prescindere dal contributo fondamentale delle imprese. Queste sono infatti uno dei principali driver della transizione stessa stimolando la cittadinanza ad avvicinarsi agli strumenti informatici, lanciando sul mercato prodotti e servizi sempre più innovativi. **Le imprese che investono nella formazione e nello sviluppo delle competenze digitali dei propri dipendenti acquisiscono un vantaggio competitivo significativo**. Queste competenze consentono alle aziende di adottare tecnologie innovative, automatizzare processi, migliorare l'efficienza operativa e creare nuove opportunità di business. Inoltre, una forza lavoro con solide competenze digitali è in grado di adattarsi agilmente ai cambiamenti tecnologici e affrontare le sfide del mercato globale, permettendo alle imprese di rimanere all'avanguardia nel panorama economico in continua evoluzione.

In merito alle competenze, il programma strategico

Fig. 9.9: Imprese e specialisti ICT (%, 2022)

Fonte: Istat



della Commissione europea per la transizione digitale prevede, oltre all'obiettivo sulle *skill* dei cittadini, anche il monitoraggio della quota di imprese che erogano ai propri addetti formazione in materia di ICT. Nella "Rilevazione sulle tecnologie dell'informazione e della comunicazione nelle imprese"[47] è stimata la quota di imprese che impiegano personale con competenze digitali specializzate. **Nel 2022 il 13,4% delle imprese italiane con almeno 10 addetti impiega esperti ICT.** Purtroppo, l'Italia anche in questo caso appare molto distante dalle principali economie dell'UE, in particolare da Germania (22,2%), Francia (17,6%) e Spagna (16,3%), oltre che **dalla media europea (21%)**. Come ci si aspetta sono le aziende più grandi a impiegare maggiormente gli specialisti ICT con una percentuale del 75%, a differenza delle imprese con un numero di dipendenti fra 10 e 49 che si fermano al 9%. Non a caso queste ultime rappresentano la categoria che esternalizza di più le funzioni ICT, solo il 17% le svolge internamente. Inoltre si osservano importanti divari fra le grandi imprese (con più di 250 dipendenti) e le imprese più piccole, aggregabili nella categoria delle PMI: circa il 12,2% delle piccole e medie imprese[48] impiega specialisti ICT contro il 75% delle grandi imprese. Sempre secondo l'Istat, addirittura il 57,2% delle piccole e medie imprese si affida esclusivamente ai fornitori esterni per le funzioni ICT contro il 14,2% delle aziende con più di 250 dipendenti.

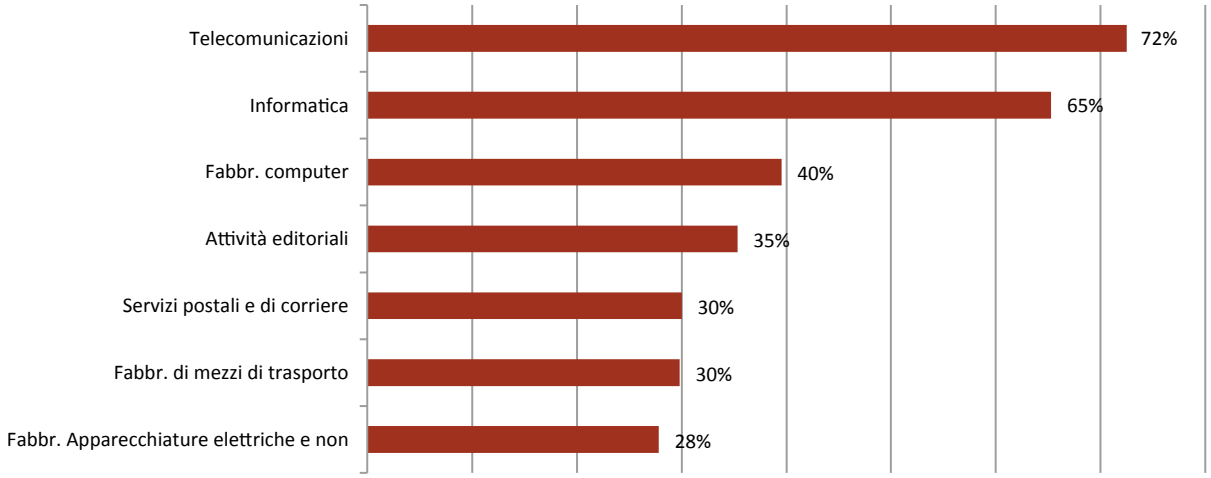
I settori delle telecomunicazioni e dell'informatica sono quelli che in percentuale impiegano più addetti ICT, rispettivamente per il 72% e il 65%. Il distacco rispetto agli altri settori è netto, infatti al quarto posto si trova la fabbricazione di computer con il 40%. Dunque si può affermare che la diffusione di competenze

47 https://www.istat.it/it/files//2023/01/REPORTICTNELLEIMPRESE_2022.pdf

48 Dato elaborato e riportato nel rapporto Istat "Cittadini e competenze digitali", 22/07/2023, https://www.istat.it/it/files/2023/06/cs-competenzedigitali.pdf

Fig. 9.10: Imprese italiane che impiegano specialisti ICT, per settore (%,2022)

Fonte: Istat

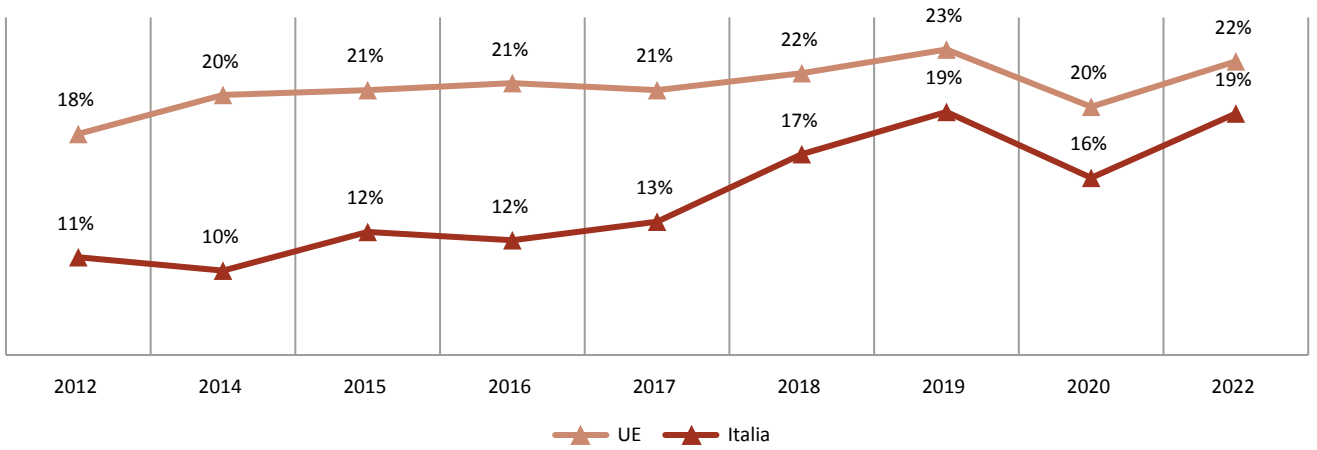


digitali dipende fortemente dal settore economico di appartenenza. Inoltre, Istat segnala l'assenza di una connessione rilevante fra la presenza di addetti specializzati in materia digitale nelle aziende e la collocazione geografica di quest'ultime.

È negativo anche il dato che emerge rispetto alle aziende che hanno erogato corsi di formazione in materie ICT al proprio personale (Fig. 9.11). L'Italia ha performato stabilmente peggio della media europea, con **la quota di aziende italiane che ha fornito**

Fig. 9.11: Aziende[49] che hanno fornito corsi di formazione in materie ICT al proprio personale

Fonte: Istat



49 Escluso il settore finanziario.

formazione che è sempre stata minore rispetto a quella delle corrispettive UE. Soltanto nel triennio 2017-2019 si è registrata una convergenza da parte dell'Italia che ha accorciato le distanze con il valore medio europeo. Nonostante quanto detto, in Italia lo stesso dato ha avuto una tendenza crescente nell'ultimo decennio, la stessa si è dimostrata particolarmente forte nel triennio 2017-2019 (la percentuale è passata dal 13% al 19%). Inoltre i dati rilevano una caduta del 3% durante la pandemia da Covid-19 seguita da un rilancio nel 2022.

In Italia dunque vi è ancora molto da fare per promuovere un'adeguata diffusione delle competenze digitali all'interno delle imprese per riempire le molteplici lacune attuali. A tal proposito il 68% delle aziende del settore telco, non sorprendentemente uno dei comparti più virtuosi in materia di digitalizzazione e competenze digitali, ritiene che sia **necessario potenziare la formazione in ambito cybersecurity**. Questa è seguita al secondo posto dalle competenze relative al cloud computing, che si attestano sul 58%, e da internet of Things, IA, machine learning e big data a pari merito con il 53%.

9.2. LA DOMANDA DI COMPETENZE TECNICHE

9.2.1. La produzione di diplomati tecnici e laureati

Le tecnologie digitali sono ormai molto diffuse fra gli studenti e gli individui di giovane età, che vengono a contatto sempre più precocemente con dispositivi e applicativi informatici. Tuttavia, la frequenza di utilizzo non sempre è sinonimo di sviluppo delle competenze digitali, siano esse generiche o specialistiche. Durante gli anni **il numero di laureati in materie STEM è rimasto grossomodo stabile** benché vi sia stata una rilevante caduta dei laureati dal 2021 al 2022 di circa 4.400 individui. Non considerando il 2022 sono costantemente aumentati i laureati in tutte le materie considerate, ad eccezione tuttavia di quelli in architettura e ingegneria civile che invece sono diminuiti da 15.572 a soli 9.630 nel 2022.

