NOVEMBRE 2023

# MISURARE IL BENESSERE DIGITALE

Alessandra Bucci, Silvia Compagnucci, Alessandro D'Amato, Enrica Lipilini, Domenico Salerno, Valerio Vinco

*La digitalizzazione sta trasformando in maniera radicale le abitudini quotidiane degli individui aprendo ad un mondo di nuove opportunità per gli individui sia nella sfera ludica che professionale. Lo spostamento della maggior parte delle attività umane sul web, oltre agli innumerevoli effetti positivi, porta con sé una nuova gamma di rischi derivanti sia dai cybercriminali che da un utilizzo problematico degli strumenti digitali.*

- La transizione digitale e la conseguente migrazione sul web di una gamma di servizi sempre più ampia stanno gradualmente ridisegnando le abitudini di individui, abilitando nuovi canali relazionali e creando opportunità di business innovative. Nell'arco di poco più di un decennio è significativamente cresciuta la quota di italiani che utilizzano internet tutti i giorni, passata dal 50,9% del 2012 all'82% del 2022.
- Un elemento fondamentale per garantire il benessere degli utenti che navigano in Internet è un'adeguata dotazione di competenze digitali. Nonostante ciò, gli ultimi dati diffusi da Eurostat mostrano in questo ambito un'arretratezza generalizzata da parte dell'Italia, che si posiziona al quartultimo posto in UE per quota di popolazione (46%) in possesso di skill digitali almeno basilari.
- Tra i rischi legati all'uso di Internet, riveste un ruolo preminente l'*hate speech*, che è divenuto oggetto di attenzione delle principali piattaforme digitali, le quali si impegnano a rimuovere tutti i video, le immagini, i post con finalità di istigazione, prevedendo anche procedure di ripristino in caso di erronea valutazione dell'inadeguatezza del contenuto.
- Il monitoraggio su bullismo e cyberbullismo effettuato dal Miur a maggio 2022 evidenzia che il 7,9% degli studenti e delle studentesse partecipanti ha dichiarato di aver subito episodi di cyberbullismo (6,6% occasionalmente e 1,3% sistematicamente), mentre il 7,4% afferma di aver esperito attivamente tali condotte.
- A novembre 2023 I-Com ha effettuato un'indagine volta a comprendere il grado di consapevolezza degli studenti italiani rispetto ai principali rischi collegati all'utilizzo degli strumenti informatici, nonché sulle possibili iniziative utili a potenziare conoscenze e competenze necessarie ad affrontare le sfide dell'ecosistema digitale.

# SOMMARIO

# EXECUTIVE SUMMARY

La transizione digitale e la conseguente migrazione sul web di una gamma di servizi sempre più ampia stanno gradualmente ridisegnando le abitudini di individui, abilitando nuovi canali relazionali e creando opportunità di business innovative. Nell'arco di poco più di un decennio è significativamente cresciuta la quota di italiani che utilizzano internet tutti i giorni, passando dal 50,9% del 2012 all'82% del 2022. Tale dato dimostra chiaramente l'estrema pervasività che i canali digitali hanno raggiunto nelle nostre attività quotidiane.

*Nell'arco di poco più di un decennio è significativamente cresciuta la quota di italiani che utilizzano internet tutti i giorni, passando dal 50,9% del 2012 all'82% del 2022*

Non è solo la frequenza con cui gli individui accedono al web a crescere ma anche il ventaglio di attività che questi svolgono sulla rete. Ormai, ogni giorno nascono nuovi servizi e opportunità online che, grazie alla cassa di risonanza rappresentata dai social media, riescono ad affermarsi a livello globale in brevissimo tempo. Tra il 2016 e il 2022 la quota di italiani che utilizza la rete per fruire di contenuti video on demand tramite piattaforme di streaming è quadruplicata, raggiungendo il 41% nel 2022. Sempre nell'ambito dell'intrattenimento, in Italia è cresciuta anche la quota di individui che utilizza internet per giocare o scaricare videogiochi, passata dal 21% al 28%.

La connettività digitale non ha vissuto un andamento crescente solo relativamente alle finalità ludiche, ad esempio 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.

*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*

La crescita dirompente dei canali digitali ha riguardato anche le tipologie di dispositivi tramite i quali gli individui fruiscono di servizi connessi, andando così a ridefinire il nostro modo di interagire con la tecnologia nella quotidianità. Dagli ultimi dati diffusi da We Are Social, emerge come al 2022 quasi la totalità della popolazione tra italiana tra i 16 e i 64 anni accede ad internet tramite smartphone (97,5%), circa il 30% in più rispetto a chi utilizza abitualmente un PC (62,2%). Particolarmente rilevante è anche la quota di individui che utilizzano altri tipi di device connessi, come le console da gaming (35,9%), gli smartwatch (33,2%), le smart TV (22,6%) e i dispositivi di smart home (20,5%). Nonostante rappresenti ancora una percentuale residuale (4,5%), è in forte

aumento anche la quota di italiani che usa device di realtà virtuale che, infatti, tra il 2021 e il 2022 ha sperimentato una crescita anno su anno di oltre il 60%.

Infine, la digitalizzazione ha modificato radicalmente anche sia le modalità con cui gli italiani gestiscono e spendono i propri soldi. Tra il 2015 e il 2022 la quota di italiani che ha effettuato almeno un acquisto online nel corso dell'anno è raddoppiata (passando dal 26,4% al 49,3%), mettendo in luce una dinamica simile a quella dell'internet banking che ha raggiunto un tasso di penetrazione pari al 48,4%.

*Tra il 2015 e il 2022 la quota di italiani che ha effettuato almeno un acquisto online nel corso dell'anno è raddoppiata (passando dal 26,4% al 49,3%), mettendo in luce una dinamica simile a quella dell'internet banking che ha raggiunto un tasso di penetrazione pari al 48,4%*

Un altro elemento fondamentale per garantire il benessere degli utenti che navigano in Internet è un'adeguata dotazione di competenze digitali. Rispetto alla quale, purtroppo, anche gli ultimi dati diffusi da Eurostat mostrano un'arretratezza generalizzata da parte dell'Italia, che si posiziona al quartultimo posto in UE per quota di popolazione (46%) in possesso di skill digitali almeno basilari. Inoltre, un'analisi di Istat relativa al 2021, evidenzia un cambiamento di tendenza in merito 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. Tali differenze si evincono anche in merito ad altri fattori socio-culturali come il livello di istruzione e la condizione occupazionale degli individui. Peraltro, le competenze digitali possono essere suddivise in cinque diverse dimensioni: comunicazione e collaborazione; alfabetizzazione su informazioni e dati; risoluzione di problemi; capacità di creare contenuti digitali; abilità di sicurezza. Utilizzando questa classificazione, è possibile tracciare una mappa dei punti di forza e delle carenze nei livelli di preparazione dei cittadini italiani rispetto al panorama europeo.

*Gli ultimi dati diffusi da Eurostat mostrano un'arretratezza generalizzata in ambito competenze digitali da parte dell'Italia, che si posiziona al quartultimo posto in UE per quota di popolazione (46%) in possesso di skill almeno basilari*

La transizione ecologica e la transizione digitale sono parallele e interconnesse. Secondo la *Global e-Sustainability Initiative* (GESI) l'implementazione delle tecnologie digitali può accelerare i progressi verso gli SDGs del 22%. Le reti di ultima generazione come la fibra ed il 5G hanno il potenziale per colmare il divario digitale consentendo l'accesso all'istruzione a distanza, ai servizi finanziari e migliorando la telemedicina e il lavoro flessibile.

*Secondo la Global e-Sustainability Initiative (GESI) l'implementazione delle tecnologie digitali può accelerare i progressi verso gli SDGs del 22%*

L'*Internet of Things* (IoT) e i device mobili stanno rivoluzionando il monitoraggio ambientale, in quanto, attraverso la raccolta di dati in tempo reale da sensori posizionati in tutto il mondo, le imprese e le istituzioni possono tracciare e gestire risorse in modo più efficiente, comprese quelle energetiche e rinnovabili. Inoltre, nel 2021 si è verificato un notevole aumento dell'uso dei cellulari per l'accesso a informazioni educative, coinvolgendo 2,5 miliardi di persone (pari al 48% degli abbonati di telefonia mobile). A loro volta anche le applicazioni sanitarie mobili e i social media stanno vivendo una crescita esponenziale e un impatto rilevante sulla sostenibilità.

*L'Internet of Things (IoT) e i device mobili stanno rivoluzionando il monitoraggio ambientale, in quanto, attraverso la raccolta di dati in tempo reale da sensori posizionati in tutto il mondo, le imprese e le istituzioni possono tracciare e gestire risorse in modo più efficiente, comprese quelle energetiche e rinnovabili*

Oggigiorno, Internet e le nuove tecnologie sono fonte di innumerevoli opportunità, ma possono anche celare rischi significativi per gli individui. L'*hate speech* rappresenta una delle problematiche principali, in quanto i social media ne agevolano la diffusione. Il Meta Transparency Center ha mappato le attività condotte dai social network Instagram e Facebook rilevando che nel 2021 Instagram ha rimosso 25,9 milioni di contenuti incitanti all'odio, ossia 9,7 milioni in più rispetto al 2022, mentre nel primo semestre del 2023 tale operazione ha interessato 14,9 milioni di dati presenti sulla piattaforma. Tra questi, dal 2021 fino a giugno del 2023, ne sono stati ripristinati 4,35 milioni. A sua volta Facebook ha rimosso 96,4 milioni di contenuti nel 2021; 50,2 milioni nel 2022 e 28,7 milioni nei primi sei mesi dell'anno in corso, reintegrandone complessivamente 9,58 milioni. Tali operazioni hanno interessato anche YouTube che nel primo semestre del 2023 ha eseguito la rimozione di 369 mila contenuti incitanti all'odio.

L'uso problematico della rete può esplicitarsi mediante il fenomeno del cyberbullismo. Nel primo semestre del 2023 sono state trattate da parte della Polizia Postale 164 denunce in merito, provenienti principalmente da vittime con un'età tra i 14 e i 17 anni, anche se è evidente che solo una piccola frazione degli abusi emerga.

*L'uso problematico della rete può esplicitarsi mediante il fenomeno del cyberbullismo. Nel primo semestre del 2023 sono state trattate da parte della Polizia Postale 164 denunce in merito, provenienti principalmente da vittime con un'età tra i 14 e i 17 anni, anche se è evidente che solo una piccola frazione degli abusi emerga*

Considerato il crescente uso dei social media per scopi informativi e formativi, non va sottovalutato il problema della disinformazione manifestato attraverso la proliferazione di fake news. Il report "*Public opinion in the European Union*" di Eurobarometer evidenzia che il 64% degli italiani dichiara di imbattersi spesso in notizie false, le quali per il 39% del campione sono difficili da identificare, mentre per il 57% non appare complicato riconoscere un atto di disinformazione. Ad accrescere e rafforzare tali fenomeni è sicuramente il divario tra la quota di individui che utilizzano la rete e quella dei soggetti che hanno competenze almeno basilari di sicurezza informatica, in quanto queste ultime sono fondamentali per riconoscere e potersi difendere da attacchi mirati online, tra cui le truffe. Dal dato più recente fornito dalla Polizia Postale, emerge che nel primo semestre del 2023 sono stati registrati nello specifico 7.661 episodi relativi a truffe informatiche, per un valore complessivo di somme sottratte pari a €58,2 milioni.

*Dal dato più recente fornito dalla Polizia Postale, emerge che nel primo semestre del 2023 sono stati registrati nello specifico 7.661 episodi relativi a truffe informatiche, per un valore complessivo di somme sottratte pari a €58,2 milioni*

Altro profilo critico è quello delle dipendenze comportamentali che possono essere provocate sia dai social media che dai videogame. Difatti, il *gaming disorder* coinvolge il 12% degli studenti (circa 480.000), prevalentemente di sesso maschile; diversamente la dipendenza da social media, che tra i soggetti affetti colpisce circa 99.600 studenti, colpisce in particolare il sesso femminile, verificandosi nel 3,1% delle studentesse di 11-13 anni e nel 5,1% della fascia 14-17 anni. Inoltre, accanto a queste risultanze, dallo studio "Dipendenze comportamentali nella Generazione Z" dell'Istituto Superiore di Sanità (ISS), emerge che da detti fenomeni possono nascere disturbi comuni da monitorare attentamente, tra cui rientrano l'ansia sociale, la depressione e il basso rendimento scolastico.

*Il gaming disorder coinvolge il 12% degli studenti (circa 480.000), prevalentemente di sesso maschile; diversamente la dipendenza da social media, che tra i soggetti affetti colpisce circa 99.600 studenti, colpisce in particolare il sesso femminile, verificandosi nel 3,1% delle studentesse di 11-13 anni e nel 5,1% della fascia 14-17 anni*

Al fine di raggiungere il c.d "*digital wellbeing*", a seguito dell'appurata inadeguatezza della Direttiva *e-commerce*, la strategia individuata dall'Unione Europea ha rivisto il passaggio dal ricorso ad atti di *soft law* (tra cui spiccano i codici di condotta) all'adozione di un modello definito di "*public-private cooperation and co-optation*". Il 31 maggio 2016 la Commissione europea ha promosso un Codice di condotta per il contrasto all'illecito incitamento all'*hate speech*, al quale hanno aderito i principali operatori privati di servizi online (tra cui Google, Instagram e Facebook). Inoltre, l'11 ottobre scorso, nell'ambito del gruppo ad alto livello sulla lotta contro l'incitamento all'odio e i crimini d'odio e di intolleranza, sono state discusse le previsioni del prossimo "Codice di Condotta+".

Per quanto concerne la disinformazione, nell'ottobre 2018 i rappresentanti delle piattaforme online, delle principali imprese tecnologiche e degli operatori del settore pubblicitario hanno concordato il Codice di buone pratiche sulla disinformazione. La Commissione europea ha eseguito una valutazione del suo primo periodo di attuazione e, nel maggio 2021, ha pubblicato orientamenti dettagliati per rimediare alle carenze del Codice del 2018, allo scopo di aumentare la sua efficacia. Successivamente, a seguito del processo di revisione avviato nel giugno 2021, è stato firmato, in data 16 giugno 2022, il Codice di Condotta Rafforzato sulla disinformazione.
In merito al contrasto del cyberbullismo, in ambito nazionale la legge 29 maggio 2017, n. 71 ha riconosciuto un sistema di *enforcement* nei confronti delle piattaforme digitali per intervenire prontamente sulla questione. Successivamente, il legislatore italiano ha emanato le "Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo" rivolte ai dirigenti, ai docenti e agli operatori scolastici e, il 6 settembre scorso, la Camera ha approvato il testo unificato delle proposte di legge 536, 891 e 910, intervenendo sulla legge n. 71/2017.