Un ennesimo preoccupante record negativo dell'Italia viene registrato nella **quota di laureati ICT sui laureati totali**. Essa si posiziona **ultima nella classifica di tutte le nazioni dell'Unione Europea con solamente**

Fig. 9.12: Hard skill digitali che necessitano potenziamento nelle imprese italiane (% di imprese delle telecomunicazioni, 2022)

Fonte: Survey Osservatori Digital Innovation Politecnico di Milano su associati AssTel, Rapporto sulla filiera TLC 2022

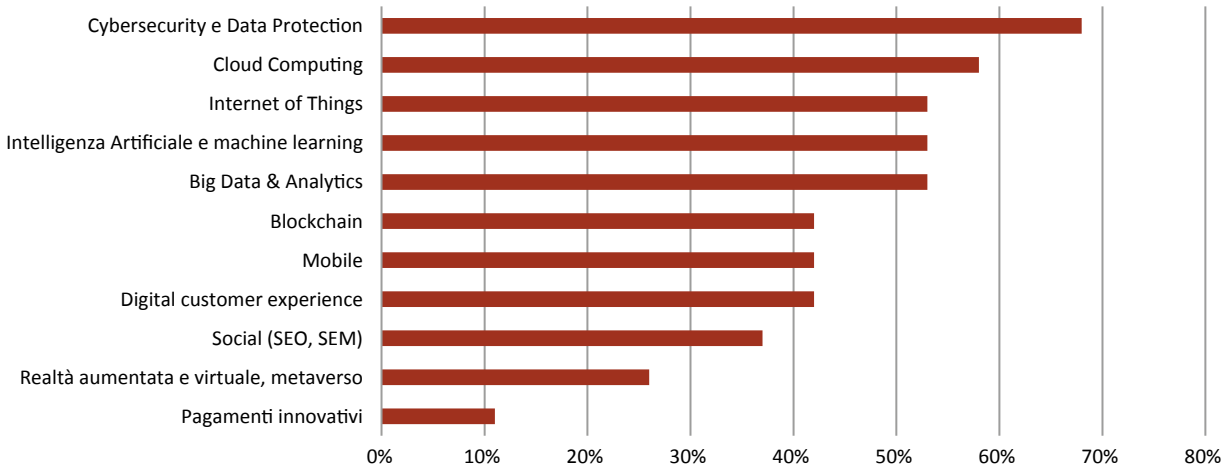
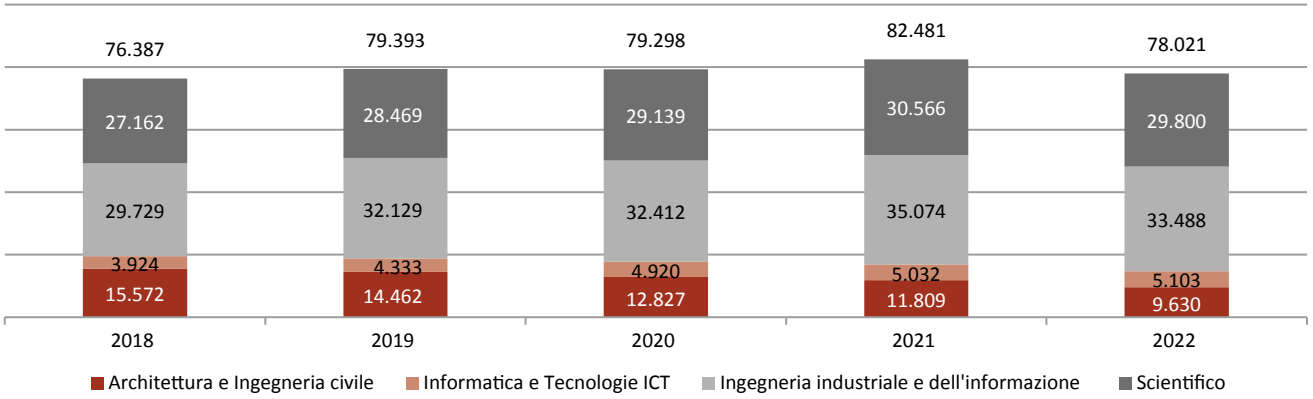


Fig. 9.13: Laureati in materie STEM in Italia

Fonte: Almalaurea



l'1,4% di laureati in materie ICT, contro una media comunitaria del 3,9%. Delle grandi economie dell'Europa occidentale soltanto la Francia è insieme all'Italia sotto la media europea con il 3,6%; la Spagna e la Germania si posizionano rispettivamente al 4% e al 4,9%, ben più che doppiando l'Italia.

Un altro elemento da considerare per poter valutare la preparazione alla transizione digitale da parte dell'Italia sono i **diplomati negli istituti tecnici** (è stato preso in considerazione il settore tecnologico). Negli anni i dati (Fig. 9.15) mostrano un'evidente **tendenza discendente**: i diplomati in istituti tecnici tecnologici sono scesi da 8.274 nel 2018 ad appena 5.854, con un calo pari circa al 30%. L'unico anno in cui si è invertita la tendenza è il 2021 in cui i diplomati sono aumentati da 6.330 a 7.110. È da segnalare comunque che non sembra esserci stato un effetto particolarmente rilevante della pandemia di Covid-19.

Fig. 9.14: Laureati in materie ICT in percentuale dei laureati totali del paese (2022)

Fonte: Eurostat

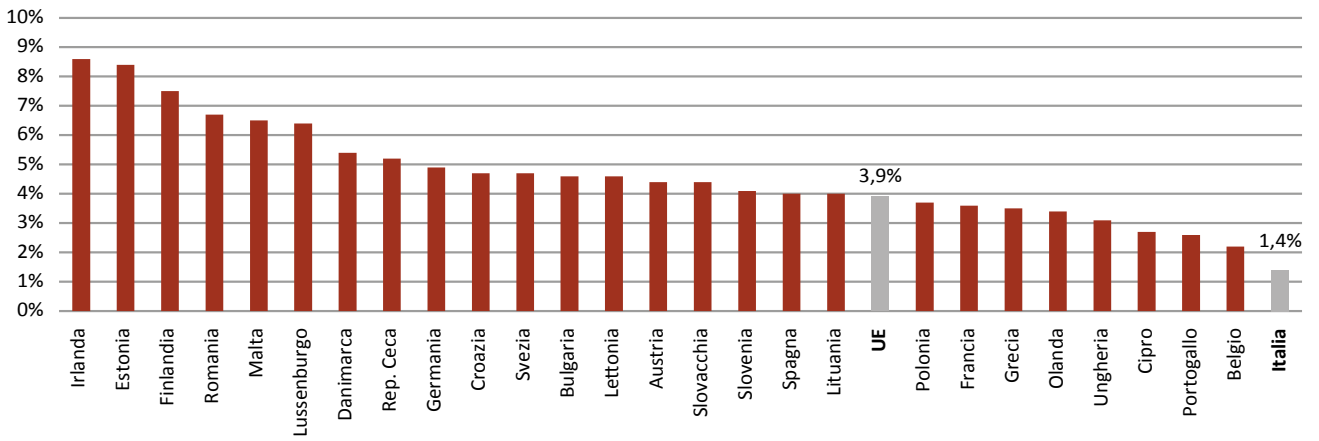
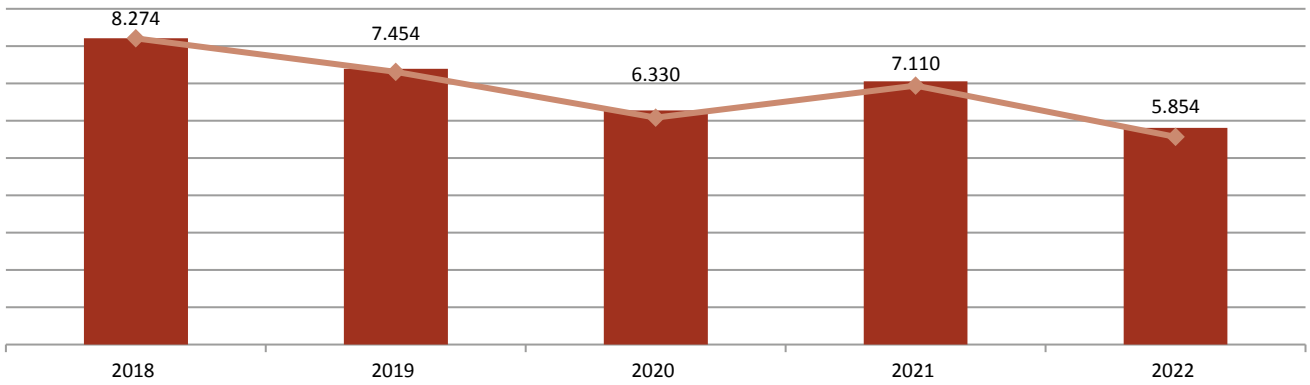


Fig. 9.15: Diplomati negli istituti tecnici in Italia (settore tecnologico)

Fonte: Almadiploma



9.2.2. Le competenze in cybersecurity

L'evoluzione digitale ha condotto con maggiore frequenza negli ultimi anni ad accrescere l'uso che i cittadini fanno della rete, con un conseguente e reciproco adattamento della stessa alle attività tipiche della vita quotidiana, come quella lavorativa, scolastica, sociale e così via. Inevitabilmente, si tratta di una tendenza che ha osservato un aumento significativo durante la pandemia da Covid-19, in quanto le limitazioni legate alla circolazione e al contatto sociale hanno determinato un impiego sempre più pervasivo di internet, sia da parte di soggetti pubblici che privati.

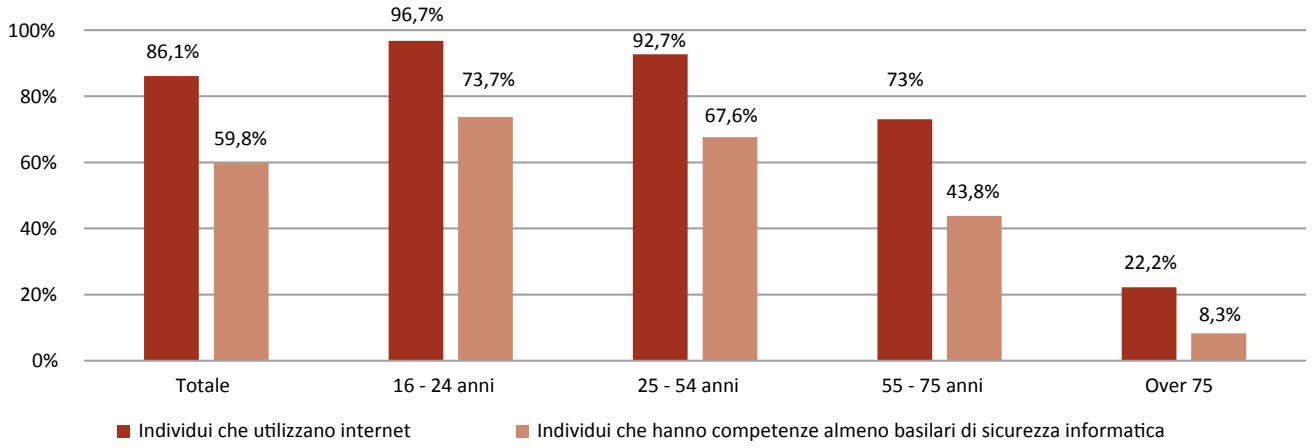
Ciò ha permesso di trarre vantaggi e nuove opportunità dall'innovazione tecnologica, pur non escludendo una serie di rischi che hanno interessato l'esperienza online di un numero considerevole di utenti, i quali non sempre presentano le competenze adeguate per prevenire e gestire al meglio le minacce cibernetiche a cui sono esposti. Difatti, **lo *human factor* rappresenta una delle maggiori cause di attacchi informatici** soprattutto perché, quando il bersaglio è un individuo, la possibilità di attuare frodi online, mediante tecniche di persuasione, di manipolazione e di convincimento, produce effetti particolarmente distruttivi. Per ridurre tali pericoli è necessario puntare sull'aumento del livello di consapevolezza e competenza degli utenti.

L'analisi dei dati forniti da Eurostat con riferimento all'anno 2022 (Fig. 9.16) evidenzia che solo il 59,8% dei cittadini ha competenze almeno basilari in materia di sicurezza informatica. Inoltre, puntando il focus sulla scomposizione per età, la quota di persone impreparate in cibersicurezza cresce in maniera direttamente proporzionale all'età anagrafica. Dai dati emerge come **un italiano su quattro tra i 16 e i 54 anni è carente di conoscenze di sicurezza informatica di base**, quota che sale ad uno su tre se si considera la fascia di età 55-74 e a due su tre per gli over 75. Nonostante ciò, la percentuale di utilizzo di internet è superiore di 26,3 p.p. rispetto al grado di competenze succitato, con un distacco maggiore nella fascia 16-24 anni. Pertanto, si sottolinea che fattori come l'utilizzo inconsapevole della rete, l'inadeguata gestione delle password, l'incapacità di distinguere tentativi di phishing tramite e-mail e l'assenza di policy aggiornate, nonché adeguate, rappresentino elementi attrattivi per i cybercriminali.

Per comprendere al meglio il quadro nazionale sulle iniziative finalizzate ad aumentare le competenze in cybersecurity, va preso in considerazione il

Fig. 9.16: Quota di italiani che utilizzano internet (2021) e di individui che hanno almeno competenze basilari di sicurezza informatica (%, 2022)

Fonte: Eurostat



monitoraggio delle attività di formazione sulla cibersicurezza in ambito universitario avviato a partire da gennaio 2022 dall'Istituto per la Competitività (I-Com). Nello specifico, con riferimento all'anno accademico 2022/2023[50], si registra la presenza di **271 corsi di formazione universitaria** che comprendono sia insegnamenti singoli all'interno di corsi di laurea più generici – "offerta formativa non specializzata" – sia corsi di laurea specifici sul tema, insieme a Master e Dottorati – "offerta formativa specializzata" – nell'ambito di 97 Università statali e non statali (private, straniere e telematiche) riconosciute dal Miur. Precisamente, sono stati osservati 112 insegnamenti singoli all'interno di corsi di laurea magistrale, 56 insegnamenti singoli all'interno delle lauree triennali, 44 dottorati, 22 lauree magistrali, a fronte di 13 corsi all'interno di dottorati di ricerca, 18 master e 4 lauree triennali interamente concernenti la cybersecurity (Fig. 9.17).

La formazione specializzata post-laurea si affianca a quella universitaria con differenze in termini quantitativi importanti, ovverosia ben 62 corsi "specializzati" tra master e dottorati a fronte delle 26 tra lauree triennali e biennali dedicate. Pertanto, **è importante notare come la formazione specializzata in materia di cibersicurezza in Italia abbia raggiunto quota 88 corsi di studio interamente dedicati.**

In merito alla distribuzione dell'offerta formativa specializzata e non specializzata a livello regionale, si osserva come questa appaia piuttosto frammentata (Fig. 9.18), segnalando una forte concentrazione nel Lazio (46 corsi), in Piemonte (33 corsi) e in Campania (32), seguite da Lombardia e Toscana (23 corsi ciascuno). Il Piemonte, in particolare, risulta nettamente primo in termini di corsi in cybersecurity normalizzati per il numero di università presenti sul territorio regionale (con un rapporto di 8,3:1), seguito da Liguria (5:1) e Sicilia (4,5:1). D'altro canto, sono 29 le Università che non presentano nella propria offerta formativa alcun insegnamento o un corso di studio relativo alla cybersecurity. A livello regionale, a gennaio 2023 solo Basilicata e Valle d'Aosta risultavano non proporre corsi di questo genere.

50 Il monitoraggio condotto nel 2022 è stato aggiornato e rimodulato all'inizio dell'anno in corso, includendo l'offerta formativa 2022-2023 disponibile sui siti web delle università statali e non statali, incluse quelle online.

Fig. 9.17: Offerta formativa specializzata e non specializzata in materia di cybersecurity, per tipo (a.a. 2022-23)

Fonte: I-Com, gennaio 2023
*Include corsi generici sulla cybersecurity che possono essere seguiti per ottenere crediti formativi, nonché singoli corsi all'interno di Master
**Comprende i 41 progetti di ricerca che rientrano nell'ambito del dottorato nazionale in cybersicurezza

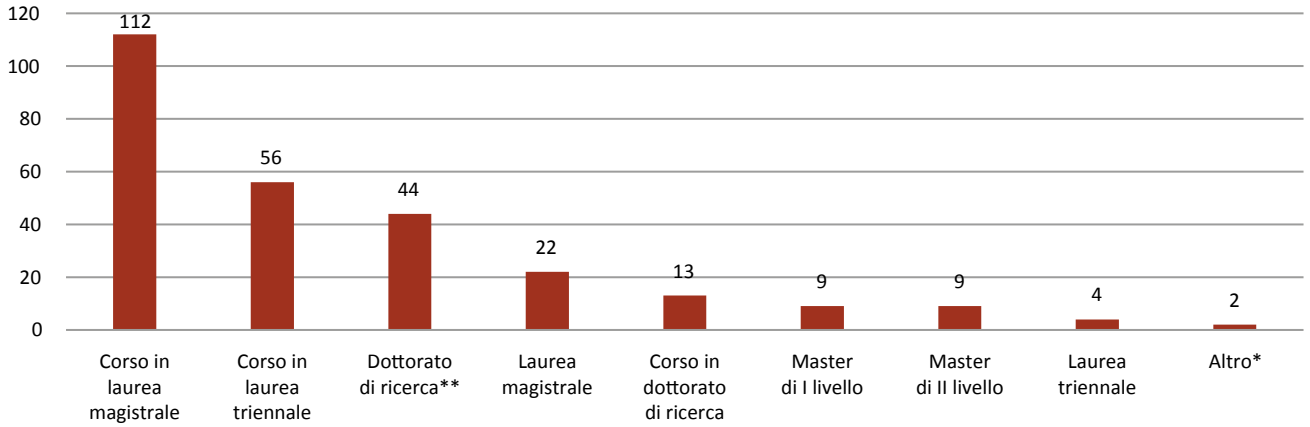
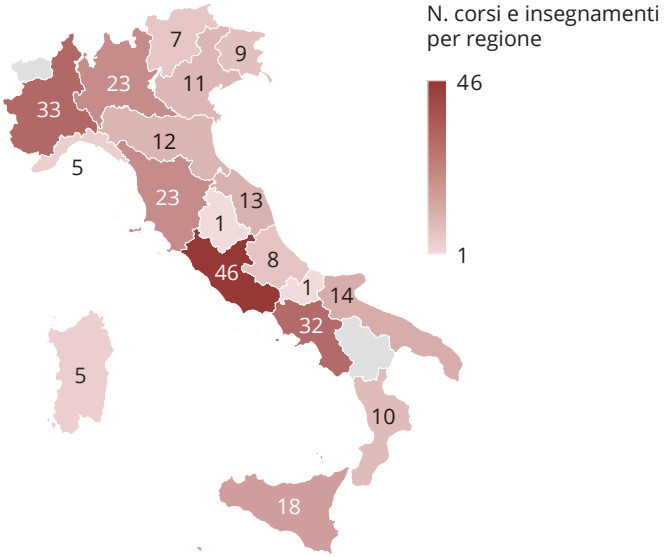


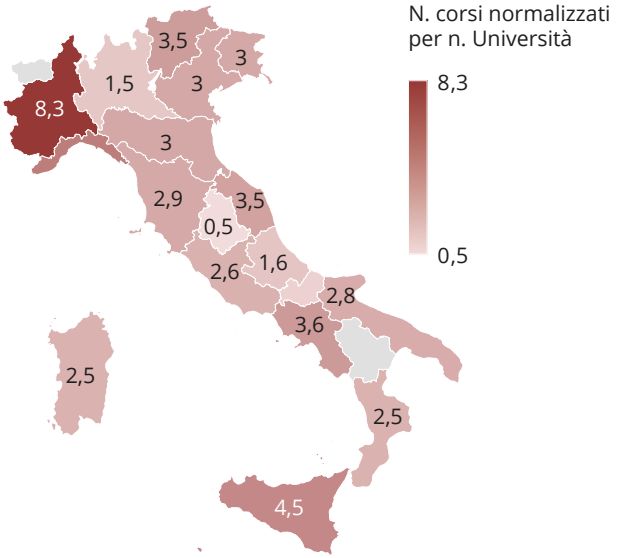
Fig. 9.18: Offerta formativa sulla cybersecurity, per regione (a.a. 2022-2023)