Con la perdita di efficacia delle misure di *soft law*, si è fatta viva la necessità di uniformare il quadro legislativo sui servizi digitali, allo scopo di garantire libertà e sicurezza a chi ne fruisce direttamente. Pertanto, la Commissione europea ha presentato nel dicembre 2020 il *Digital Services package*, ossia due proposte di regolamento inerenti la concorrenza equa dei mercati digitali (*Digital Markets Act*) e il mercato unico dei servizi digitali (*Digital Services Act*).
Il DMA stabilisce norme armonizzate volte a garantire che i mercati nel settore digitale nei quali sono presenti *gatekeeper* (controllori dell'accesso) siano equi e contendibili in tutta l'Unione. Mentre, il DSA impone ai prestatori di servizi di *hosting* di intervenire immediatamente per la rimozione o l'oscuramento di contenuti illeciti appena essi ne siano venuti a conoscenza, prevedendo obblighi di *due diligence* e, al contempo, escludendo obblighi di sorveglianza o accertamento attivo.
Infine, un profilo critico da non sottovalutare è quello inerente l'impego da parte delle piattaforme digitali di dati personali resi pubblici dall'utente e il relativo trattamento automatizzato per scopi di profilazione.

Nel mese di novembre 2023 I-Com avviato un'indagine campionaria volta a comprendere il grado di consapevolezza degli studenti italiani rispetto ai principali rischi collegati all'utilizzo degli strumenti informatici, nonché sulle possibili iniziative utili a potenziare conoscenze e competenze necessarie ad affrontare le sfide dell'ecosistema digitale.

*Nel mese di novembre 2023, I-Com avviato un'indagine campionaria volta a comprendere il grado di consapevolezza degli studenti italiani rispetto ai principali rischi collegati all'utilizzo degli strumenti informatici, nonché sulle possibili iniziative utili a potenziare conoscenze e competenze necessarie ad affrontare le sfide dell'ecosistema digitale*

L'indagine si è articolata su due assi principali: il primo ha previsto la somministrazione di un questionario di 15 domande agli studenti di scuola secondaria e ad universitari, al fine di identificare le loro abitudini di utilizzo degli strumenti digitali e la loro preparazione nel rispondere alle minacce informatiche; il secondo si è sostanziato nella somministrazione di un questionario ai

docenti composto da 8 domande volte a comprendere il grado di consapevolezza dei propri studenti, delle scuole primarie e secondarie, rispetto ai principali rischi collegati all'utilizzo degli strumenti informatici, nonché sul possibile ruolo della scuola e della famiglia nell'acquisizione delle conoscenze e competenze necessarie ad affrontare le sfide dell'ecosistema digitale.

Sul versante degli studenti, in merito alle attività svolte online, osservando le risposte è possibile notare come solo l'1% degli studenti di scuola superiore non utilizza i canali digitali per nessuna finalità, tra gli universitari invece nessuno ha selezionato questa opzione. Tra le attività maggiormente svolte, spiccano i social media (fruiti dall'87% degli studenti di scuola secondaria e del 92% degli universitari) e la ricerca di informazioni (rispettivamente l'75% e il 95%).

Agli studenti delle scuole secondarie è stato inoltre chiesto da quanti anni utilizzassero i social network. Appare particolarmente interessante notare come la maggioranza dei rispondenti (45%) abbia affermato di utilizzare i social da più di 5 anni, quindi con tutta probabilità in un'età precedente al limite legale previsto in Italia di 14 anni (decreto legislativo 101 del 2018).

*Agli studenti delle scuole secondarie è stato inoltre chiesto da quanti anni utilizzassero i social network. Appare particolarmente interessante notare come la maggioranza dei rispondenti (45%) abbia affermato di utilizzare i social da più di 5 anni, quindi con tutta probabilità in un'età precedente al limite legale previsto in Italia fissato a 14 anni*

Sono molto alte le percentuali di coloro che affermano di aver ricevuto una richiesta di informazioni personali, rispettivamente il 50% degli studenti di scuola secondaria e il 59% degli universitari. Considerevoli sono anche le percentuali di studenti che dichiarano di non voler rispondere, il 15% sia di quelli di scuola secondaria che di universitari. Da ciò emerge chiaramente quanto i ragazzi possano essere vulnerabili, se non correttamente informati, tramite queste piattaforme.

Ciò detto, desta preoccupazione anche la quota di coloro che affermano di aver ricevuto messaggi o mail da soggetti malintenzionati, ossia l'80% degli universitari, dato che scende di ben 27 punti percentuali, al 53%, per gli studenti di scuola secondaria, che però in virtù della giovane età possono certamente essere considerati più vulnerabili. Allo stesso tempo è da segnalare come, ancora una volta, l'8% di questi non abbia voluto rispondere.

Dal sondaggio inoltre emerge che, almeno nella percezione degli studenti, vi è una buona diffusione delle informazioni relative a come proteggersi dai pericoli della rete. La quota maggiore di rispondenti afferma infatti di essere abbastanza informato, con una percentuale leggermente maggiore negli studenti di scuola secondaria, il 53% contro il 42% degli universitari. Quest'ultimi, sempre secondo un giudizio personale, sono in media meno informati degli studenti di scuola secondaria, infatti, dice di essere poco informato rispettivamente il 15% e il 5%. Tale dato potrebbe essere condizionato dalla maggiore consapevolezza degli individui anagraficamente più grandi.

Inoltre, in base ai risultati della survey emerge anche che il 52% degli universitari non ha mai ricevuto informazioni su come proteggersi in rete. Di converso, la larga maggioranza degli studenti di scuola secondaria hanno dichiarato di aver ricevuto informazioni a proposito, ben l'79%, contro il 34% degli universitari. Questo potrebbe dimostrare una maggiore sensibilità anche delle istituzioni scolastiche verso tali tematiche che sfocia in una maggiore diffusione di iniziative dedicate a tali tematiche.

*Il 52% degli universitari non ha mai ricevuto informazioni su come proteggersi in rete. Di converso, la larga maggioranza degli studenti di scuola secondaria hanno dichiarato di aver ricevuto informazioni a proposito, ben il 79%, contro il 34% degli universitari*

È da sottolineare anche la diffusione di incertezza sull'adeguatezza dei comportamenti adottati per proteggersi dai pericoli digitali. Infatti, un terzo degli intervistati non riesce a dare una risposta precisa a proposito, mentre un quarto degli stessi crede che questi comportamenti non siano sufficienti. Si palesa un'incertezza diffusa anche riguardo ai soggetti da contattare in caso di problematiche online, come phishing o furto d'identità. Il 36% degli studenti di scuola secondaria e il 48% degli universitari non sa a chi rivolgersi; ciò accentua la necessità di un identificare un punto di riferimento noto a cui gli studenti (e non) possono appellarsi nel caso incorrano in situazioni di pericolo online.

*Si palesa un'incertezza diffusa anche riguardo ai soggetti da contattare in caso di problematiche online, come phishing o furto d'identità. Il 36% degli studenti di scuola secondaria e il 48% degli universitari non sa a chi rivolgersi; ciò accentua la necessità di un identificare un punto di riferimento noto a cui gli studenti (e non) possono appellarsi nel caso incorrano in situazioni di pericolo online*

Un segnale positivo è rappresentata dal fatto che la larghissima maggioranza dei partecipanti alla survey ha definito come molto (34% degli studenti di scuola secondaria e 38% degli universitari) o abbastanza importanti (46% e 44%) le iniziative per accrescere la consapevolezza digitale. Da ciò si può desumere che la quasi totalità dei giovani comprendono che l'ecosistema digitale abbia dei punti oscuri da cui sia necessario difendersi e che possedere un adeguato bagaglio di skill è lo strumento più importante per agire in tal senso.

*La larghissima maggioranza dei partecipanti alla survey ha definito come molto (34% degli studenti di scuola secondaria e 38% degli universitari) o abbastanza importanti (46% e 44%) le iniziative per accrescere la consapevolezza digitale*

Analizzare anche la prospettiva dei docenti rispetto al livello di awareness digitale dei propri studenti è fondamentale per delineare un quadro coerente in merito al tema, poiché non è scontato che il punto di vista dei primi coincida con quello dei secondi. Per questo, si è deciso in parallelo di costruire e somministrare una survey rivolta agli insegnanti.

Innanzitutto, è stato chiesto al campione di valutare il livello di consapevolezza dei propri studenti circa i rischi connessi all'utilizzo di strumenti digitali ed è emerso che per la maggioranza di docenti appartenenti alle scuole secondarie di secondo grado (42%) e alle scuole primarie (42%) c'è poca consapevolezza, mentre viene valutata come parziale da chi insegna in scuole secondarie di primo grado (35%). I risultati si mostrano preoccupanti se si considera che complessivamente solo il 3% e il 20% dei docenti affermano che i propri studenti sono, rispettivamente, molto o abbastanza consapevoli dei pericoli connessi alla rete. Inoltre, secondo il 31% degli insegnanti (19% tra quelli appartenenti alle primarie; il 4% tra i docenti delle secondarie di primo grado e l'8% tra i professori delle secondarie di secondo grado) vi è una totale assenza di awareness in merito alla tematica, aspetto che invece non è stato per niente valutato dal 5% dei docenti.

*Per la maggioranza di docenti appartenenti alle scuole secondarie di secondo grado (42%) e alle scuole primarie (42%) c'è poca consapevolezza, mentre viene valutata come parziale da chi insegna in scuole secondarie di primo grado (35%)*

Dalla survey è emerso anche che i principali pericoli in cui rischiano di imbattersi i giovani nell'ottica degli insegnanti sono: la dipendenza da Internet (secondo il 77% dei docenti delle scuole secondarie di secondo grado, il 78% di quelli delle scuole primarie e l'80% di quelli delle scuole secondarie di primo grado); la violazione della privacy secondo il 73% degli insegnanti delle scuole secondarie di secondo grado; il cyberbullismo per il 63% delle primarie e, in egual misura, delle secondarie di primo grado. Diversamente, sembra che la perdita di dati personali non sia un fenomeno così diffuso, essendo rilevante solo per il 9% dei docenti delle secondarie di primo grado, per l'8% di quelli appartenenti alle secondarie di secondo grado e per il 4% di coloro che insegnano alle primarie. Oltre ai pericoli esplicitamente indicati nelle domande, tra le risposte libere vengono individuati anche la pornografia, la disinformazione, la propaganda e l'imitazione di modelli che producono influenze negative legate allo sviluppo di comportamenti violenti e alla percezione distorta dell'aspetto fisico.

*I principali pericoli in cui rischiano di imbattersi i giovani nell'ottica degli insegnanti sono: la dipendenza da Internet (secondo il 77% dei docenti delle scuole secondarie di secondo grado, il 78% di quelli delle scuole primarie e l'80% di quelli delle scuole secondarie di primo grado); la violazione della privacy secondo il 73% degli insegnanti delle scuole secondarie di secondo grado; il cyberbullismo per il 63% delle primarie e, in egual misura, delle secondarie di primo grado*

Gli studenti, dalla primaria fino alla secondaria di secondo grado, tendono mediamente a rivolgersi ai docenti per problematiche legate all'utilizzo di strumenti digitali. In particolare, gli studenti delle primarie sembrano affidarsi agli insegnanti prevalentemente per questioni legate al cyberbullismo, contenuti offensivi online e video di istigazione a comportamenti pericolosi. Tra i discenti di entrambi i gradi della scuola secondaria emergono principalmente le medesime problematiche: cyberbullismo, diffusione online non autorizzata di dati, foto e video privati (violazione della privacy), incontri indesiderati sui social e chiarimenti sui pericoli della rete.

*Gli studenti, dalla primaria fino alla secondaria di secondo grado, tendono mediamente a rivolgersi ai docenti per problematiche legate all'utilizzo di strumenti digitali. In particolare, gli studenti delle primarie sembrano affidarsi agli insegnanti prevalentemente per questioni legate al cyberbullismo, contenuti offensivi online e video di istigazione a comportamenti pericolosi*

Con riguardo al grado di competenza nel consigliare i propri studenti in termini di prevenzione e risposta alle minacce informatiche, la maggior quota di docenti della primaria (55%), della secondaria di primo (46%) e secondo grado (45%) ritengono di esserne abbastanza in grado. Al contrario il 12% degli insegnanti della primaria, il 4% della secondaria di primo grado e il 10% di quella di secondo grado, si ritengono poco o per niente preparati.

La maggioranza dei docenti ritiene però molto o abbastanza utile partecipare a iniziative per accrescere la propria consapevolezza e competenza rispetto ai pericoli della rete. Preoccupante, invece, che resiste una sacca di minoranza ma comunque consistente di insegnanti che considerano poco o per niente utile essere coinvolti in tali iniziative formative, di cui larga parte, in particolare nei due gradi della scuola secondaria.
Infine, è stato chiesto ai docenti del campione di selezionare le iniziative che ritengono idonee a promuovere la consapevolezza digitale dei propri discenti ed è emerso che la maggioranza degli insegnanti di tutte le tipologie di istituti considera particolarmente importante sensibilizzare il gruppo classe con l'ausilio di esperti nell'uso etico delle tecnologie digitali. A seguire, la seconda voce maggiormente individuata dai docenti riguarda il ruolo da non sottovalutare delle famiglie, anch'esse da formare su questi temi. In terza posizione tra le risposte maggiormente selezionate si colloca il supporto alla formazione dei docenti.