Fonte: I-Com, gennaio 2023

N. corsi e insegnamenti per regione



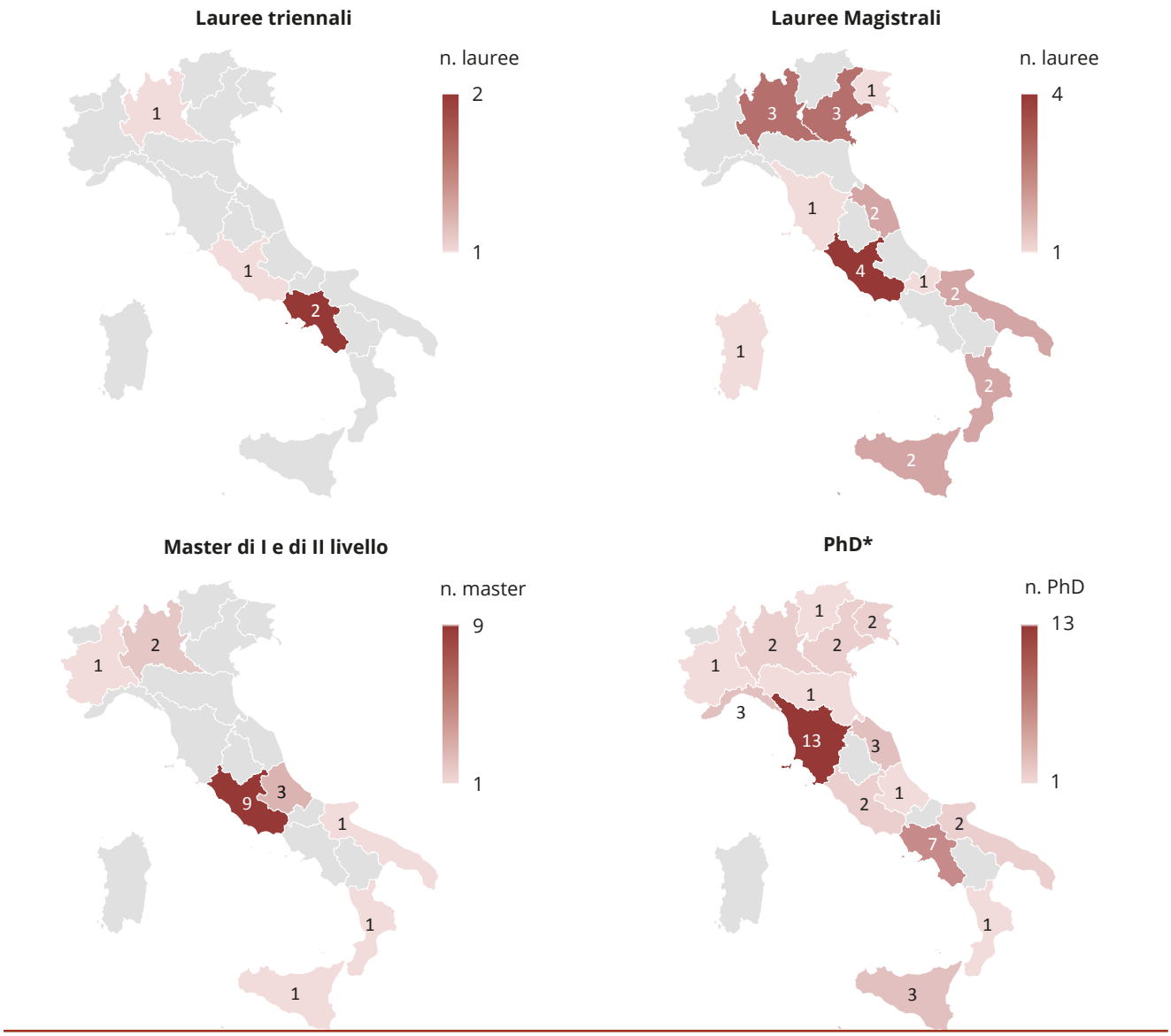
N. corsi e insegnamenti normalizzati per n. di università per regione



Analizzando la mappa geografica dell'offerta formativa universitaria specializzata (Fig. 9.19), il Lazio si conferma la regione più interessata con 16 percorsi complessivi, catalizzando gran parte dell'offerta in termini di lauree dedicate (5 tra magistrali e triennali). Per quanto concerne la specializzazione

Fig. 9.19: Offerta formativa specializzata sulla cybersecurity per regione (a.a. 2022-23)

Fonte: I-Com, gennaio 2023
Note: L'offerta formativa specializzata comprende una Laurea Triennale, una Laurea Magistrale, un Master I Livello, un Master II Livello o un Phd incentrati sul tema della cybersecurity
*Comprende i 41 progetti di ricerca che rientrano nell'ambito del dottorato nazionale in cybersicurezza



post-laurea, in Toscana si contano 13 corsi di dottorato, seguita dal Lazio (9 master e 2 dottorati) e dalla Campania (2 master e 7 dottorati), mentre chiude la classifica il Trentino-Alto Adige con un unico dottorato. **Nel contesto della formazione specializzata, è interessante notare anche l'elevato numero di master specifici sui temi della cybersicurezza, per cui su tutto il territorio nazionale ne sono stati rilevati 18, 9 di I Livello e ulteriori 9 di II Livello, di cui oltre la metà con sede nel Lazio.**

Una maggiore attenzione per la formazione in sicurezza informatica si è evinta anche nell'ambito degli Istituti Tecnici Superiori (ITS). Ciò è ancor più chiaro in virtù del fatto che **il 5 ottobre 2022 è stato firmato, presso il Ministero dell'Istruzione, l'Accordo per la Rete di coordinamento nazionale per lo sviluppo di percorsi formativi specifici in cybersecurity nell'ambito degli ITS Academy**, che rientra nel percorso di rafforzamento della formazione terziaria professionalizzante ottenuto con l'approvazione in Parlamento della riforma degli ITS ad opera della L. n. 99 del 15 luglio 2022.

L'accordo in questione avrà durata di un anno dalla sottoscrizione, prevedendo la futura costituzione di un comitato di coordinamento scientifico e tecnico.

Secondo l'aggiornamento risalente a giugno 2023 del monitoraggio INDIRE e un'analisi svolta da I-Com (Fig. 9.20), gli ITS interessati alla cybersicurezza sono il 14% rispetto al numero complessivo di quelli attivi. La Lombardia primeggia con 3 istituti su 24 totali, seguita dal Lazio che ne presenta 3 su 16. Il Veneto, il Friuli-Venezia Giulia e la Toscana registrano 2 istituti che si occupano di cibersicurezza, rispettivamente, su un numero di 8, 4 e 9 totali per regione.

Tra gli ITS specializzati in sicurezza informatica alcuni avvieranno i loro corsi a partire dall'anno accademico 2023-2024, con un'offerta formativa incentrata anche sulla protezione dei dati personali oltre che sulla gestione delle *cyber threats* che colpiscono reti, sistemi e servizi informatici.

Differenziando i corsi sulla sicurezza informatica dai corsi con almeno un insegnamento incentrato sul tema (Fig. 9.21), **a livello regionale la Lombardia presenta una relazione di 3 corsi specifici rispetto a 10**

Fig. 9.20: Comparazione tra il numero di ITS per regione e ITS che si occupano di cybersecurity

Fonte: INDIRE; I-Com, giugno 2023

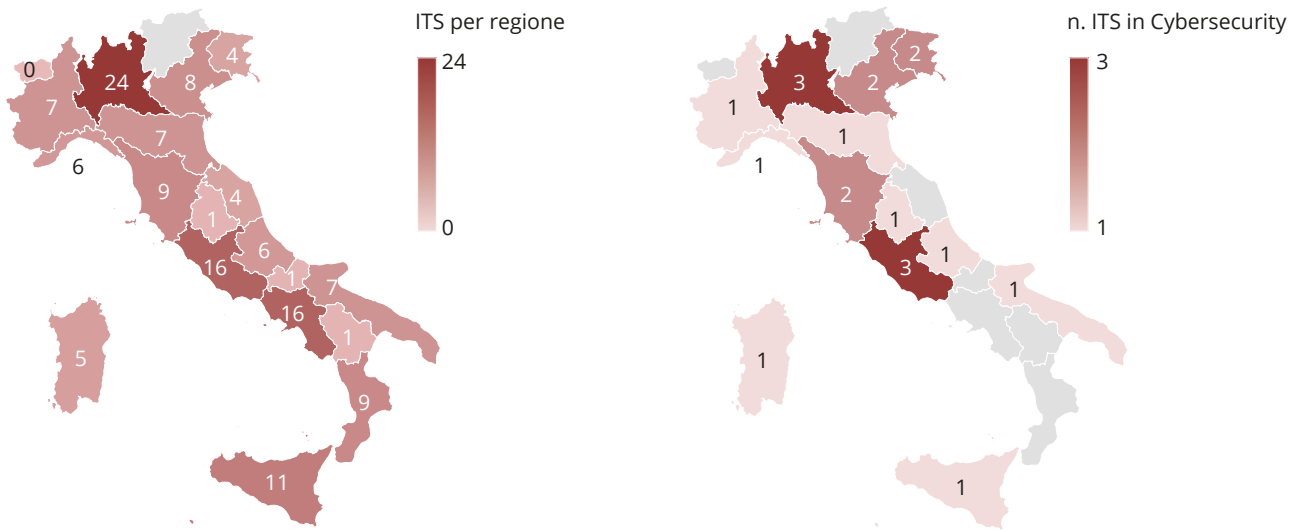
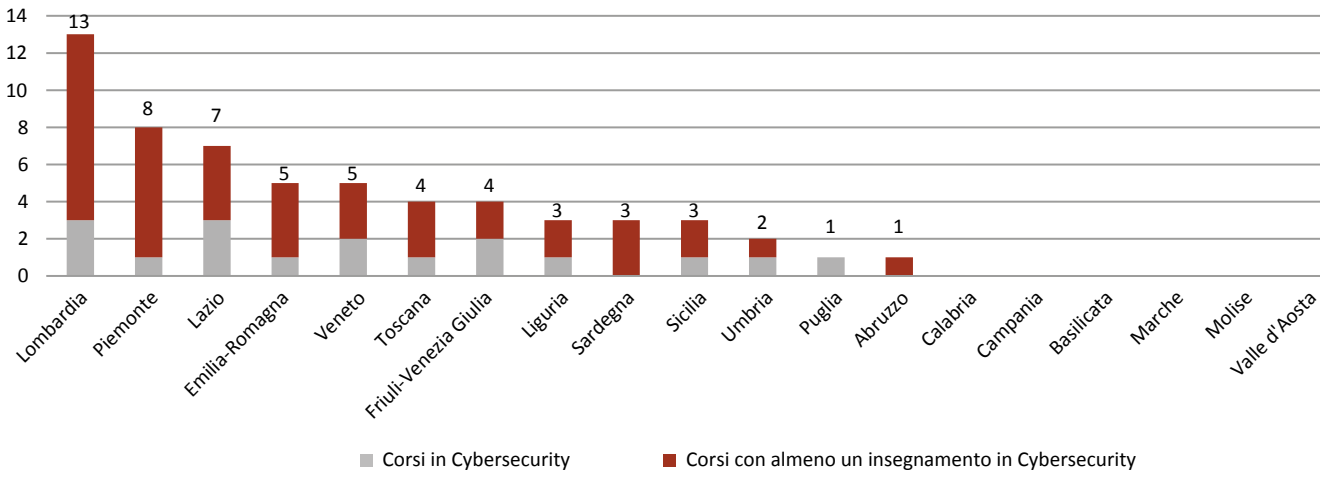


Fig. 9.21: Distribuzione per regione corsi in cybersecurity e corsi con almeno un insegnamento in cybersecurity

Fonte: I-Com, gennaio 2023



insegnamenti appartenenti alla seconda categoria, distribuiti su tutto il territorio. A sua volta, il Piemonte è connotato da un rapporto di 7 a 1, seguito dal Lazio e dall'Emilia-Romagna. Mentre Puglia e Abruzzo, a pari merito, hanno un unico corso in cybersecurity, per quanto riguarda la prima, e un unico insegnamento legato a corsi non specifici cyber, con riferimento al secondo. Inoltre, sono ben 6 le regioni (Calabria, Campania, Basilicata, Marche, Molise, Valle d'Aosta) che non presentano alcun corso afferente alle due tipologie summenzionate.

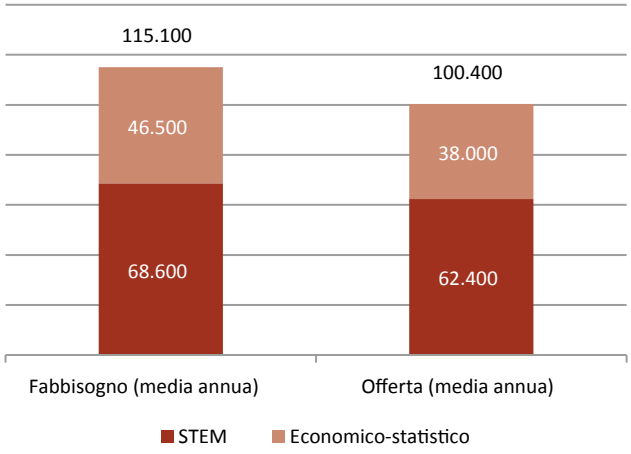
9.2.3. Il mismatch fra domanda e offerta

Secondo il Report di Anpal-Unioncamere relativo al periodo 2023-2027[51], nello stesso arco temporale è previsto un fabbisogno da parte del sistema economico italiano di occupati in possesso di una formazione terziaria (ovvero di una laurea o un diploma di un Istituto Tecnologico Superiore – ITS Academy) pari a circa 1,3 milioni di unità, che corrispondono a oltre 250mila in media all'anno. **Le materie STEM e quelle economico-statistiche sono quelle che primeggiano tanto nel fabbisogno quanto nell'offerta**. Il fabbisogno annuo medio ammonta a 68.600 unità per le materie STEM e 46.500 per le economico-statistiche (in totale 115.100), l'offerta media annua invece è di 62.400 individui delle materie STEM e 38.000 di quelle economico-statistiche (in totale 100.400). Risulta quindi un divario fra le due di circa 15.000 unità annue per un totale di 73.500 lavoratori mancanti in tutto il quinquennio analizzato. Dei lavoratori in possesso di una formazione terziaria in ambito STEM, il 44% del fabbisogno è rappresentato dalla richiesta di lauree in ingegneria insieme a diplomi ITS Academy in mobilità sostenibile, meccanica e moda, il 21% dall'ingegneria civile ed architettura e ai diplomi ITS Academy "Efficienza energetica" e "Sistema casa" e il 17% dagli indirizzi in scienze matematiche, fisiche e informatiche. Invece, per le discipline economico-statistiche, una parte rilevante del fabbisogno è determinata dalla filiera della consulenza e della finanza. Questi settori saranno sempre più interessati dall'innovazione

51 https://excelsior.unioncamere.net/pubblicazioni/2023/previsioni-dei-fabbisogni-occupazionali-e-professionali-italia-medio-termine

Fig. 9.22: Fabbisogno e offerta di laureati STEM e economico-statistici nel periodo 2023-2027

Fonte: Unioncamere-ANPAL, Sistema Informativo Excelsior

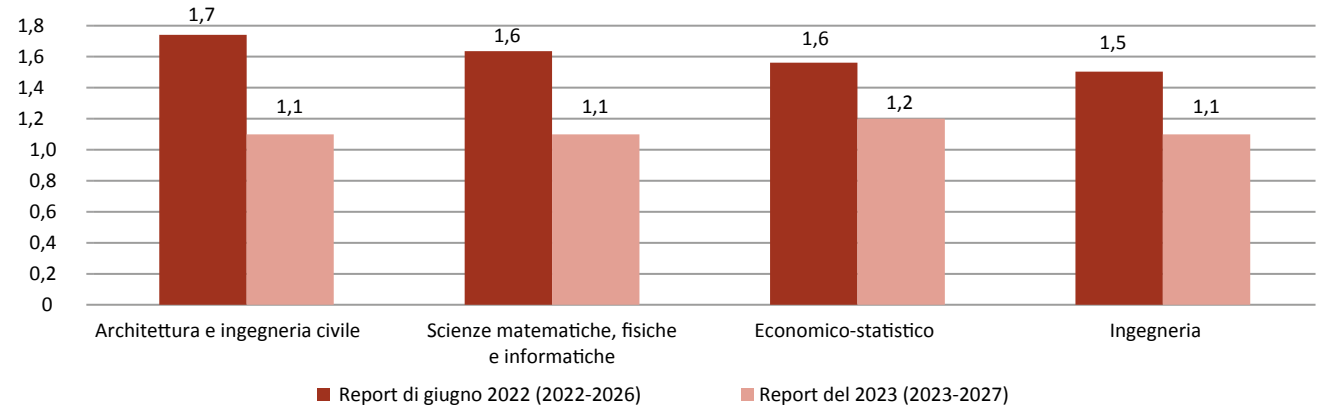


tecnologica, richiedendo professionisti in possesso di elevate competenze digitali, ad esempio per operare nel fintech ovvero nell'ambito delle blockchain e della sicurezza. I servizi consulenziali saranno fondamentali per la gestione dei progetti legati al PNRR.

In tutti i casi il fabbisogno è maggiore dell'offerta e quindi il rapporto fra i due (Fig. 9.23) è sempre maggiore di uno. Una versione poco più datata dello stesso studio, quella di giugno 2022, presentava i dati dettagliati del rapporto fabbisogno/offerta per ogni singola area disciplinare; nell'ultima versione disponibile invece le matterie STEM sono state raggruppate in un'unica area, nella figura che segue dunque si utilizza lo stesso dato per le singole materie. Il rapporto relativo all'ambito economico-statistico risultava essere molto alto a giugno 2022, ossia 1,6, mentre nell'ultimo documento scende a 1,2. Rispetto alle materie STEM invece il rapporto fabbisogno/offerta è molto vicino a 1 (quindi l'offerta riesce quasi a coprire la domanda), ma questo dato potrebbe essere distorto proprio perché le materie sono raccolte in un unico gruppo. Se invece si osserva la versione immediatamente precedente dello studio, il settore per cui c'è più domanda è quello dell'architettura e dell'ingegneria civile, probabilmente proprio per realizzare i progetti infrastrutturali del PNRR. Le scienze matematiche, fisiche e informatiche si posizionano subito dopo, a pari merito con le materie economico-statistiche con un rapporto pari a 1,6; invece i laureati in ingegneria sono richiesti con un rapporto di 1,5 fra domanda e offerta. Per tutte le materie lo studio di giugno 2022 rileva molta più richiesta dell'offerta effettiva.

Fig. 9.23: Rapporto Fabbisogno/Offerta per area disciplinare

Fonte: Unioncamere-ANPAL, Sistema Informativo Excelsior



9.3. L'IMPATTO DEL PNRR E LE INIZIATIVE SULLE COMPETENZE

Numerose iniziative sono state adottate per potenziare l'offerta educativa fornita dal sistema pubblico di istruzione italiano. Tra queste, **la riforma 1.1 all'interno della M4C1.1 del Piano Nazionale di Ripresa e Resilienza** (PNRR) **ha l'obiettivo di allineare i programmi di studio degli istituti tecnici e professionali alle richieste di competenze digitali provenienti dal mondo produttivo nazionale**. Essa mira dunque a ridurre la discrepanza già evidenziata tra la domanda e l'offerta di competenze. Inoltre, sono previste ulteriori iniziative per rafforzare questo legame tra istituti di istruzione e imprese. La riforma del sistema degli Istituti Tecnici Superiori (ITS), approvata con la Legge n. 99/2022, amplia i programmi formativi per lo sviluppo delle competenze tecnologiche e promuove una maggiore interazione con il mondo imprenditoriale locale. In questa prospettiva di rafforzamento dei legami tra istituti di istruzione e imprese, l'investimento 1.5 all'interno della M4C1.1 del PNRR prevede l'allocazione di 1,5 miliardi di euro per la creazione di reti di collaborazione tra aziende, università, centri di ricerca tecnologica e scientifica, autorità locali e istituzioni educative e formative. Inoltre, è prevista l'istituzione di una piattaforma digitale nazionale dedicata alle opportunità di lavoro destinate agli studenti con qualifiche professionali, con l'obiettivo di aumentare il numero di studenti coinvolti nei percorsi degli ITS. Si mira a raddoppiare almeno il numero attuale di partecipanti. Infine, per potenziare le competenze digitali e le competenze STEM (Scienze, Tecnologia, Ingegneria e Matematica), sono previste misure all'interno del Piano Scuola 4.0, finalizzate alla digitalizzazione di

Tab. 9.1: Iniziative per le competenze digitali della popolazione

Fonte: PNRR

Iniziative	Risorse	Principali misure
Riforma degli istituti tecnici e professionali e del sistema degli ITS	Riforme	• Riforma 1.1: allineare i curricula degli istituti tecnici e professionali alla domanda di competenze digitali che proviene dal tessuto produttivo del Paese, riducendo il *mismatch* tra domanda e offerta
		• Ampliamento dei percorsi per lo sviluppo delle competenze tecnologiche e rafforzamento della presenza attiva all'interno del tessuto imprenditoriale dei singoli territori
Sviluppo del sistema di formazione professionale terziaria	€1,5 mld	• Creazione di network con aziende, università e centri di ricerca tecnologica/scientifica, autorità locali e sistemi educativi/formativi
		• Istituire una piattaforma digitale nazionale per le offerte di lavoro rivolte agli studenti in possesso di qualifiche professionali
Piano Scuola 4.0	€2,10 mld	• Trasformazione di circa 100.000 classi tradizionali in connected learning environments, con l'introduzione di dispositivi didattici connessi
		• Creazione di laboratori per le professioni digitali
		• Digitalizzazione delle amministrazioni scolastiche
		• Cablaggio interno di circa 40.000 edifici scolastici e relativi dispositivi
Rafforzamento delle competenze digitali di base della popolazione	€20 milioni	• Rafforzamento del network territoriale di supporto digitale, alle fasce della popolazione a maggior rischio di subire le conseguenze del *digital divide*
		• Servizio Civile Digitale: reclutamento di diverse migliaia di giovani che aiutino circa un milione di utenti ad acquisire competenze digitali di base
Centri di facilitazione digitale	€195 milioni	• Istituzione di punti di accesso fisici come biblioteche, scuole e centri sociali che forniscano ai cittadini formazione sia di persona che online sulle competenze digitali, supportando l'inclusione digitale

tutto l'ambiente scolastico. Questa iniziativa rientra nell'ambito dell'investimento 3.2 del PNRR, Missione 4, Componente 1, e punta a promuovere una significativa trasformazione degli spazi scolastici in contesti innovativi per l'apprendimento, oltre a favorire la creazione di laboratori per le professioni digitali del futuro. In totale, saranno investiti 2,1 miliardi di euro per questo importante obiettivo.

Sono numerose le iniziative volte a potenziare le competenze all'interno delle imprese, ma tra di esse spiccano per importanza le misure legate alla Transizione 4.0 (bisognerà osservare con attenzione quali confluiranno nella nuova "Transizione 5.0"). In questo contesto, le imprese che investono in programmi di formazione dedicati alla digitalizzazione e alle relative competenze possono beneficiare di crediti d'imposta. Queste misure si coordinano in modo sinergico con gli interventi che riguardano la riforma del percorso formativo offerto dal sistema pubblico di istruzione italiano, come precedentemente detto. Qui, l'attenzione è rivolta al potenziamento della ricerca di base e applicata insieme alla promozione del trasferimento tecnologico.