*La maggioranza degli insegnanti di tutte le tipologie di istituti considera particolarmente importante sensibilizzare il gruppo classe con l'ausilio di esperti nell'uso etico delle tecnologie digitali*

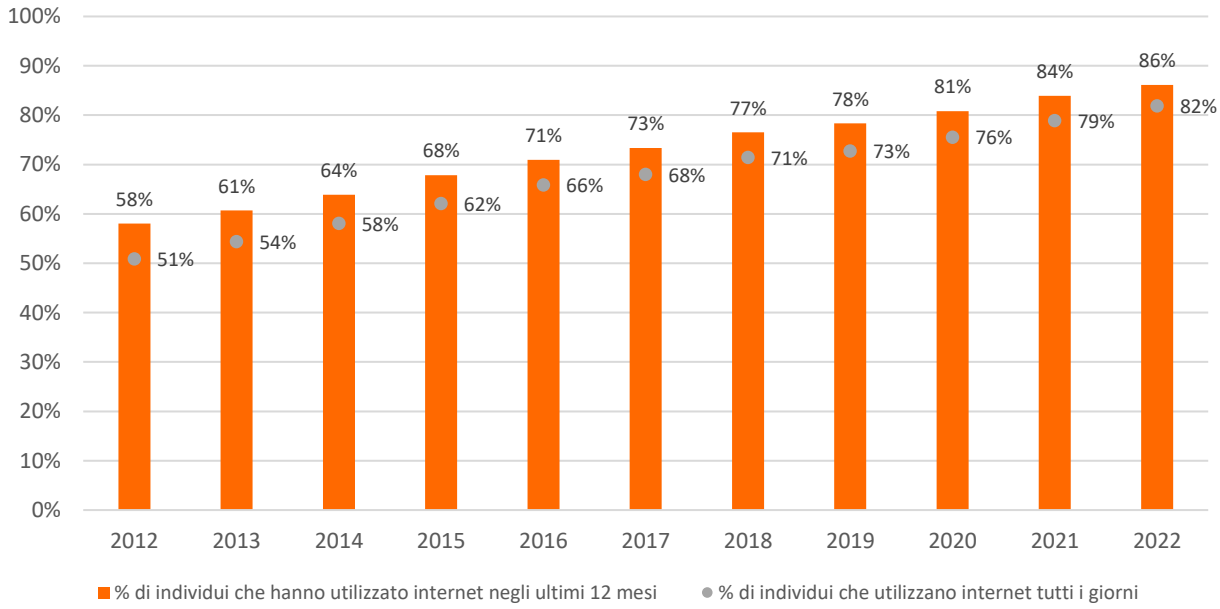
# 1. L'IMPATTO DELLA DIGITALIZZAZIONE SUL CAMBIAMENTO DELLE ABITUDINI DEGLI INDIVIDUI

## 1.1. L'utilizzo degli strumenti digitali da parte della popolazione

La transizione digitale e la conseguente migrazione sul web di una gamma di servizi sempre più ampia stanno gradualmente ridisegnando le abitudini di individui, abilitando nuovi canali relazionali e creando opportunità di business innovative. Il numero di italiani che utilizzano Internet è notevolmente cresciuto nell'ultimo decennio arrivando, nel 2022, a rappresentare l'86% della popolazione nazionale, ovvero oltre 50 milioni di persone. È interessante notare come, nell'arco di poco più di un decennio, sia significativamente cresciuta anche la quota di individui che utilizzano internet tutti i giorni, passata dal 50,9% del 2012 al 82% del 2022. Tale dato dimostra chiaramente l'estrema pervasività che i canali digitali hanno raggiunto nelle nostre attività quotidiane (Fig.1.1).

**Fig.1.1: Individui che utilizzano Internet in Italia (%)**

Fonte: Eurostat




*Il numero di italiani che utilizzano Internet è notevolmente cresciuto nell'ultimo decennio arrivando nel 2022 a rappresentare l'86,1% della popolazione nazionale, ovvero oltre 50 milioni di persone*

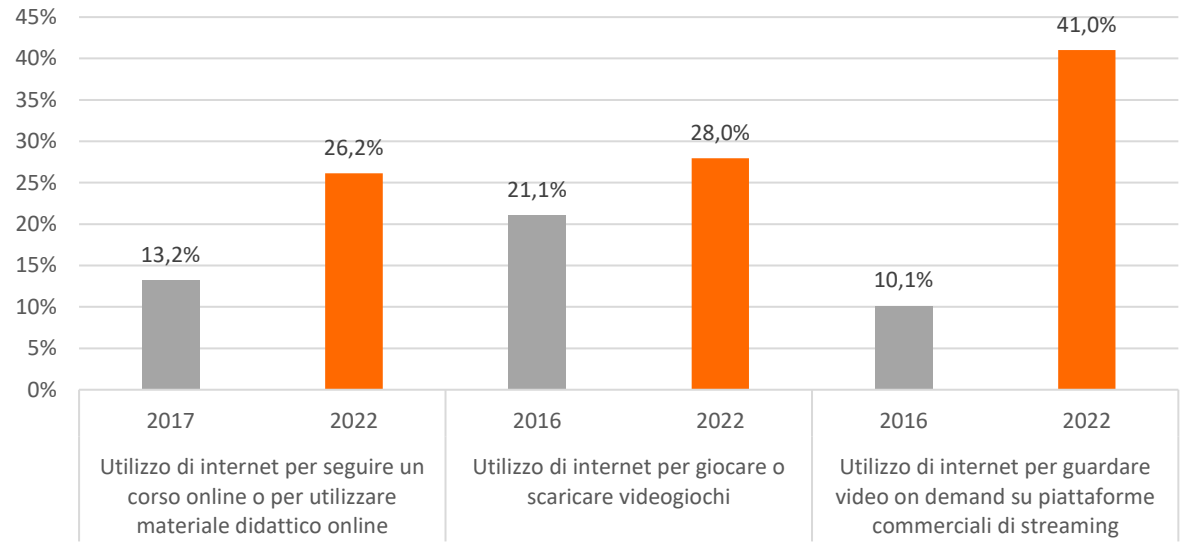
Non è solo la frequenza con cui gli individui accedono al web a crescere ma anche il ventaglio di attività che questi svolgono sulla rete. Ormai, ogni giorno nascono nuovi servizi e opportunità online che, grazie alla cassa di risonanza rappresentata dai social media, riescono ad affermarsi a livello globale in brevissimo tempo. Nel 2016, circa il 10% dei 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 quadruplicata, raggiungendo il 41% nel 2022. Sempre nell'ambito dell'intrattenimento, in Italia è cresciuta anche la quota di individui che utilizza internet per giocare o scaricare videogiochi, passata dal 21% al 28%.

La connettività digitale non ha vissuto un andamento crescente solo relativamente alle finalità ludiche, ad esempio 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.1.2).

**Fig.1.2: Individui che utilizzano Internet in Italia, per tipologia di attività (%)**

Fonte: Eurostat



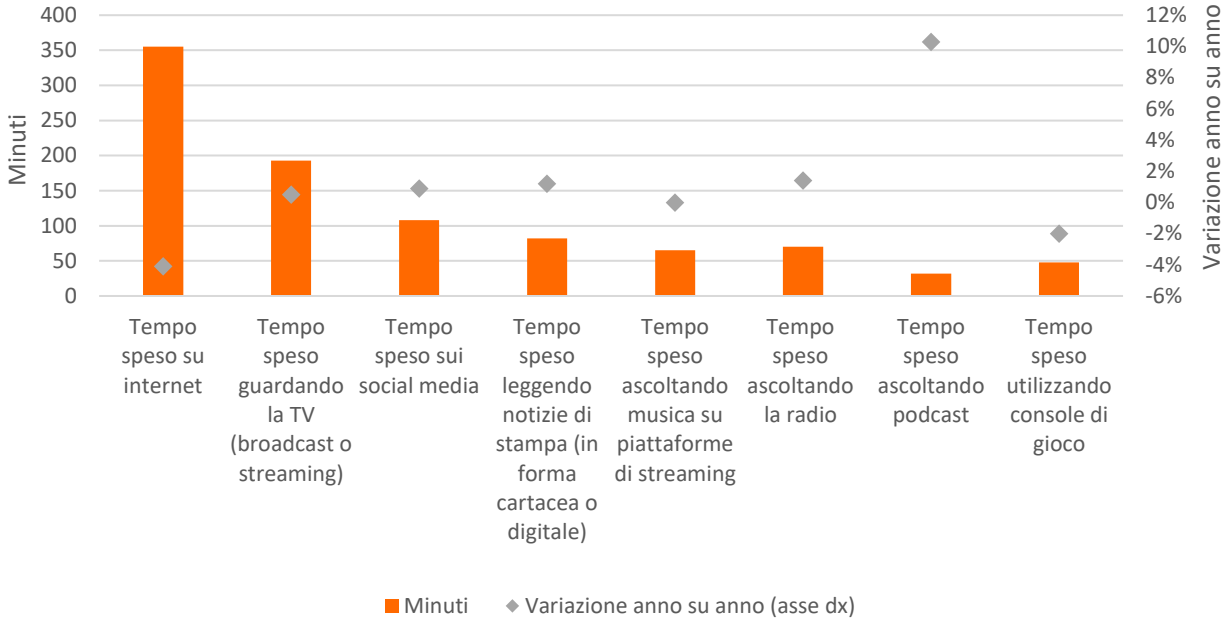

*Nel 2016, circa il 10% dei cittadini italiani utilizzava la rete per fruire di contenuti video on demand tramite piattaforme di streaming. Nel corso di soli sei anni, questa percentuale è quadruplicata, raggiungendo il 41%. Sempre nell'ambito dell'intrattenimento, in Italia è cresciuta anche la quota di individui che utilizza internet per giocare o scaricare videogiochi, passata dal 21% al 28%*

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 hanno trascorso in media 335 minuti al giorno online, segnando una leggera diminuzione del 4% rispetto all'anno precedente (Fig.1.3). 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.

**Fig.1.3: Minuti spesi ogni giorno svolgendo diverse attività, in Italia (individui tra i 16 e i 64 anni, 2022)**

Fonte: We Are Social, Digital 2023



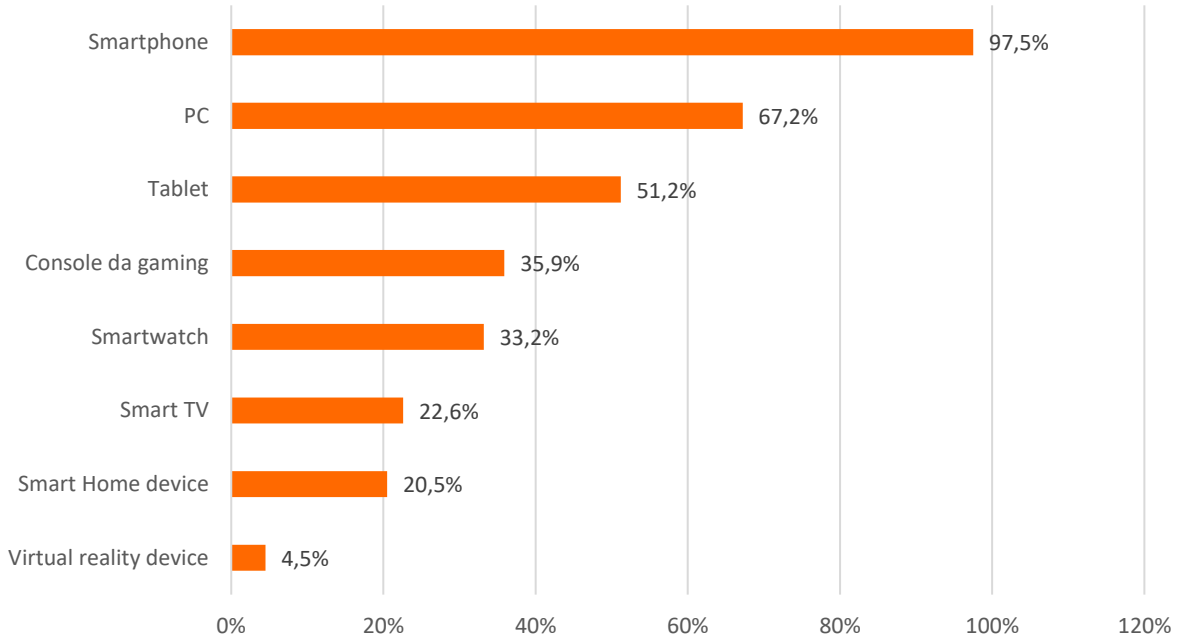

La crescita dirompente dei canali digitali ha riguardato anche le tipologie di dispositivi tramite cui gli individui fruiscono di servizi connessi, andando così a ridefinire il nostro modo di interagire con la tecnologia nella quotidianità. Dagli ultimi dati diffusi da We Are Social (Fig.1.4), emerge come al 2022 quasi la totalità della popolazione tra italiana tra i 16 e i 64 anni accede ad internet tramite smartphone (97,5%), circa il 30% in più rispetto a chi utilizza abitualmente un PC (62,2%).

*Dagli ultimi dati diffusi da We Are Social, emerge come al 2022 quasi la totalità della popolazione tra italiana tra i 16 e i 64 anni accede ad internet tramite smartphone (97,5%), circa il 30% in più rispetto a chi utilizza abitualmente un PC (62,2%)*

Particolarmente rilevante è anche la quota di individui che utilizzano altri tipi di device connessi, come le console da gaming (35,9%), gli smartwatch (33,2%), le smart TV (22,6%) e i dispositivi di smart home (20,5%). Nonostante rappresenti ancora una percentuale residuale (4,5%), è in forte aumento anche la quota di italiani che usa device di realtà virtuale che, infatti, tra il 2021 e il 2022 ha sperimentato una crescita anno su anno di oltre il 60%.

**Fig.1.4: Utilizzo di dispositivi connessi da parte dei cittadini italiani (2022)**

Fonte: We Are Social, Digital 2023




L'evoluzione nelle preferenze degli utenti riguardo alla fruizione di dispositivi digitali emerge anche dall'osservazione dei dati relativi alle pagine web visitate per ciascun tipo di dispositivo. I dati We Are Social 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.1.5).