Particolare rilevanza è attribuita alle misure destinate a rafforzare le competenze del personale della Pubblica Amministrazione (PA), con un budget di €490 milioni, che operano su tre fronti. In primo luogo, è prevista un'ampia offerta di corsi online per il "reskilling" e "upskilling" delle competenze dei dipendenti pubblici. Questi corsi mirano a sviluppare le competenze manageriali necessarie per una moderna e efficiente amministrazione pubblica.

Tab. 9.2: Iniziative per le competenze del personale delle imprese e della PA

Fonte: PNRR

Iniziative	Risorse	Principali misure
Transizione 4.0	€13,38 mld	• Crediti di imposta alle imprese che investono in attività di formazione alla digitalizzazione e alle relative competenze
		• Riqualificazione manageriale, focalizzato sulle PMI, con programmi di formazione per la crescita di competenze gestionali in ambito digitale
		• Programmi di formazione continua per l'*upskilling* e il *reskilling* dei lavoratori in cassa integrazione
Portale unico reclutamento personale PA	€20 milioni	• Nuova piattaforma digitale per centralizzare le procedure di assunzione nella PA e favorire la meritocrazia e la competenza
		• Raccogliere in un unico punto le informazioni riguardanti le competenze dei dipendenti della PA in servizio, semplificando la gestione e la pianificazione delle risorse umane a disposizione
		• La misura è già stata portata totalmente a compimento
Miglioramento delle competenze e della capacità amministrativa della PA	€490 milioni	• Mettere a disposizione dei lavoratori della PA un'ampia offerta di corsi online (almeno 100) per il *reskilling* e *upskilling* delle competenze
		• Promuovere la diffusione delle best practice all'interno delle PA, attraverso l'introduzione di 20 comunità di competenze
		• Introduzione di voucher formativi per il *retraining* del personale per l'aggiornamento delle competenze digitali
Revisione della normativa e delle procedure per il reclutamento dei dipendenti pubblici	Riforma	• Miglioramento della normativa e delle procedure per il reclutamento dei dipendenti pubblici, rendendole più veloci ed efficaci
		• Differenziazione delle modalità di selezione coerentemente con i profili da assumere
		• Revisione degli strumenti per l'analisi dei fabbisogni di competenze delle Pubbliche Amministrazioni
		• Istituire programmi specificatamente dedicati al reclutamento di profili specialistici e di giovani con un elevato livello di qualifiche

La modernizzazione della PA richiede anche una selezione efficiente del personale, basata sulla meritocrazia e sulla competenza. A questo scopo, sono stati destinati €20 milioni per la creazione di un portale unico di reclutamento, una piattaforma digitale che centralizza le procedure di assunzione nella PA. I profili e i curricula dei candidati saranno disponibili direttamente sulla piattaforma, accelerando le fasi di "preselezione" preliminari alla selezione vera e propria. L'obiettivo entro il 2023 è di avere l'80% dei dati di tutte le amministrazioni sulla piattaforma. Questo investimento sarà accompagnato da riforme mirate a migliorare e velocizzare le procedure di reclutamento dei dipendenti pubblici, adattandole ai profili da assumere e rivedendo gli strumenti per l'analisi delle competenze necessarie nelle Pubbliche Amministrazioni. Inoltre, oltre ai corsi di reclutamento standard, saranno istituiti programmi dedicati al reclutamento di profili specialistici e giovani con elevate qualifiche.
Ciò detto, nel a settembre 2020, la Commissione ha proposto un nuovo piano d'azione per l'istruzione digitale per il periodo 2021-2027 che mira a incentivare l'adeguamento sostenibile ed efficace dei sistemi di istruzione e formazione degli Stati membri dell'UE all'era digitale. A tal fine, il piano d'azione definisce due settori prioritari: la promozione dello sviluppo di un ecosistema altamente efficiente di istruzione digitale ed il miglioramento delle competenze e le abilità digitali per la trasformazione digitale. Il primo ruota intorno alla disponibilità di infrastrutture, connettività ed apparecchiature digitali, piattaforme sicure e rispettose della e-privacy, insegnanti e personale competenti sulle tecnologie digitali, mentre il secondo richiede, da un lato, sviluppo di capacità e competenze digitali di base sin dall'infanzia ed alfabetizzazione digitale e, dall'altro, la messa in atto azioni che consentano una buona conoscenza e comprensione delle tecnologie ad alta intensità di dati, oltre all'acquisizione di competenze digitali avanzate e all'accesso delle donne alle carriere digitali.
L'assoluta centralità assunta dalle competenze ha trovato piena esplicazione anche nella Comunicazione "**Bussola per il digitale 2030: il modello europeo per il decennio digitale**" del 9 marzo 2021, **nella quale la Commissione europea ha presentato una visione e prospettive per la trasformazione digitale dell'Europa** entro il 2030, proponendo una bussola digitale che si sviluppa intorno a quattro punti cardinali. Tra questi, insieme a infrastrutture, imprese e servizi pubblici, uno è costituito proprio dalle competenze, rispetto alle quali l'obiettivo proposto per il 2030 consiste nel diffondere competenze digitali di base presso l'80% di tutti gli adulti e raggiungere quota 20 milioni di specialisti ICT impiegati nell'UE, con una crescente convergenza tra uomini e donne.
Il 26 gennaio 2022 è stata inoltre adottata la "European Declaration on Digital Rights and Principles for the Digital Decade", iniziativa straordinariamente rilevante che, partendo dalla constatazione dell'impatto della trasformazione digitale su ogni aspetto della vita quotidiana, delle grandi opportunità di crescita ed innovazione (anche in termini di sostenibilità) e delle nuove sfide che ad essa si accompagnano, declina una serie di diritti e di principi che assumono particolare rilevanza nel contesto della trasformazione digitale, definisce le modalità attraverso le quali essi dovrebbero trovare applicazione nel mondo online ed individua una serie di impegni tesi a garantirne la salvaguardia e la valorizzazione. In particolare, nel secondo dei sei capitoli di cui si compone la dichiarazione si affermano i principi di solidarietà ed inclusione, riconoscendo il diritto di ogni persona all'istruzione, alla formazione ed all'apprendimento permanente e ad acquisire tutte le competenze digitali di base e avanzate.

CONCLUSIONI E SPUNTI DI POLICY

La competizione globale si gioca in buona misura sulla capacità dei singoli paesi di sviluppare, offrire ed applicare i sempre più complessi servizi che le nuove tecnologie e le reti di ultima generazione supportano. Si tratta di una sfida, dunque, quella della digitalizzazione, alla quale nessun continente e nessuna singola realtà nazionale può sottrarsi, pena l'impossibilità di cogliere le straordinarie opportunità che il presente ed un futuro ormai sempre più vicino ci offre.

Ci si riferisce, in particolare, a tutto il fermento legato all'intelligenza artificiale. L'**intelligenza artificiale (IA)** è sicuramente una delle più strabilianti frontiere tecnologiche dei tempi odierni e i suoi ambiti applicativi sono davvero innumerevoli e spaziano dal campo della sanità a quello dell'Internet of Things, dal campo del fintech e dell'insurtech, fino a quello della privacy e della sicurezza informatica, con impatti importanti sulle attività di imprese e pubbliche amministrazioni, oltre che sulla vita delle persone. **L'indagine realizzata da Bytek e I-Com** e che prende in considerazione cinque Paesi (**Italia**, **Stati Uniti**, **Francia**, **Germania** e **Spagna**) **ha avuto l'obiettivo di comprendere quanto sia centrale**, oggi, **il tema dell'intelligenza artificiale** soprattutto in un momento storico, come quello attuale, in cui il lancio di ChatGPT di Open AI e poi di altri prodotti hanno acceso i riflettori su questa famiglia di tecnologie e influenzato la percezione degli individui. Ciò che è emerso è uno spiccato interesse per l'argomento, trainato anche dall'avvento dell'intelligenza artificiale generativa, che si concentra da un lato sulle opportunità lavorative e di investimento che l'IA può offrire e, dall'altro, sui rischi e le paure legate all'impatto dell'IA sul mondo del lavoro ma anche per la tenuta dei sistemi democratici.

A spiccare però è anche **il ritardo dell'Unione europea rispetto alla nuova frontiera tecnologica**, presidiata in primis dagli Stati Uniti e in seconda fila dalla Cina e poi a seguire da Paesi extra-UE come Canada, Regno Unito e Israele. Dei due pilastri della strategia UE del 2018, investimenti e regole, si è proceduti con decisione sul secondo fronte mentre il primo, nonostante gli incrementi registrati, ha segnato il passo rispetto alle enormi risorse messe in campo in particolare dagli USA. In tutto questo, contrariamente alla stragrande maggioranza degli Stati membri UE, **l'Italia non si è ancora dotata di una vera e propria strategia IA**, che per essere definita tale deve disporre di un adeguato orizzonte temporale e spaziale, risorse proprie nonché un meccanismo di governance che ne governi e monitori l'attuazione. Nulla di tutto questo si può ascrivere al Piano strategico licenziato alla fine del 2021 dal Governo Draghi. Appare dunque ora di porre rimedio dotando finalmente il Paese di una vera e propria strategia IA.

D'altra parte, l'IA è senza dubbio una delle tecnologie in grado di aprire le porte a mondi nuovi ed il dibattito sul metaverso ne è una dimostrazione. Nell'ultimo biennio, ed in particolare da quando Facebook nel 2021 ha cambiato la propria denominazione in Meta, **l'attenzione sulla tematica del metaverso è cresciuta in maniera notevole.** Nonostante tale accelerazione, ad oggi, **i suoi confini non appaiono ben definiti** né agli occhi della maggioranza dei consumatori, né tantomeno agli stessi addetti ai lavori. L'esistenza di più di 40 ecosistemi che vengono assimilati alla parola metaverso, peraltro con caratteristiche tecniche molto diverse tra loro, restituisce l'idea di **un panorama ancora estremamente frammentato e in costante evoluzione**.

Il fatto che non vi sia ancora una chiara idea di come sarà strutturato il metaverso nel prossimo futuro non sta frenando però l'interesse delle imprese, che **stanno investendo notevoli risorse per sfruttare le opportunità scaturite da questo nuovo ecosistema digitale**.

Tale interesse è certificato, oltre che dalle previsioni ampiamente illustrate nel documento, da una stima della Commissione Europea pubblicata l'11 luglio 2023 nell'abito della comunicazione sul **"Web 4.0 e i mondi virtuali"** in cui si prevede che **il mercato del metaverso raggiunga gli 800 miliardi di euro entro il 2030**. **L'avvento del metaverso avrà ricadute importanti anche dal punto di vista occupazionale**: infatti, secondo l'UE, grazie anche all'impatto della realtà virtuale e aumentata porterà alla **creazione di 860 mila posti di lavoro entro il 2025 solo in Europa**. Nell'ottica della Commissione il metaverso potrà rappresentare una inestimabile opportunità di crescita per numerosi settori economici, come la Salute, l'Educazione, l'Industria, l'arte e soprattutto la transizione verde (ad esempio permettendo lo sviluppo di modelli 3D che permettono di prevedere l'impatto dei cambiamenti climatici).

Il metaverso, in virtù delle sue caratteristiche e funzioni, impatterà notevolmente su differenti aree del diritto, ponendo queste ultime dinanzi a nuove sfide. In primis, sarà coinvolta la **tutela dei dati personali**, in quanto essi costituiscono una risorsa indispensabile per una *user experience* pienamente soddisfacente. Difatti, facendo riferimento alla disciplina delineata nel GDPR, è inevitabile tener conto delle complesse questioni che tale tecnologia pone rispetto alla difficoltà di definire a priori le finalità di trattamento, nel conciliare il principio di minimizzazione dei dati con i sistemi di IA e nella raccolta di un consenso esplicito. Anche il tema dell'**identità digitale** sarà un aspetto fondamentale e in virtù di ciò sarà cruciale valutare gli effetti della proposta di Regolamento **eIDAS 2.0**. Inoltre, avranno rilievo le riflessioni in termini di protezione della proprietà intellettuale, in particolar modo per i contenuti *user-generated*, come gli NFT e, allo stesso modo, sarà di primaria importanza comprendere le implicazioni dei sistemi di IA nel metaverso, soprattutto se ad alto rischio, valutando quindi se l'**AI Act** potrà essere considerato sufficiente in tal senso. Per di più, nel metaverso assumeranno rilevanza le norme stabilite dal **DMA**, per cui una delle sfide principali in tema riguarderà la necessità per i *gatekeepers* di garantire l'effettiva portabilità dei dati personali dell'utente, ivi inclusi quelli da esso generati, oltre che l'accesso continuo in tempo reale agli stessi dati. Ulteriore disciplina potrà rivedersi nel **DSA**, che ha introdotto un'ampia gamma di obblighi di trasparenza, organizzativi e procedurali, i quali andranno opportunamente declinati rispetto alle peculiarità del metaverso. Peraltro, gli anni che precedono una più ampia evoluzione e diffusione del metaverso saranno indubbiamente preziosi per testare il quadro normativo eurounitario in materia di cybersicurezza, in particolare per valutare, una volta applicabile, la proposta di **Cyber-Resilience Act**, che risulterà indispensabile per proteggere i numerosi dispositivi e sensori alla base dei mondi virtuali di domani, nonché l'eventuale necessità di ulteriori regolamentazioni settoriali, così come si è iniziato a fare con il **Regolamento DORA**. L'11 luglio scorso, la Commissione europea ha presentato la **prima strategia sul Web 4.0 e i mondi virtuali** per sostenere la futura transizione tecnologica nel rispetto dei principi di diritto. In particolare, essa evidenzia la possibile crescita del mercato globale dei mondi virtuali, che da 27 miliardi di euro registrati nel 2022 potrebbe raggiungere oltre 800 miliardi entro il 2030, offrendo in considerevoli settori circa 860.000 nuove occupazioni lavorative. La scelta di prevedere una strategia sui mondi virtuali, incluso il metaverso, risulta coerente con la necessità di porre delle regole anticipate nella gestione di un'esperienza virtuale piena di opportunità e rischi, e, per altro verso, con l'esigenza di non ricadere in una tutela normativa rigida che intervenga *ex ante*, nell'attesa di valutare i futuri riscontri dell'espansione del metaverso.

L'effettiva capacità di tali sistemi di vivere ed alimentarsi poggia **sull'ampia e diffusa disponibilità di infrastrutture di TLC fisse e mobili performanti**. Dato l'obiettivo di copertura in reti VHCN al 2030 (100%) sebbene i progressi registrati, l'UE e l'Italia hanno

ancora molta strada da percorrere sia rispetto alla copertura che con riguardo al take up delle reti di ultima generazione. Secondo il Digital Decade report 2023 riferito a dati del 2022, infatti, la copertura VHCN a livello UE si è attestata al 73%, percentuale che scende al 54% nel territorio nazionale, mentre la copertura FTTP europea è sostanzialmente in linea con quella nazionale (56% a livello UE, 54 % in Italia).

Se si guarda al take up, la **percentuale di abbonamenti ad almeno 100 Mbps sul totale di abbonamenti alla rete fissa**, la performance europea rivela ampi margini di miglioramento, con una percentuale del 55% (l'Italia si allinea quasi al dato europeo con una percentuale del 60%). Al contrario per le tecnologie VHC, secondo la metodologia Europea, l'Italia risulta avere dei valori non dissimili da quelli Europei. Il take up delle reti VHC è del 13,8% in Europa e del 13,4% in Italia. Si osserva, inoltre, che altre analisi del settore riportano valori differenti, secondo i quali il take up italiano si attesta al 22%, mentre quello europeo intorno al 53%[52], facendo comunque emergere una situazione in cui risulterà complesso raggiungere gli obiettivi di connettività stabiliti.

In ogni caso, tali dati, dimostrano come sarebbero auspicabili misure nazionali e comunitarie di sostegno alla domanda, quali voucher per l'attivazione dei servizi più performanti e l'adozione di piani di switch off delle vecchie tecnologie.

Lato 5G, nonostante i dati dimostrino una forte accelerazione del continente europeo e dell'Italia, con una percentuale di copertura che è passata a livello europeo dal 14% del 2020 al 81,2% in termini di famiglie raggiunte, ed in Italia dall'8% del 2020 a ben il 99,7% del 2022, risultando al quarto posto in Europa, non può non segnalarsi come tali risultati siano in buona misura frutto della **condivisione dinamica dello spettro (DSS)** che consente agli operatori telefonici di usare lo spettro di frequenze del 4G anche per il 5G e che quindi buona parte delle reti 5G sono ancora non stand-alone.

È certo dunque che serve un cambio di passo per poter competere con le aree del mondo più digitalizzate, prime tra tutte USA e Cina, e le istituzioni europee ne sono consapevoli tanto da aver recentemente lanciato un pacchetto, il Connectivity Package, con il quale da un lato si cerca di accelerare lo sviluppo delle reti attraverso la definizione di un set armonizzato di regole, procedure e tempistiche e, dall'altro, si cerca di individuare le tendenze e gli investimenti realizzati e pianificati per adottare eventuali azioni. Sul punto è evidente il beneficio derivante dall'armonizzazione del quadro normativo che il **Gigabit Infrastructure Act** potrà assicurare ma è al contempo ineludibile la necessità di assicurare il rispetto delle peculiarità nazionali soprattutto quando, come in Italia, gli interventi di semplificazione che si sono succeduti negli anni, al di là della disomogeneità applicativa su cui è necessario agire, sono riusciti a disegnare un quadro normativo avanzato. Quanto al futuro del settore e al tema della cosiddetta ***fair contribution,*** si tratta di un tema che ha animato un ampio dibattito all'interno della consultazione pubblica conclusasi nel mese di maggio e che ha registrato, invero, molte posizioni contrarie, non solo da parte degli OTT, all'introduzione di tale strumento, imponendo, in sede di valutazione circa l'opportunità di adottare eventuali iniziative legislative in materia, l'attenta analisi di tutti gli argomenti in campo e, dunque, considerazioni economiche, tecniche e di neutralità della rete oltre ai possibili impatti sul mercato dei contenuti e sugli investimenti che tale strumento potrebbe comportare così da trovare un equo contemperamento degli interessi coinvolti all'insegna dell'innovazione e della crescita dell'UE.

Se si guarda al contesto italiano, attraverso il Piano BUL

52 I dati si riferiscono al market panorama elaborato dall'FTTH Council in collaborazione con IDATE. La discrasia sembra essere dovuta alle differenti metodologie usate. Infatti, la Commissione europea calcola il take-up sul totale delle famiglie, mentre l'FTTH Council calcola il take-up sulla base del totale delle linee VHC attive.

e i successivi Piani Italia a 1 Giga e Italia 5G sono state stanziate risorse ingenti per favorire lo sviluppo delle infrastrutture di TLC fisse e mobili nel nostro paese. Ciò nonostante sono ancora molte le criticità legate alla complessità delle procedure autorizzative, alla difficoltà di reperire manodopera specializzata e di individuare spazi idonei alla realizzazione degli impianti che mettono a rischio il raggiungimento degli obiettivi di copertura fissati al 2026 esigendo la messa in campo di correttivi. In tale logica e al fine specifico di superare i gap attualmente presenti lungo la "catena del valore" della BUL, ovvero degli interventi attualmente in essere per la creazione e diffusione delle reti ad altissima capacità in Italia, l'estate appena trascorsa ha visto nascere la **Strategia italiana per la Banda Ultra Larga 2023-2026** che ha declinato un insieme di azioni tese a traguardare gli obiettivi fissati al 2026. Si tratta di una articolata serie di misure ed iniziative, alcune solo annunciate e dunque da definire nei concreti meccanismi di azione (vedi ad esempio le misure a sostegno della domanda), che cercano di offrire soluzioni idonee a ridurre e sostenere gli investimenti degli operatori (si pensi alle risorse stanziate per la creazione di una rete Edge Cloud Computing che dovrebbe garantire migliore qualità dei servizi applicativi e significativi risparmi fino al 60% per le telco), a semplificare le complessità concretamente registrate negli *iter* realizzativi delle reti fisse e mobili e a creare anche nuove opportunità di sviluppo (si pensi ad esempio all'iniziativa di realizzare, in collaborazione con Ferrovie dello Stato, un'infrastruttura radio mobile multi operatore 5G di proprietà pubblica con priorità lungo le tratte ad alta velocità o a quella di garantire copertura e connettività mobili – 4G e/o 5G – lungo la rete stradale, incluse le tratte in galleria, per tutte le linee di comunicazione principali verso le sedi di svolgimento degli eventi olimpici relativi a "Milano – Cortina 2026"). Si tratta certamente di azioni importanti che devono valorizzare le infrastrutture esistenti e prevedere forme di sostegno all'ulteriore sviluppo nel rispetto delle dinamiche di mercato e degli investimenti già compiuti dagli operatori sulle proprie reti, dalle quali sarebbe opportuno partire per poi estendere l'azione su altri ambiti alle stesse collegati come la **gestione dello spettro** che da un lato esige particolare attenzione, in generale, in merito a tematiche di interesse transnazionale quale l'assegnazione di frequenze ai vertical (vedi la Germania) che devono necessariamente tenere conto delle peculiarità nazionali, del mercato e degli investimenti compiuti sulle frequenze oltre che di questioni legate alla sicurezza delle reti in quanto asset di rilevanza strategia cruciale e, dall'altro, richiede ordine e chiarezza rispetto al futuro in particolare con riferimento ad alcune frequenze – si pensi alla banda 26 GHz, fondamentale per offrire connettività fino a 1 Gbps in tecnologia *fixed-wireless*, le cui licenze sono state prorogate fino al 2026 – rispetto alle quali non c'è possibilità, allo stato attuale, di pianificare gli investimenti e gli usi.