**Fig.1.5: Percentuale del totale delle pagine web in esecuzione su ciascun tipo di dispositivo, in Italia (2022)**

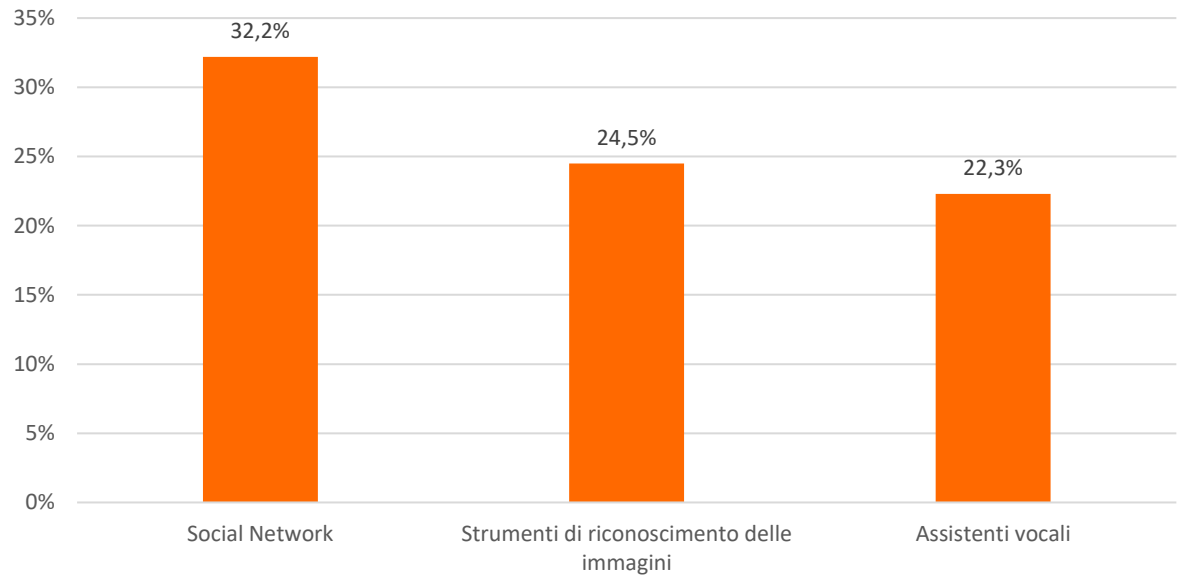
Fonte: We Are Social, Digital 2023

*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*

In constante evoluzione sono anche le modalità tramite il quale gli italiani ricercano informazioni online. Oltre ai classici motori di ricerca, crescono anche altre tipologie di canali di accesso alle informazioni come: i social network, utilizzati nel 2022 dal 32,2% della popolazione, con una crescita del 4,2% rispetto all'anno precedente; gli strumenti di riconoscimento delle immagini, che hanno raggiunto una penetrazione del 24,5%, in aumento del 3,8% anno sul 2021; gli assistenti vocali, che hanno raggiunto il 22,3% degli italiani, con una crescita anno su anno dello 0,9% (Fig.1.6).

**Fig.1.6: Quota di individui che utilizzano strumenti innovativi di ricerca delle informazioni in Italia, per tipologia di strumento (2022)**

Fonte: We Are Social, Digital 2023



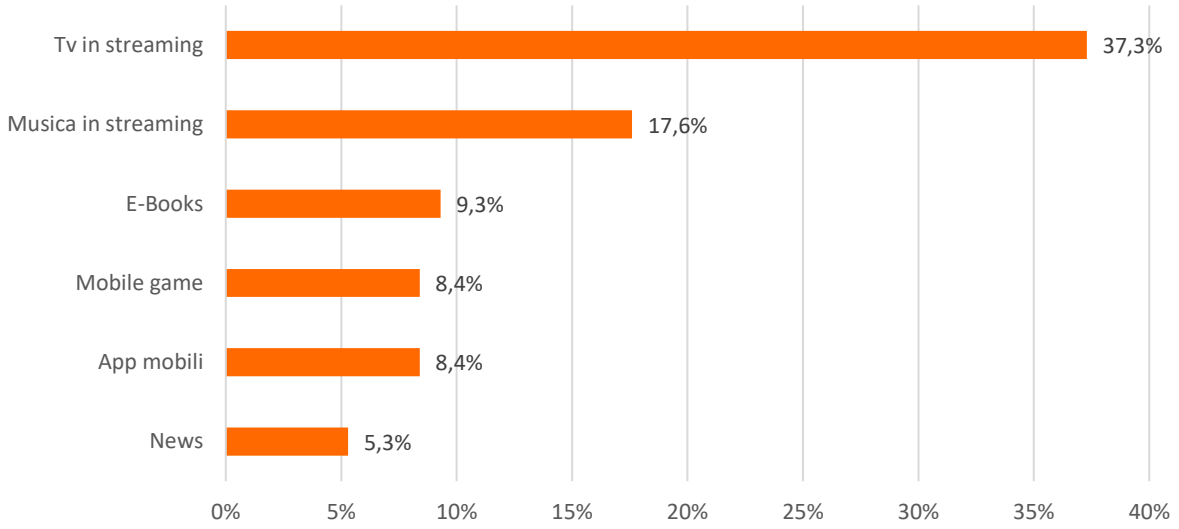

*Oltre ai classici motori di ricerca, crescono anche altre tipologie di canali di accesso alle informazioni come: i social network, utilizzati nel 2022 dal 32,2% della popolazione, con una crescita del 4,2% rispetto all'anno precedente; gli strumenti di riconoscimento delle immagini, che hanno raggiunto una penetrazione del 24,5%, in aumento del 3,8% anno sul 2021; gli assistenti vocali, che hanno raggiunto il 22,3% degli italiani, con una crescita anno su anno dello 0,9%*

Il cambiamento delle abitudini quotidiane degli italiani traspare in maniera chiara anche dalle scelte di consumo relative ai servizi digitali. Dai dati We Are Social emerge come nel 2022 il 37,3%

degli individui dai 16 ai 64 anni abbia scelto di acquistare un servizio di tv in streaming, il 17,6% lo streaming di musica e il 9,3% libri in formato digitale (Fig.1.7).

**Fig.1.7: Quota di italiani che pagano i servizi digitali, per tipologia di servizio acquistato (2022)**

Fonte: We Are Social, Digital 2023



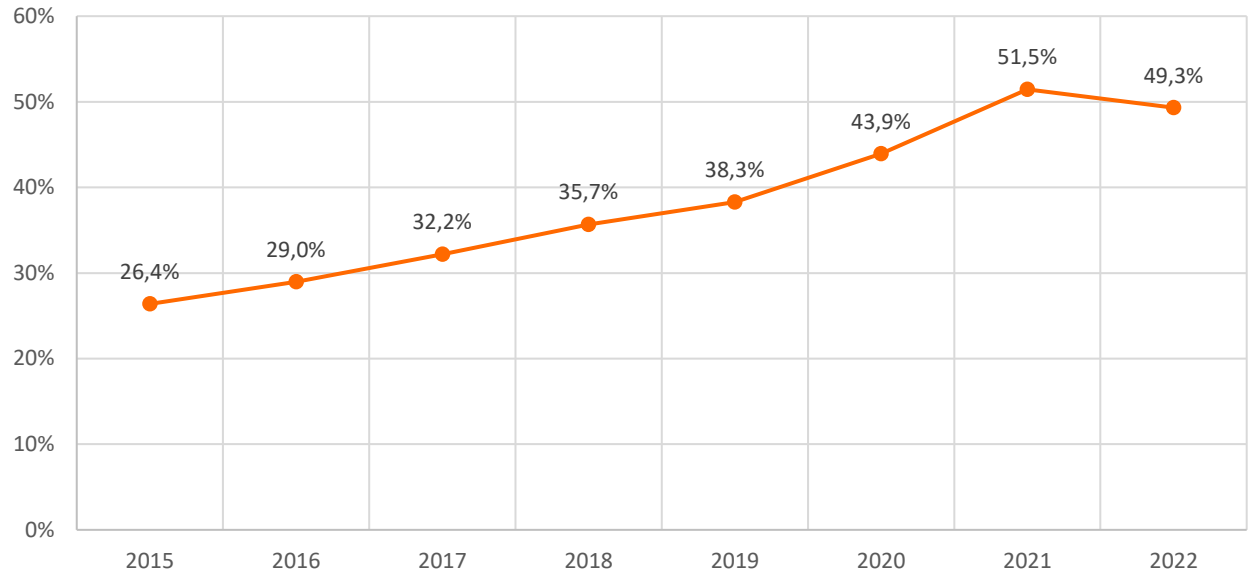

La digitalizzazione ha modificato radicalmente anche le modalità di acquisto di beni e servizi da parte della popolazione italiana. Osservando i dati Eurostat, vediamo come tra il 2015 e il 2022 la quota di italiani che ha effettuato almeno un acquisto online nel corso dell'anno sia raddoppiata (passando dal 26,4% al 49,3%), arrivando a coinvolgere circa la metà della popolazione nazionale (Fig.1.8).

*Osservando i dati Eurostat, vediamo come tra il 2015 e il 2022 la quota di italiani che ha effettuato almeno un acquisto online nel corso dell'anno sia raddoppiata, arrivando a coinvolgere la metà della popolazione nazionale*

Dall'analisi della serie temporale si nota chiaramente come la crescita del canale online, già sostenuta, abbia vissuto una forte accelerazione nel periodo pandemico. Questo dimostra ancora una volta quanto le restrizioni domiciliari abbiano giocato un ruolo importantissimo nella transizione digitale del Paese.

**Fig.1.8: Individui che effettuano acquisti online (2022)**

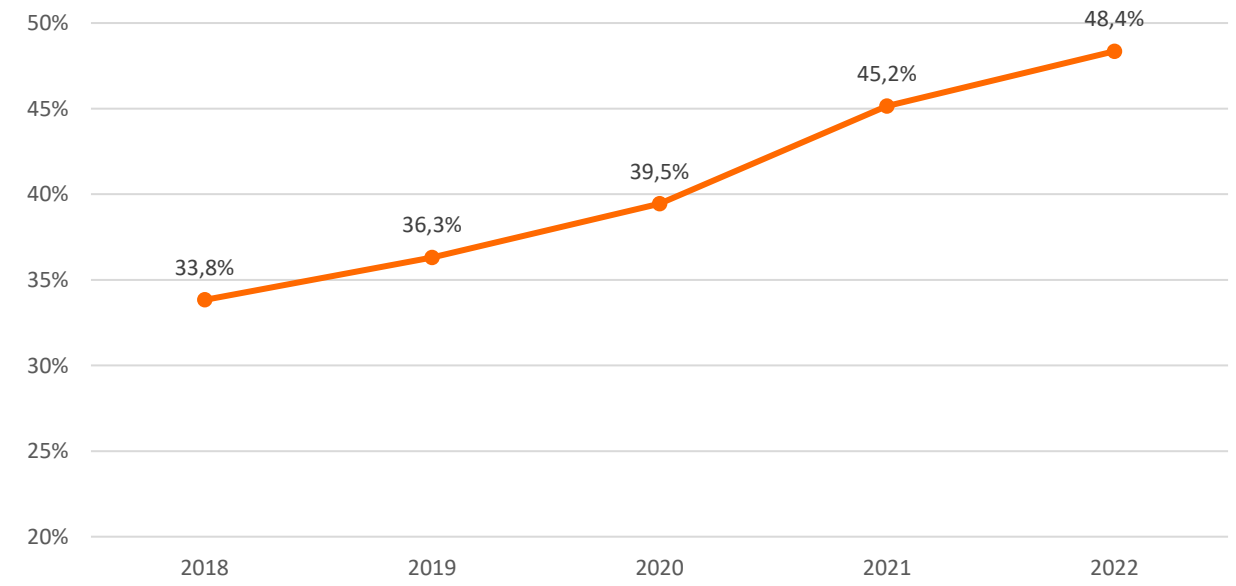
Fonte: Eurostat




Infine, unitamente al cambiamento delle abitudini di consumo si è inevitabilmente evoluta anche la modalità con cui gli italiani gestiscono le proprie finanze. Nel 2022 quasi metà della popolazione italiana utilizzava un servizio di internet banking (Fig.1.9). Tale percentuale è cresciuta in maniera costante dal 2018, registrando un incremento pari al 14,6%.

**Fig.1.9: Utilizzo dell'internet banking da parte dei cittadini italiani ed europei (%)**

Fonte: Eurostat



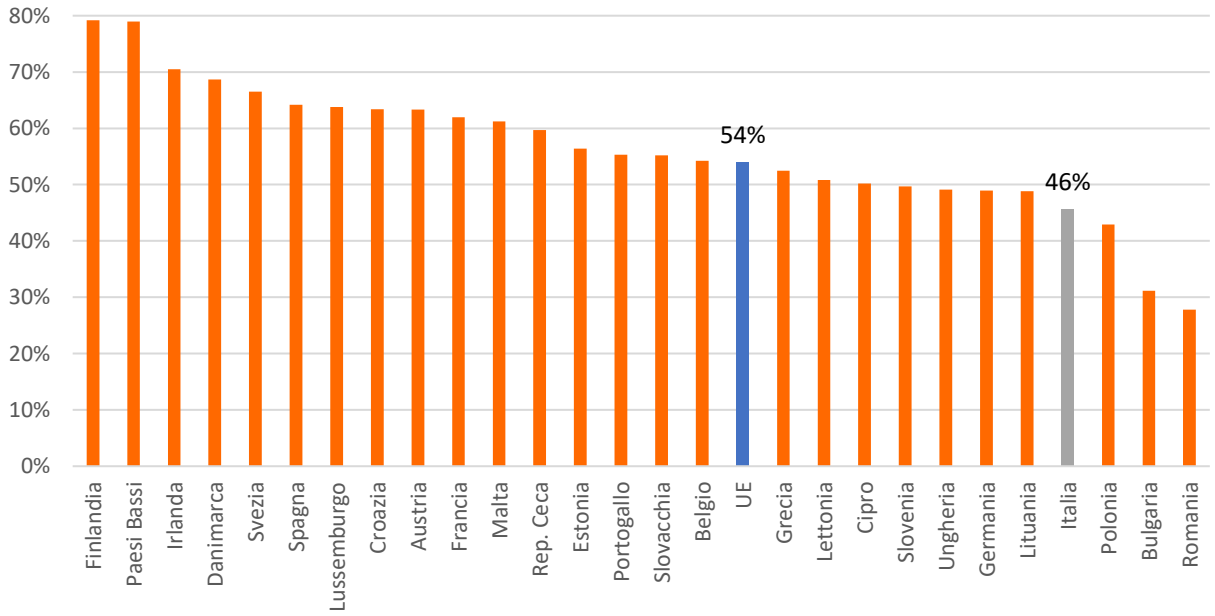
## 1.2. Le competenze digitali degli italiani

La digitalizzazione rappresenta sia una sfida che un'opportunità per l'Italia, alla quale è necessario rispondere mediante un'idonea preparazione dei suoi protagonisti, ossia gli utenti della rete, che fruiscono delle nuove tecnologie essendo esposti ai rischi che da esse ne derivano. Perciò, al fine di affrontare con successo tale evoluzione è necessario investire nella formazione e nell'aggiornamento delle competenze della popolazione considerata nella sua interezza, comprendendo sia giovani che adulti. Un simile approccio comporta inevitabilmente il miglioramento dell'esperienza dei singoli in Internet, innalzando la consapevolezza rispetto al funzionamento e agli effetti tipici derivanti dalle interazioni nel cyberspazio.

Nonostante quanto appena esposto sia generalmente condiviso nelle strategie adottate dalle Istituzioni nazionali, gli ultimi dati diffusi da Eurostat mostrano ancora 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.1.10). 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.

**Fig.1.10: Quota della popolazione con competenze digitali almeno basilari per Stato Membro UE (2021)**

Fonte: DESI 2023

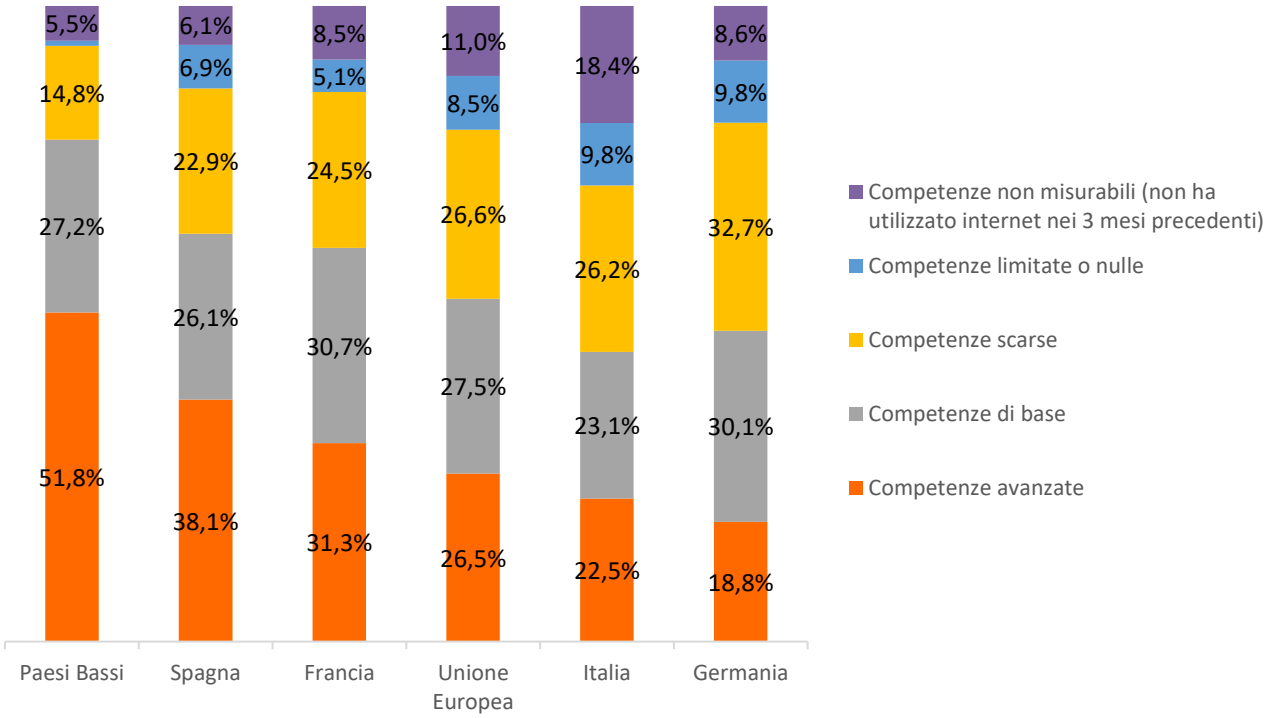



*Gli ultimi dati diffusi da Eurostat mostrano ancora un'arretratezza generalizzata da parte dell'Italia in questo ambito. Il nostro Paese si posiziona al quartultimo posto in UE per quota di popolazione (46%) in possesso di competenze digitali almeno basilari*

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.1.11). 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.1.11: Composizione delle competenze digitali della popolazione per nazione (2021)**

Fonte: Eurostat

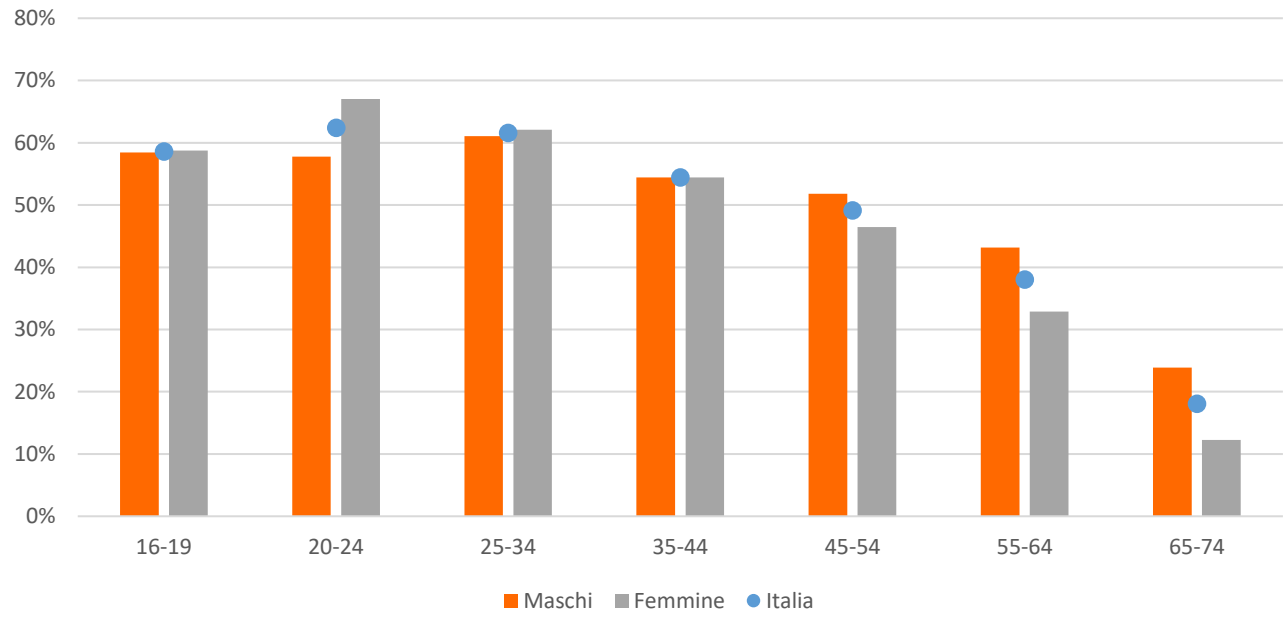



Focalizzando l'attenzione sul contesto nazionale, gli ultimi dati pubblicati dall'Istat[1] a gennaio 2023 (relativi al 2021) evidenziano un interessante cambiamento di tendenza relativamente alle distribuzioni delle competenze digitali tra genere maschile e femminile. Se infatti storicamente il genere 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.1.12).
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.

[1] *04/01/2023, https://www.istat.it/it/files/2023/06/cs-competenzedigitali.pdf.*

**Fig.1.12: Individui con competenze digitali almeno di base per genere e classe di età (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 dirigenti, 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.

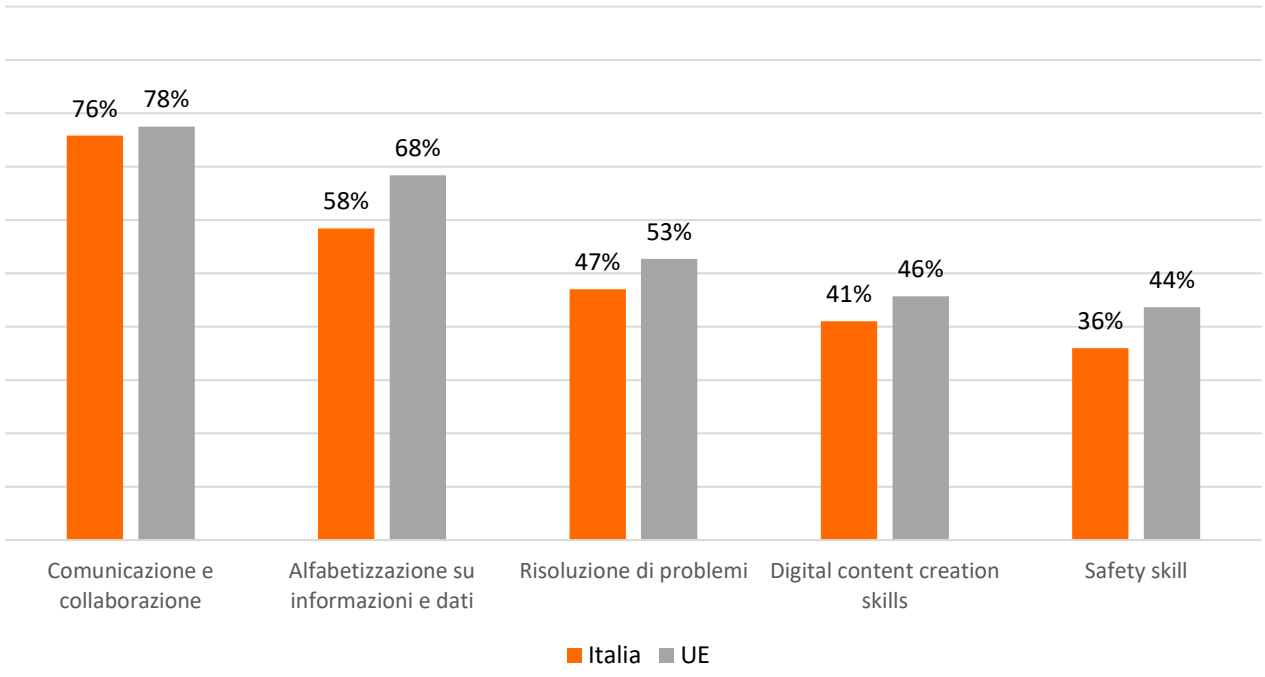
*L'80,3% delle persone di età compresa tra i 25 e i 54 anni con istruzione terziaria ha almeno competenze digitali di base, una percentuale quasi allineata con la media UE. Tuttavia, tale quota scende al 25% per le persone con titoli di studio bassi, fino alla licenza media, presentando un divario di circa l'8% rispetto alla media europea*

Le competenze digitali possono essere suddivise, secondo le rilevazioni Istat e Eurostat, in cinque diverse dimensioni (Fig. 1.13): 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.

**Fig.1.13: Individui con competenze elevate nelle 5 componenti delle competenze digitali (2021)**

Fonte: Istat 2023




*Le competenze digitali possono essere suddivise, secondo le rilevazioni Istat e Eurostat, in cinque diverse dimensioni (Fig. 1.13): comunicazione e collaborazione; alfabetizzazione su informazioni e dati; risoluzione di problemi; capacità di creare contenuti digitali; abilità di sicurezza*

# 2. STRUMENTI DIGITALI QUALI DRIVER DI SOSTENIBILITÀ

Spesso si parla di come transizione ecologica e transizione digitale siano parallele e interconnesse. Infatti, se da una parte la crisi climatica e la rivoluzione digitale sono due trasformazioni globali, profonde e irreversibili, è anche vero che il digitale può considerarsi un prezioso strumento e facilitatore per raggiungere la sostenibilità ambientale, economica e sociale. La tecnologia può essere utilizzata per contrastare il cambiamento climatico e l'inquinamento, nonché essere un facilitatore di soluzioni di *work – life balance* e quindi in sostanza portare benessere sia alle persone sia al pianeta.

Le tecnologie come intelligenza artificiale, *super computing* e *quantum computing*, il cloud, l'analisi dei dati, le reti 5G e wi-fi consumano una grande quantità di energia e hanno per alcuni versi contribuito ad accelerare il cambiamento climatico ma oggi possono decisamente contribuire a fermarlo.

Secondo la *Global e-Sustainability Initiative* (GESI), la tecnologia ha il potenziale di contribuire a tutti i 17 obiettivi ONU per lo Sviluppo sostenibile entro il 2023. Secondo il Rapporto, l'implementazione delle tecnologie digitali può accelerare i progressi verso gli SDGs del 22%. Ciò è raggiungibile se Stati, ONG, cittadini e aziende collaborano e adottano comportamenti coerenti. La svolta è rappresentata dalla crescente capacità di generare, catturare e trasmettere dati digitali e di analizzarli per metterli al servizio degli obiettivi di sostenibilità.

*Secondo la Global e-Sustainability Initiative (GESI), la tecnologia ha il potenziale di contribuire a tutti i 17 obiettivi ONU per lo Sviluppo sostenibile entro il 2023. Secondo il Rapporto, l'implementazione delle tecnologie digitali può accelerare i progressi verso gli SDGs del 22%*

La diminuzione degli spostamenti, la dematerializzazione dei processi, la gestione domotica dei consumi energetici sono solo alcuni degli esempi che evidenziano come il digitale semplifichi la vita delle persone e contribuisca a ridurre le emissioni, producendo un impatto positivo sulla società e un vantaggio significativo in termini di sostenibilità ambientale. Inoltre, il diritto all'accesso a forme di connettività evoluta rappresenta un elemento di inclusione sociale per tutte le fasce di popolazione e il territorio.

Il digitale può essere un abilitatore della sostenibilità sociale e ambientale in molteplici ambiti. Infatti, le reti di ultima generazione come le infrastrutture digitali, quali pali, torri e tralicci, la fibra ed il 5G hanno il potenziale per colmare il divario digitale e sostenere una ripresa economica inclusiva, aumentando le opportunità delle popolazioni nelle comunità rurali o svantaggiate e contribuendo a collegarle alla opportunità di istruzione, conoscenza e apprendimento, lavoro flessibile, accesso a nuovi mestieri, ecc.
Da un punto di vista sociale, le infrastrutture e la tecnologia digitale consentono l'accesso all'istruzione a distanza, aprendo opportunità educative anche a persone in aree remote o con risorse limitate e contribuendo a ridurre il divario educativo con un conseguente incremento dell'alfabetizzazione, e l'accesso alla medicina, dove la telemedicina e i dispositivi indossabili

consentono un migliore accesso ai servizi sanitari, migliorando la qualità delle cure mediche, consentendo a persone con limitazioni di mobilità di ricevere assistenza sanitaria di alta qualità. Le infastrutture e la tecnologia digitale, inoltre, favoriscono il lavoro flessibile, consentendo agli individui di conciliare meglio il lavoro con altre responsabilità familiari e personali, migliorando la qualità della vita e l'equilibrio tra lavoro e vita. Nel 2023 i lavoratori da remoto in Italia sono circa 3,6 milioni.[2]
Infine, le soluzioni di pagamento e microfinanza digitali offrono a individui a basso reddito e comunità svantaggiate l'accesso ai servizi finanziari, promuovendo l'indipendenza economica e la stabilità.
Anche banalmente aumentando nelle varie fasce di popolazione il grado di diffusione ed utilizzo dei *device* mobili di ultima generazione, supportanti applicazioni intelligenti e utili, è dimostrato che si concorre agli obiettivi di sviluppo sostenibile.