A ciò si aggiunge, sicuramente, l'annosa ed ancora irrisolta questione dell'innalzamento dei **limiti elettromagnetici**. È fuor di dubbio, infatti, che in mancanza di evidenze scientifiche, la vigenza di limiti così ingiustificatamente restrittivi rappresenti un vulnus importante per il nostro paese e per le aziende chiamate a realizzare impianti in un contesto generale che vede aumentare i costi di materie prime ed energia, che registra crescenti difficoltà di individuazione di spazi idonei ad accogliere gli impianti e che impone interventi sostenibili e rispettosi dell'ambiente e del paesaggio. Si tratta di un ostacolo rilevante che ostacola e rallenta lo sviluppo delle reti con evidente impatto non solo sulle imprese che realizzano reti, ma anche su tutte le imprese che tardano ad avere la possibilità di accedere a tali reti e alle opportunità che le stesse offrono in termini di innovazione e competitività. In un contesto generale così complesso è senza dubbio importante il contributo che può offrire l'FWA, per la sua capacità di garantire l'accesso ultraveloce – soprattutto se capace di raggiungere prestazioni fino ad 1 Gbps

grazie alle onde millimetriche e all'utilizzo del 5G in ambito fisso – anche nelle aree più remote del Paese in tempi più rapidi e a costi più contenuti – in particolare quelle che è più complicato e costoso coprire con fibra fino alle abitazioni.

Un passo avanti andrebbe fatto anche sul versante degli **stimoli alla domanda**, che, come evidenziato dai dati presenti nel rapporto, ad oggi non hanno avuto un effetto rilevante nel guidare individui e imprese verso la connettività di ultima generazione. A tale riguardo, è certamente indispensabile, con un percorso graduale che non produca shock di mercato o gravi impatti occupazionali, favorire lo switch-off del rame e dunque il passaggio verso le migliori tecnologie disponibili nelle singole aree del paese. Lato imprese, sarebbe senza dubbio opportuno, in sede di legge di bilancio, definire, come annunciato nei mesi scorsi, il Piano Transizione 5.0 inserendo specifiche forme di sostegno ed incentivazione per la connettività. È sempre più chiaro, infatti, che l'acquisto di macchinari e tecnologie di ultimissima generazione senza la disponibilità di reti performanti, come ad esempio reti 5G private, appare fortemente depotenziato in termini di opportunità per le imprese.

Se si resta sul mondo delle imprese, nell'ambito della **Strategia 2030** l'UE mira al raggiungimento di un livello di intensità almeno di base nel 90% delle PMI e all'adozione di servizi di big data, cloud computing e intelligenza artificiale in almeno il 75% delle imprese entro il 2030. Ebbene, il rapporto annuale sullo stato del Decennio Digitale pubblicato a settembre 2023 sottolinea che, in assenza di **ulteriori investimenti**, la traiettoria prevista non consentirebbe di raggiungere tali obiettivi entro il 2030 ponendo all'attenzione delle istituzioni europee e dei singoli Stati membri la necessità, ineludibile, di favorire ed accelerare il percorso di digitalizzazione delle imprese.

Al ritardo nel processo di transizione digitale si aggiunge anche una carenza di **investimenti delle imprese in cybersecurity**. Ed infatti, nonostante il continente europeo si posizioni nelle prime tre posizioni per distribuzione geografica degli attacchi informatici sia nel 2021 che nel 2022 (in quest'ultimo periodo in crescita del 3% rispetto all'anno precedente), gli OSE/DSP hanno destinato mediamente una percentuale inferiore del proprio budget IT alla cybersicurezza nel 2021 (-1% su base annua). Sarà pertanto indispensabile comprendere se, sulla base del prossimo report "*NIS Investments*" di ENISA riferito al 2022, si sia trattato di un caso isolato, oppure dell'inizio di un trend in negativo a cui prestare prontamente maggiore attenzione, al fine di porvi rimedio anche, ma non solo, con diverse e opportune forme di incentivo e finanziamento. Se si considera però che l'aver subito una violazione dei dati ha rappresentato il penultimo motivo per un incremento degli investimenti dedicati alla cybersecurity, con un mero 7,7% delle risorse allocate, è ragionevole presumere che sia diffusa un'insufficiente consapevolezza circa gli effetti meno visibili, soprattutto nel breve-medio termine, degli attacchi cibernetici e derivanti dall'esfiltrazione e successiva diffusione illecita di informazioni (riconducibili, ad esempio, ad asset aziendali o a dati personali dei clienti, il cui utilizzo improprio da parte di attori malevoli può produrre importanti pregiudizi per le attività di business delle imprese), con conseguente necessità di un rapido ed efficace intervento correttivo.

Allo stesso tempo, **oltre ad investire di più, il settore privato deve investire bene.** Per questo lo Stato dovrebbe incoraggiare con voucher e altre misure **audit 4.0 (o a questo punto 5.0)** forniti da soggetti specializzati a imprese piccole e micro la valutazione del proprio stato tecnologico e degli investimenti prioritari per migliorarlo dato lo stato di partenza e il contesto di mercato di riferimento. In questo modo, peraltro, si indirizzerebbero le imprese, soprattutto quelle meno attrezzate a prendere decisioni di investimento sulle tecnologie, a usare al meglio le risorse pubbliche, migliorando il ritorno per i denari spesi dallo Stato (e altri attori istituzionali).

Se il mondo business necessita di specifiche azioni incentivanti ed acceleranti il processo di digitalizzazione e gli investimenti in cybersecurity, per quanto riguarda la **digitalizzazione della pubblica amministrazione**, la situazione nel complesso risulta **favorevole** e molti Stati membri si trovano in condizione tale da poter raggiungere gli obiettivi di digitalizzazione previsti dalla Strategia 2030. Tuttavia, soprattutto in Italia, la strada da percorrere in tema di trasparenza dei processi, coinvolgimento degli utenti nella progettazione dei servizi e gestione da parte di questi ultimi dei propri dati personali è ancora lunga e, come evidenzia anche la Commissione Europea, vi è necessità di migliorare le prestazioni dei servizi e garantire una maggiore disponibilità in Europa **di servizi pubblici transfrontalieri**.

Decisamente preoccupante appare invece la situazione lato competenze digitali, cruciali per la transizione digitale. Rispetto a tale indicatore, **l'Italia conquista gli ultimi posti delle classifiche europee** (per competenze digitali avanzate è penultima). Nella pubblica amministrazione vi sono molte differenze a seconda del tipo di pubblica amministrazione, con i comuni che risultano quelli che trovano più difficoltà a formare il proprio personale, o a seconda della provenienza geografica. Non a caso **la mancanza di formazione è il maggiore ostacolo fronteggiato dalle PA**. Anche per le **imprese** la formazione risulta uno degli aspetti critici, come testimoniano le rilevazioni statistiche che documentano una percentuale minore della media europea di quelle che erogano corsi per formare il proprio personale. Dai dati emerge anche che **nel quinquennio 2023-2027 ci sarà una mancanza di laureati in materie STEM e economico-statistiche**.

Tenendo conto dell'analisi dei dati forniti da Eurostat con riferimento all'anno 2022, il quadro italiano in tema di **competenze in cybersecurity** appare particolarmente critico. Ciò però non scoraggia l'utilizzo che gli utenti fanno della rete, basti pensare al fatto che solo il 59,8% dei cittadini ha competenze almeno basilari in materia di sicurezza informatica, nonostante la percentuale di impiego di Internet sia pari all'86,1%, ben superiore di 26,3 p.p. Una simile condizione aumenta i rischi relativi alla possibilità che soggetti malevoli attacchino gli utenti mediante frodi online, esperite tramite tecniche di persuasione e convincimento. Proprio al fine di ridurre tali pericoli è necessario puntare sull'aumento del livello di consapevolezza e competenza in cybersecurity dei cittadini. Le iniziative nazionali sul punto hanno interessato particolarmente la **formazione superiore**, dunque competenze specialistiche, sia in ambito universitario che in merito agli ITS. Ciò denota un aumento della sensibilità in merito al tema della sicurezza informatica che nell'anno accademico 2022/2023 è divenuto oggetto di ben **271 corsi di formazione universitaria** e ha interessato il **14% degli ITS** diffusi sul territorio nazionale rispetto al numero complessivo di quelli attivi.

Le variegate dinamiche che caratterizzano la transizione digitale italiana trovano conferma nelle risultanze **dell'IBI, l'I-Com Ultrabroadband Index,** giunto alla decima edizione, che fotografa lo sviluppo delle reti e dei servizi digitali nei mercati nazionali europei, dal quale emerge come l'Italia abbia risalito ben 9 posizioni dal 2021 al 2023 piazzandosi nell'ultima rilevazione al sedicesimo posto. Si tratta di un risultato riconducibile a molteplici fattori, tra i quali risulta determinante l'imponente crescita della copertura 5G, che dall'8% delle aree popolate e dallo 0% rurale nel 2020 passa al 100% nel 2022 (sempre con la precisazione che il dato non distingue copertura 5G stand alone e non stand alone) e dalla buona performance nel campo dell'e-government, dove il 40% degli italiani ha interagito con la PA via web. Un avanzamento considerevole riguarda anche la diffusione delle reti fisse, indicate dalla copertura VHCN e FTTP a livello rurale, che passa dall'8% al 26% in entrambi i casi, a testimonianza dell'evoluzione, seppur con tutte le difficoltà indicate, dei piani di cablatura dei numeri civici nelle aree grigie e bianche.

Si evidenzia inoltre che la presente pubblicazione contiene informazioni
di carattere generale. Prima di prendere decisioni o adottare iniziative che possano incidere
sui risultati aziendali, si consiglia di rivolgersi a un consulente
per un parere professionale qualificato. L'Istituto per la Competitività
è da ritenersi non responsabile per eventuali perdite subite da chiunque utilizzi
o faccia affidamento su questa pubblicazione.

Crediti fotografici:
Copertina – DilokKlaisataporn/shutterstock.com

Impaginazione:
kreas.it

icom
reti & servizi di nuova generazione

Roma
Piazza dei Santi Apostoli 66 - 00187
www.i-com.it

Bruxelles
Avenue des Arts 50 - 1000
www.i-comEU.eu

info@i-com.it