*Le infrastrutture e la tecnologia digitale, inoltre, favoriscono il lavoro flessibile, consentendo agli individui di conciliare meglio il lavoro con altre responsabilità familiari e personali, migliorando la qualità della vita e l'equilibrio tra lavoro e vita. Nel 2023 i lavoratori da remoto in Italia sono circa 3,6 milioni*

Da un punto di vista ambientale, l'*Internet of Things* (IoT) e i *device* mobili stanno rivoluzionando il monitoraggio ambientale. In tal senso, l'evoluzione delle infrastrutture digitali da mero elemento passivo a tower as a service, attraverso la raccolta di dati in tempo reale da sensori posizionati in modo capillare su tutto il territorio, consente alle imprese e alle istituzioni di tracciare e gestire risorse in modo più efficiente.
Secondo il rapporto "*IoT in Environmental Monitoring*" di MarketsandMarkets, il mercato IoT per il monitoraggio ambientale dovrebbe crescere a un CAGR del 21,3% dal 2021 al 2026. Ciò consente di ridurre sprechi e minimizzare l'impatto sull'ambiente, in quanto permetterebbero di raccogliere dati che possono essere utilizzati per rilevare inquinanti, cambiamenti climatici, deforestazione e altri problemi ambientali, al fine di avere una risposta tempestiva alle minacce all'ambiente.

Inoltre, l'automazione e i sistemi di gestione energetica basati su dati contribuiscono all'ottimizzazione del consumo energetico negli edifici, nell'industria e nei trasporti, riducendo così l'impatto ambientale e il consumo di risorse. Inoltre, la tecnologia digitale è utilizzata per gestire in modo efficiente l'energia da fonti rinnovabili come il solare e l'eolico, migliorando la distribuzione e la produzione di energia green. In questo ambito vengono utilizzate le reti energetiche intelligenti, le quali utilizzano sensori e algoritmi di gestione dell'energia al fine di ottimizzare la distribuzione di energia e favorire l'adozione delle energie rinnovabili. Secondo l'Agenzia Internazionale dell'Energia (IEA), l'energia rinnovabile ha superato il carbone come principale fonte di elettricità a livello globale nel 2022.

Infine, le applicazioni mobili e i servizi di condivisione di veicoli stanno rivoluzionando il modo in cui ci spostiamo. Il rapporto di Deloitte "*The Future of Mobility*" evidenzia che il *car sharing* e il

[2] *Fonte: Osservatorio Smart Working della School of Management del Politecnico di Milano*

*ride-sharing* possono ridurre il numero di veicoli nelle strade, contribuendo a ridurre le emissioni di carbonio.
Nel settembre 2022 scorso la *Global System for Mobile Communications Association (*GSMA) ha presentato il suo *"*Rapporto sull'impatto del settore mobile 2022: Obiettivi di sviluppo sostenibile".
La GSMA è un'organizzazione globale che riunisce gli attori dell'ecosistema dei dispositivi mobili con l'intento di promuovere e sviluppare innovazioni cruciali per il progresso sostenibile negli ambiti ambientale e sociale.
Da questo Rapporto è emerso che assicurare l'accesso alla connettività dei dispositivi mobili e promuovere adeguate competenze digitali sono fondamentali per una società sempre più sostenibile.
Il report della GSMA analizza in dettaglio gli effetti dei dispositivi mobili sui 17 *Sustainable Development Goals* (SDG), gli obiettivi per uno sviluppo sostenibile, che spaziano dal superamento della povertà e della disuguaglianza alla diffusione di energie rinnovabili, passando per la creazione di nuovi modelli di business, che permettano di utilizzare materiali ed energie in modo più responsabile. Con l'obiettivo del 2030 che si avvicina rapidamente, questo rapporto annuale fornisce un aggiornamento sul progresso del settore verso gli SDG e identifica le aree che richiedono ulteriore attenzione per raggiungere gli obiettivi prefissati.

Nel 2021, si è verificato un notevole aumento dell'uso dei cellulari per l'accesso a informazioni educative, sia per uso personale che a beneficio dei propri figli, coinvolgendo 2,5 miliardi di persone (pari al 48% degli abbonati di telefonia mobile). Questo contribuisce in modo significativo al raggiungimento dell'Obiettivo di Sviluppo Sostenibile 4, "Istruzione di qualità", che ha registrato uno dei maggiori miglioramenti nell'impatto sugli SDG nel 2021. In particolare, l'uso dei cellulari a scopo educativo è cresciuto del 7% nei Paesi a reddito medio-basso e del 4% nei Paesi ad alto reddito, grazie a iniziative volte a promuovere le competenze digitali attraverso le tecnologie mobili.

*Nel 2021, si è verificato un notevole aumento dell'uso dei cellulari per l'accesso a informazioni educative, sia per uso personale che a beneficio dei propri figli, coinvolgendo 2,5 miliardi di persone (pari al 48% degli abbonati di telefonia mobile)*

Le applicazioni sanitarie mobili stanno vivendo una crescita esponenziale. Il mercato del *Mobile Health* valeva 30 miliardi di dollari nel 2018 e si prevede che, mantenendo un CAGR del 38% dal 2019 al 2025, possa arrivare a raggiungere un valore complessivo superiore ai 289 miliardi di dollari.
Ebbene, le soluzioni sanitarie mobili continuano a svolgere un ruolo importante nel sostenere il settore, con un contributo allo SDG 3 'Buona salute e benessere'. Altri 270 milioni di persone hanno utilizzato i dispositivi mobili per migliorare o monitorare la propria salute nel 2021, portando il totale a 2,1 miliardi, il 41% degli abbonati di telefonia cellulare.

Il Rapporto della GSMA mette infine in evidenza che è presente un divario considerevole nell'uso dei servizi abilitati alla mobilità tra i Paesi ad alto reddito e i Paesi a reddito medio-basso.

Le tecnologie digitali ci rendono iperconnessi soprattutto a causa dei social media, ma anche questi ultimi possono svolgere un ruolo significativo nel promuovere la sostenibilità in diverse modalità.

- Consapevolezza e informazione - I social media agevolano la rapida condivisione di notizie, informazioni e contenuti relativi alla sostenibilità, contribuendo all'educazione del pubblico su questioni ambientali, sociali ed economiche importanti. Sia organizzazioni che individui possono utilizzare piattaforme come Facebook, X (ex Twitter) e Instagram per diffondere notizie e dati relativi alla sostenibilità.

- Mobilizzazione e attivismo - I social media permettono alle persone di unirsi, diffondere petizioni, organizzare manifestazioni e sostenere cause ambientali e sociali. Le campagne di attivismo online possono avere un impatto significativo nel sensibilizzare e spingere le istituzioni a intraprendere azioni a favore della sostenibilità. Inoltre, spesso i social media sono utilizzati per coinvolgere le comunità locali in progetti specifici di sostenibilità, come la pulizia dell'ambiente o l'organizzazione di eventi dedicati alla sostenibilità. Per cause di carattere sociale e/o ambientale sono utilizzate anche le piattaforme di *crowdfunding* e i servizi di donazione online, le quali semplificano la raccolta di fondi per progetti di sostenibilità, permettendo alle organizzazioni di beneficenza di raggiungere un pubblico più esteso e, il più delle volte, globale.

- Comunicazione aziendale - Le aziende possono avvalersi dei social media per comunicare in modo trasparente le proprie iniziative di sostenibilità e mostrare come stanno riducendo il proprio impatto ambientale. Ciò può influenzare positivamente la percezione del brand e attirare i consumatori che cercano prodotti e servizi sostenibili.

- Scambio di conoscenze ed educazione - I social media consentono di condividere esperienze e conoscenze sulla sostenibilità, creando comunità di apprendimento, partecipando a discussioni e condividendo le proprie esperienze in cui gli individui possono scambiare informazioni su come vivere in modo più sostenibile. Inoltre, la fruizione dei contenuti educativi risulta essere più dinamica, attraverso webinar, immagini e video.

Le organizzazioni e le comunità possono condividere le loro migliori pratiche in materia di sostenibilità sui social media. Questo permette di diffondere idee innovative e ispirare altri a seguire l'esempio.

Tuttavia, è importante notare che l'uso dei social media per la sostenibilità deve essere sostenuto da azioni concrete al di fuori delle piattaforme online. La condivisione di contenuti e l'attivismo online dovrebbero essere complementari a comportamenti e decisioni quotidiane che promuovano la sostenibilità ambientale, sociale ed economica.

Nell'era digitale in cui viviamo la tecnologia ha radicalmente trasformato la nostra vita quotidiana, dal modo in cui lavoriamo e ci intratteniamo a come ci connettiamo con gli altri. Tuttavia, insieme alle innumerevoli opportunità offerte dal digitale, emergono anche questioni cruciali legate al benessere individuale e alla sostenibilità ambientale.

Il benessere digitale rappresenta un concetto centrale nel contesto dell'uso responsabile delle tecnologie. Si tratta di una riflessione sul modo in cui interagiamo con il digitale, con l'obiettivo di preservare la nostra salute mentale ed emotiva. La dipendenza da smartphone, la costante connessione ai social media e l'esposizione a una quantità eccessiva di informazioni possono avere effetti negativi sul nostro benessere. Pertanto, è fondamentale promuovere un utilizzo equilibrato delle tecnologie digitali, limitando il tempo trascorso online e adottando strategie di disconnessione digitale periodiche.

In conclusione, il benessere digitale e la sostenibilità sono concetti intrinsecamente collegati nell'era digitale. Promuovere un utilizzo responsabile delle tecnologie e sfruttare il digitale per la sostenibilità ambientale rappresenta un obiettivo comune per la costruzione di un futuro più equilibrato, dove l'innovazione tecnologica e il benessere umano camminano di pari passo.

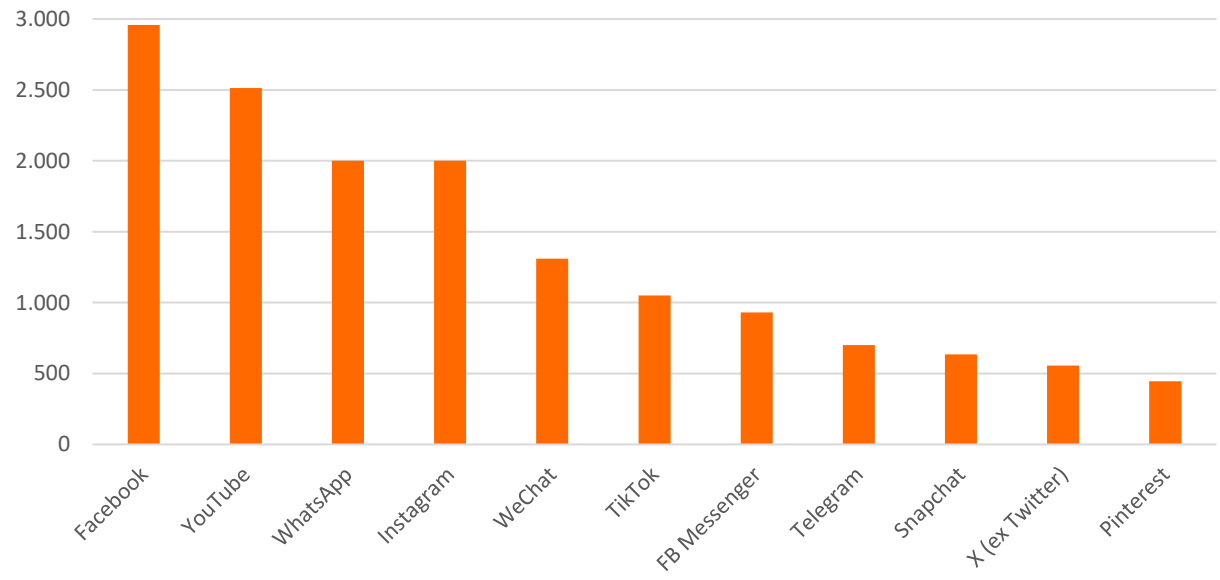
# 3. NUOVE TECNOLOGIE E NUOVI RISCHI

Negli ultimi anni si è reso evidente come l'evoluzione digitale e l'incremento del livello di accessibilità tecnologica rappresentino due punti di forza per il miglioramento delle attività umane. Difatti, in particolare durante il periodo pandemico, Internet è divenuto uno strumento utile per rispondere alle esigenze legate al lockdown. Si pensi, ad esempio, alle opportunità derivanti dallo *smart working* o dalla didattica a distanza favorita mediante piattaforme *e-learning* per la diffusione della cultura e dell'istruzione; o, ancor di più, alla necessità di intrattenere e coltivare rapporti umani soddisfatta grazie alle funzioni offerte dai social media.

In base ai dati del già citato "*Digital 2023*" (Fig. 4.1), pubblicato da We are social, è possibile osservare come, classificando le piattaforme in base agli utenti attivi mensili, Facebook detenga il primo posto a livello mondiale nel 2022 con 2,96 miliardi di individui connessi, seguito da YouTube (2,51 miliardi), Whatsapp e Instagram (2 miliardi). Nelle ultime posizioni vi sono Snapchat con 635 milioni di utenti mensili, X (ex Twitter) con 556 milioni e, in ultimo, Pinterest che chiude la classifica con 445 milioni.

**Fig.4.1: Piattaforme di social media in base al numero di utenti attivi mensili nel 2022 (in milioni)**

Fonte: We are social, Meltwater, "Digital 2023 Global Overview Report", gennaio 2023




Va però evidenziato che la popolazione tipica di questi "non luoghi" è costituita sia da utenti comuni che da utenti malevoli, i quali hanno sfruttato e attualmente impiegano le piattaforme online come mezzo per diffondere fake news, nonché contenuti illeciti e di incitamento all'*hate speech*. Quest'ultimo rappresenta un fenomeno non di semplice inquadramento a causa dell'estrema eterogeneità dei comportamenti che tende a racchiudere; pertanto, più in generale, si fa riferimento a forme di manifestazione del pensiero volte a diffondere, favorire, incoraggiare o giustificare l'odio fondato sull'intolleranza, indipendentemente dall'istigazione alla commissione di violenza e di comportamenti penalmente rilevanti.

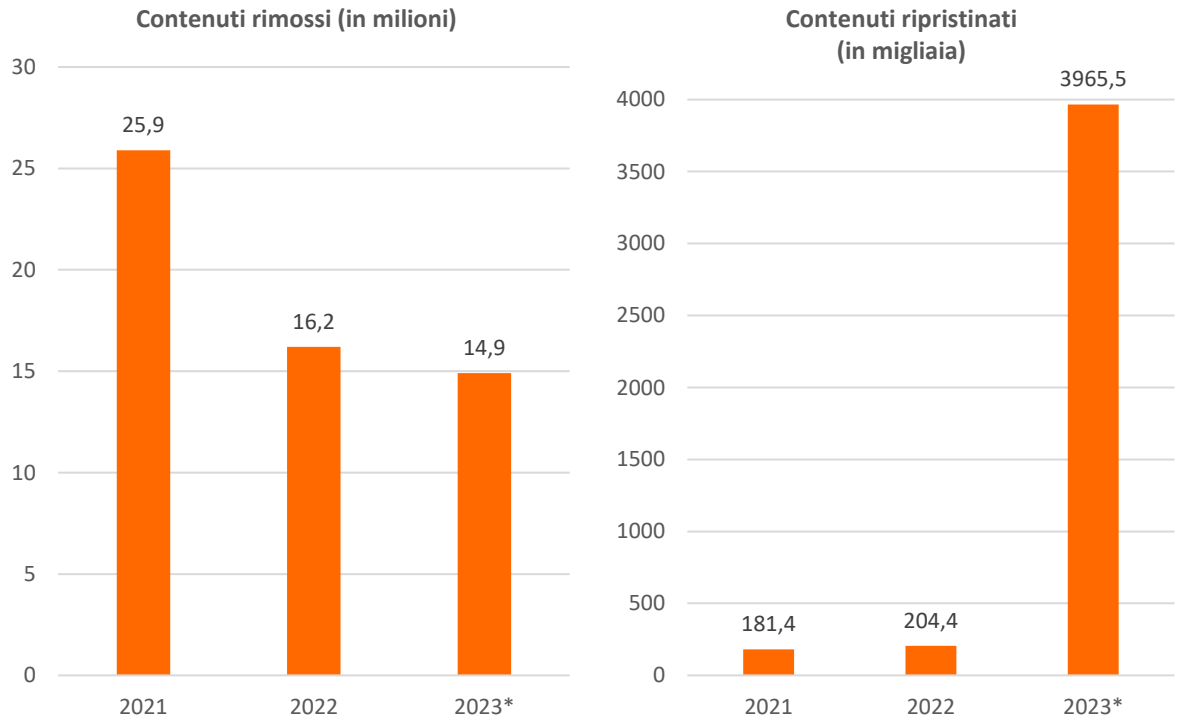
*La popolazione tipica di questi "non luoghi" è costituita sia da utenti comuni che da utenti malevoli, i quali hanno sfruttato e attualmente impiegano le piattaforme online come mezzo per diffondere fake news, nonché contenuti illeciti e di incitamento all'hate speech*

Il *Meta Transparency Center* ha mappato le attività condotte dai social network Instagram e Facebook per contrastare la diffusione di contenuti d'odio, individuandoli in tutti i discorsi violenti o disumanizzanti, nelle dichiarazioni di inferiorità, negli appelli all'esclusione o alla segregazione sulla base di caratteristiche protette[3] o di insulti. In particolare (Fig.4.2), nel 2021 Instagram ha rimosso 25,9 milioni di contenuti incitanti all'odio, ossia 9,7 milioni in più rispetto al 2022 (16,2 milioni di contenuti colpiti), mentre nel primo semestre del 2023 tale operazione ha interessato 14,9 milioni di dati presenti sulla piattaforma.

A seguito di ricorsi con esito positivo contro la decisione di rimozione e nei casi in cui vi siano stati errori nella procedura di controllo e valutazione precedentemente eseguita, Instagram e Facebook sono tenuti a ripristinare i contenuti, reintegrandoli o rimuovendo l'avviso con cui è avvenuto il loro oscuramento. Difatti, dal 2021 sono stati resi nuovamente accessibili 4,35 milioni di dati, di cui 181,4 mila nel 2021; 204,4 mila nel 2022 e 3,96 milioni nel periodo che va da gennaio a giugno del 2023.

**Fig.4.2: Contenuti rimossi e ripristinati per incitamento all'odio da Instagram dal 2021**

Note: *I dati dell'anno 2023 fanno riferimento esclusivamente al primo semestre (gennaio-giugno)
Fonte: Meta Transparency Center



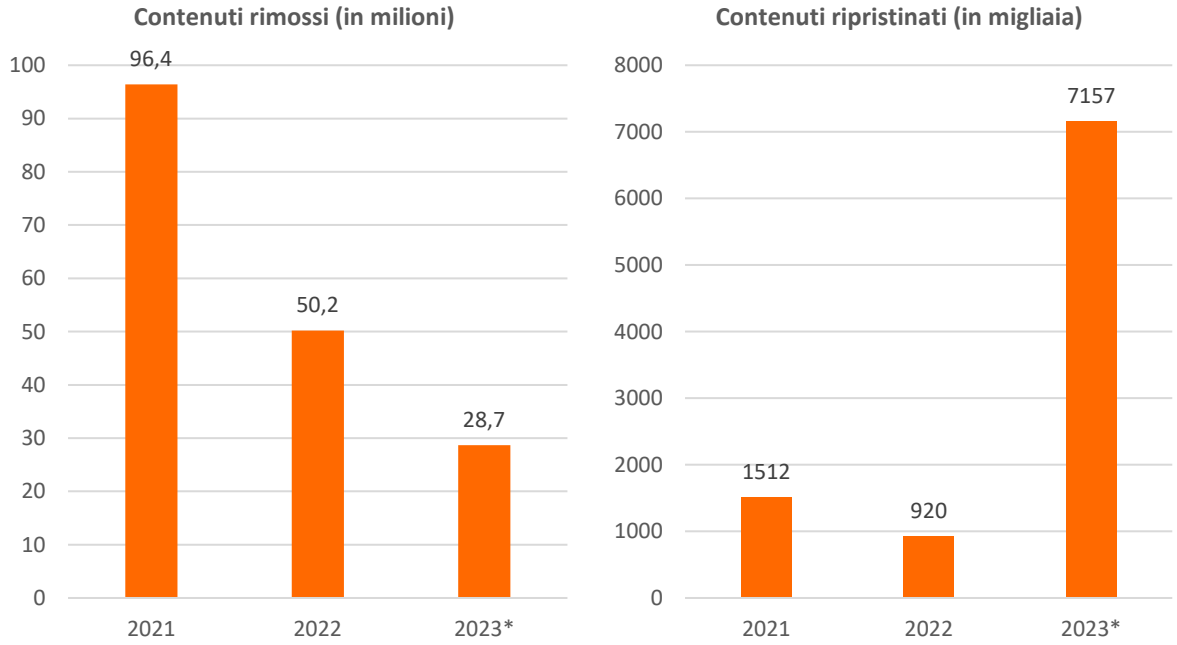

[3] *Queste caratteristiche includono razza, etnia, origine nazionale, affiliazione religiosa, orientamento sessuale, casta, sesso, genere, identità di genere e disabilità o malattie gravi.*

*Nel 2021 Instagram ha rimosso 25,9 milioni di contenuti incitanti all'odio, 9,7 milioni in più rispetto al 2022 (16,2 milioni di contenuti colpiti), mentre nel primo semestre del 2023 tale operazione ha interessato 14,9 milioni di dati presenti sulla piattaforma*

Come precedentemente detto, tali operazioni hanno interessato anche Facebook (Fig. 4.3), che ha rimosso 96,4 milioni di contenuti nel 2021; 50,2 milioni nel 2022 e 28, 7 milioni nei primi sei mesi di quest'anno. D'altro canto, tra questi ne sono stati ripristinati 9,58 milioni (1,51 milioni nel 2021; 920 mila nel 2022; 7,15 milioni nel primo semestre del 2023).

**Fig.4.3: Contenuti rimossi e ripristinati per incitamento all'odio da Facebook dal 2021**

Note: *I dati dell'anno 2023 fanno riferimento esclusivamente al primo semestre (gennaio-giugno)
Fonte: Meta Transparency Center



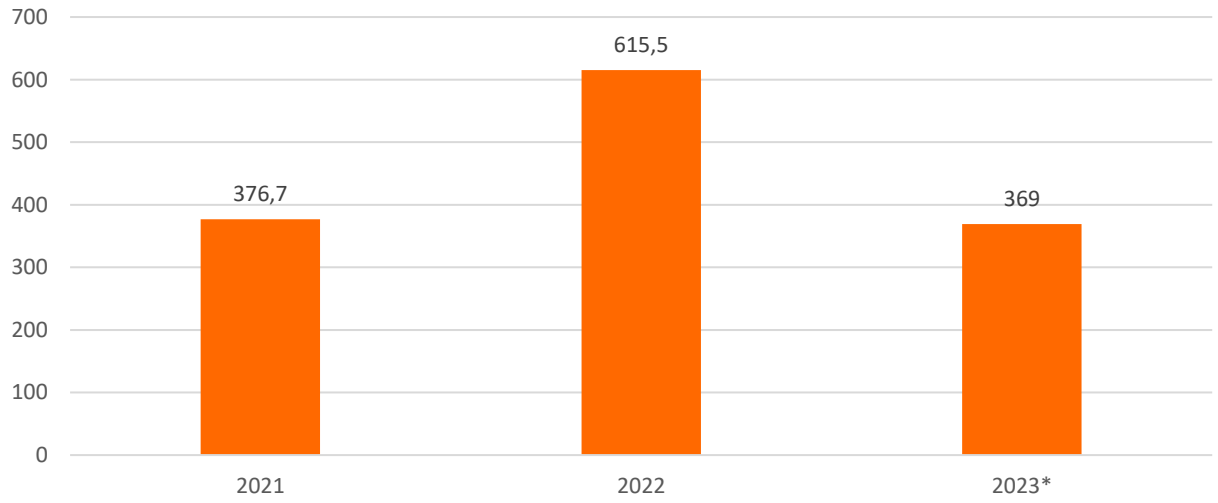

*Facebook ha rimosso 96,4 milioni di contenuti nel 2021; 50,2 milioni nel 2022 e 28,7 milioni nei primi sei mesi di quest'anno*

Allo stesso modo, anche YouTube si è impegnato al fine di rimuovere i video volti a favorire l'*hate speech*, nel pieno rispetto di quanto previsto dalle norme della community. Per cui, nel 2021 sono stati eliminati 376,7 mila video, un numero simile a quello registratosi nel primo semestre del 2023, dove la cancellazione ha interessato 369 mila contenuti di questo genere; invece, nel 2022 è stata raggiunta una cifra pari a 615,5 mila video rimossi (Fig. 4.4).

*YouTube si è impegnato al fine di rimuovere i video volti a favorire l'hate speech, nel pieno rispetto di quanto previsto dalle norme della community. Per cui, nel 2021 sono stati eliminati 376,7 mila video, un numero simile a quello registratosi nel primo semestre del 2023, dove la cancellazione ha interessato 369 mila contenuti di questo genere; invece, nel 2022 è stata raggiunta una cifra pari a 615,5 mila video rimossi*

**Fig.4.4: Contenuti rimossi per incitamento all'odio da YouTube dal 2021 (in migliaia)**

Note: *I dati dell'anno 2023 fanno riferimento esclusivamente al primo semestre (gennaio-giugno)
Fonte: Google Rapporto sulla trasparenza



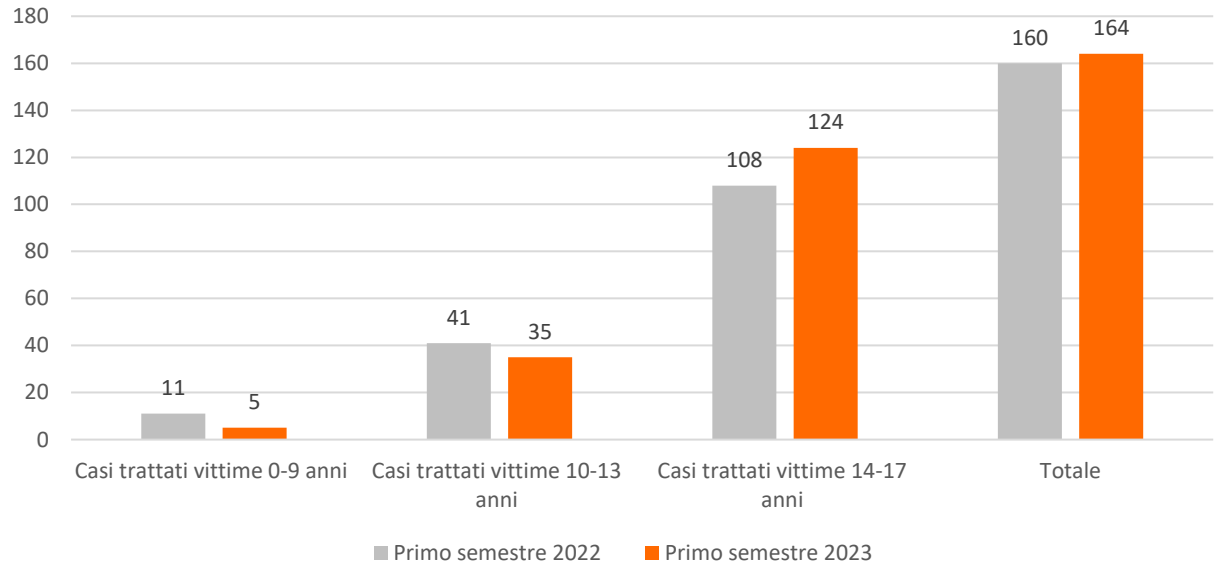

*L'uso problematico di internet si estrinseca anche mediante il fenomeno del cyberbullismo, che può essere descritto come qualsiasi comportamento messo in atto attraverso i media elettronici o digitali da individui e gruppi che comunicano messaggi ostili o aggressivi volti a causare danni o disagi agli altri*

L'uso problematico di internet si estrinseca anche mediante il fenomeno del cyberbullismo, che può essere descritto come qualsiasi comportamento messo in atto attraverso i media elettronici o digitali da individui e gruppi che comunicano messaggi ostili o aggressivi volti a causare danni o disagi agli altri. Nel primo semestre del 2023 sono stati trattati da parte della Polizia Postale 164 casi di cyberbullismo (Fig.4.5), presentando un andamento costante rispetto al medesimo periodo dell'anno precedente (160 casi trattati). Le denunce provengono principalmente da vittime con un'età tra i 14 e i 17 anni (108 nel primo semestre del 2022 e 124 nel primo semestre del 2023). Tra i soggetti che hanno dai 10 ai 13 anni la quota di denunce è più bassa (41 nel primo semestre del 2022 e 35 nel 2023) e un numero ancor più inferiore si osserva per le vittime fino a 9 anni (11 nel primo semestre del 2022 e 5 nel primo semestre del 2023).

*Nel primo semestre del 2023 sono stati trattati da parte della Polizia Postale 164 casi di cyberbullismo, presentando un andamento costante rispetto al medesimo periodo dell'anno precedente (160 casi trattati nel 2022)*

**Fig.4.5: Casi di cyberbullismo trattati dalla Polizia Postale (2022-2023)**

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

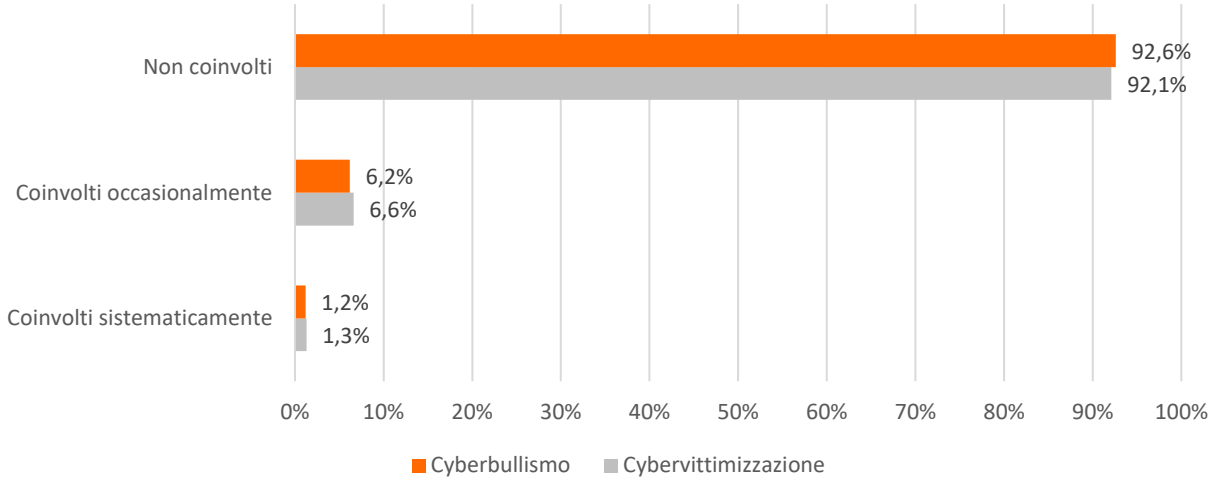



Il monitoraggio su bullismo e cyberbullismo effettuato dal Miur a maggio 2022, tramite un sondaggio condotto sulla piattaforma ELISA, ha analizzato la tendenza del cyberbullismo e della cybervittimizzazione durante l'anno scolastico 2021/22, coinvolgendo 232mila studenti di 757 scuole statali secondarie di secondo grado e 50.538 docenti di 2.100 Istituti scolastici statali, primari e secondari. In relazione al periodo di riferimento di 2/3 mesi precedenti alla rilevazione (Fig. 4.6), il 7,9% degli studenti e delle studentesse partecipanti ha dichiarato di aver subito episodi di cyberbullismo (6,6% occasionalmente e 1,3% sistematicamente), mentre il 7,4% afferma di aver preso parte attivamente a episodi di cyberbullismo (6,2% occasionalmente e 1,2% sistematicamente).

*Il 7,9% degli studenti e delle studentesse partecipanti ha dichiarato di aver subito episodi di cyberbullismo (6,6% occasionalmente e 1,3% sistematicamente), mentre il 7,4% afferma di aver preso parte attivamente a episodi di cyberbullismo (6,2% occasionalmente e 1,2% sistematicamente)*

**Fig.4.6: Coinvolgimento degli studenti in fenomeni di cyberbullismo e cybervittimizzazione**

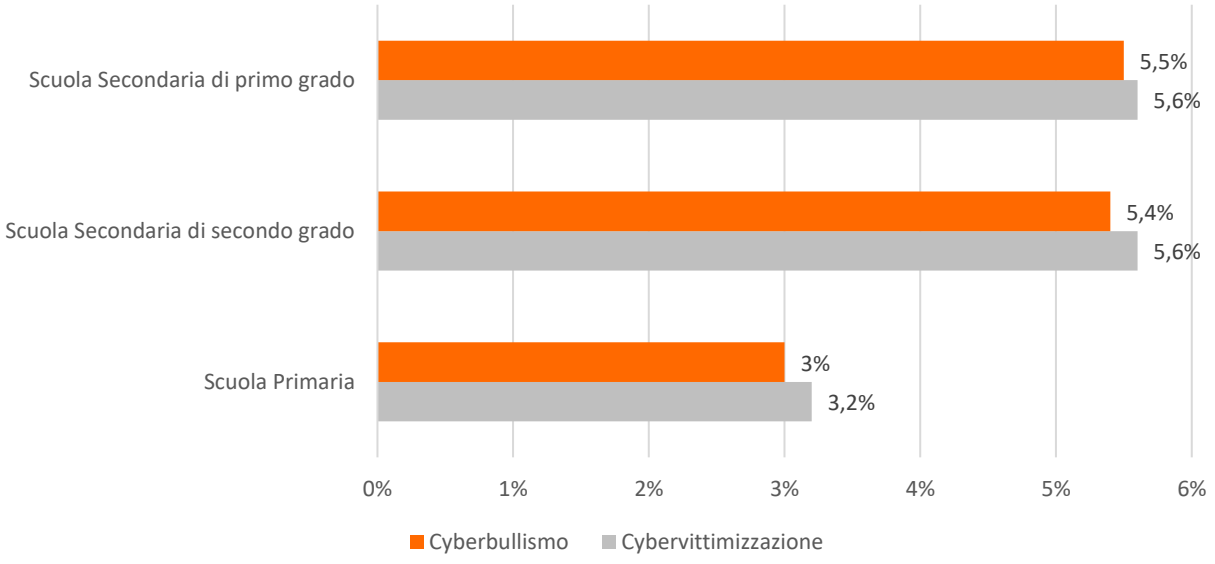
Fonte: Piattaforma Elisa, Monitoraggio del bullismo e del cyberbullismo a.s. 2021/2022




Dinanzi a queste risultanze emerge però una rilevante differenza tra la percezione degli studenti e quella dei docenti rispetto alla diffusione dei due fenomeni (Fig. 4.7). Nelle scuole secondarie di secondo grado, i docenti stimano che la percentuale di studenti e studentesse coinvolte in episodi di cyberbullismo e cybervittimizzazione sia rispettivamente pari al 5,4% e 5,6%, poco scostante da quella delle scuole secondarie di primo grado, dove si riscontra una percentuale del 5,5% e del 5,6%. Diversamente, tali eventi risultano più sporadici agli occhi degli insegnanti nelle scuole primarie, dove si considerano tra i soggetti attivi degli atti di cyberbullismo il 3% degli studenti, mentre le vittime costituirebbero il 3,2% del target.

**Fig.4.7: Percezione dei docenti rispetto ai fenomeni del cyberbullismo e della cybervittimizzazione**

Fonte: Piattaforma Elisa, Monitoraggio del bullismo e del cyberbullismo a.s. 2021/2022



In virtù dell'utilizzo sempre più frequente di Internet per scopi informativi e formativi, tra i pericoli della rete non va sottovalutato quello della diffusione di fake news, volte a concretizzare pratiche di disinformazione online. Nella comunicazione del 2020 sull'European democracy action plan, l'Unione Europea ha chiarito che con il termine disinformazione si fa riferimento più nello specifico alla proliferazione di "un contenuto falso o fuorviante, diffuso con l'intento di ingannare o ottenere un guadagno economico e che può provocare danni pubblici". Si tratta di una pratica che incide sulla vittima manipolando il suo lato razionale.

Il report "Public opinion in the European Union" di Eurobarometer evidenzia che il 64% degli italiani dichiara di imbattersi spesso in notizie false, le quali per il 39% di detti rispondenti sono difficili da identificare, mentre per il 57% degli italiani non appare complicato riconoscere un atto di disinformazione, per cui il 32% del campione afferma di non essere solito entrare a contatto con fake news. Il dato nazionale è inferiore alla media UE, dove il 69% dei soggetti coinvolti ha frequentemente esperienza con notizie false, mentre il 61% le reputa di agevole individuazione (Tab.4.1).

**Tab.4.1: La disinformazione in Italia e in UE27**

Fonte: Standard Eurobarometer 98, Public opinion in the European Union, Winter 2022-2023

| | | Media UE | Italia |
|---|---|---|---|
| Ti imbatti spesso in notizie o informazioni che travisino la realtà o sono false? (in %) | Sono d'accordo | 69% | 64% |
| | Non sono d'accordo | 26% | 32% |
| Ritieni che sia facile identificare notizie o informazioni che travisino la realtà o sono false? (in %) | Sono d'accordo | 61% | 57% |
| | Non sono d'accordo | 34% | 39% |

*Il report "Public opinion in the European Union" di Eurobarometer evidenzia che il 64% degli italiani dichiara di imbattersi spesso in notizie false, le quali per il 39% di detti rispondenti sono difficili da identificare, mentre per il 57% degli italiani non appare complicato riconoscere un atto di disinformazione, per cui il 32% del campione afferma di non essere solito entrare a contatto con fake news*

D'altro canto, l'esistenza di fake news è percepita come un problema per il 79% della popolazione italiana, quota superiore rispetto alla media dei Paesi UE (76%); i soggetti che valutano la disinformazione come un fattore negativo impattante sulla democrazia raggiungono l'82% in Italia e l'81% nell'UE (Tab. 4.2).

**Tab.4.2: I problemi derivanti dalla disinformazione in Italia e in UE27**

Fonte: Standard Eurobarometer 98, Public opinion in the European Union, Winter 2022-2023

| | | Media UE | Italia |
|---|---|---|---|
| L'esistenza di notizie o informazioni che travisino la realtà o sono false rappresenta un problema nel tuo Paese? (in %) | Sono d'accordo | 76% | 79% |
| | Non sono d'accordo | 18% | 18% |
| L'esistenza di notizie o informazioni che travisino la realtà o sono false è un problema per la democrazia in generale (in %) | Sono d'accordo | 81% | 82% |
| | Non sono d'accordo | 14% | 15% |

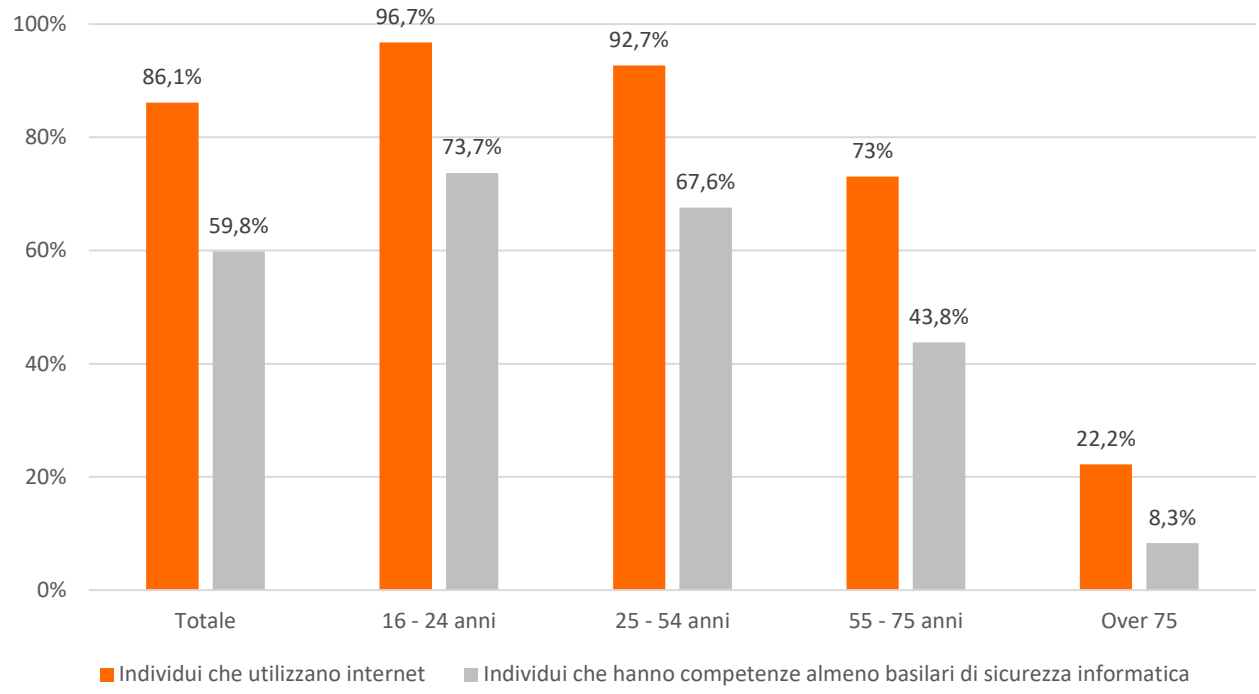
L'utilizzo inconsapevole della rete, l'inadeguata gestione delle password, l'incapacità di distinguere tentativi di *phishing* tramite e-mail e l'assenza di policy adeguate e aggiornate, rappresentano elementi attrattivi per i cybercriminali. Infatti, lo *human factor* ad oggi rientra tra le maggiori cause di attacchi informatici soprattutto in virtù del fatto che, 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, rileva che solo il 59,8% dei cittadini ha competenze almeno basilari in materia di sicurezza informatica*

L'analisi dei dati forniti da Eurostat, con riferimento all'anno 2022 (Fig.4.8), rileva che solo il 59,8% dei cittadini ha competenze almeno basilari in materia di sicurezza informatica. Dall'altro lato, analizzando la scomposizione per età, si evince una crescita direttamente proporzionale della quota di persone impreparate in cibersicurezza rispetto all'età anagrafica. Dai dati emerge come un italiano su quattro tra i 16 e i 54 anni abbia una carenza 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 del 26,3% rispetto al grado di competenze dichiarato, con un distacco maggiore nella fascia 16-24 anni.

**Fig.4.8: Quota di italiani che utilizzano internet e di individui che hanno almeno competenze basilari di sicurezza informatica (2022)**

Fonte: Eurostat

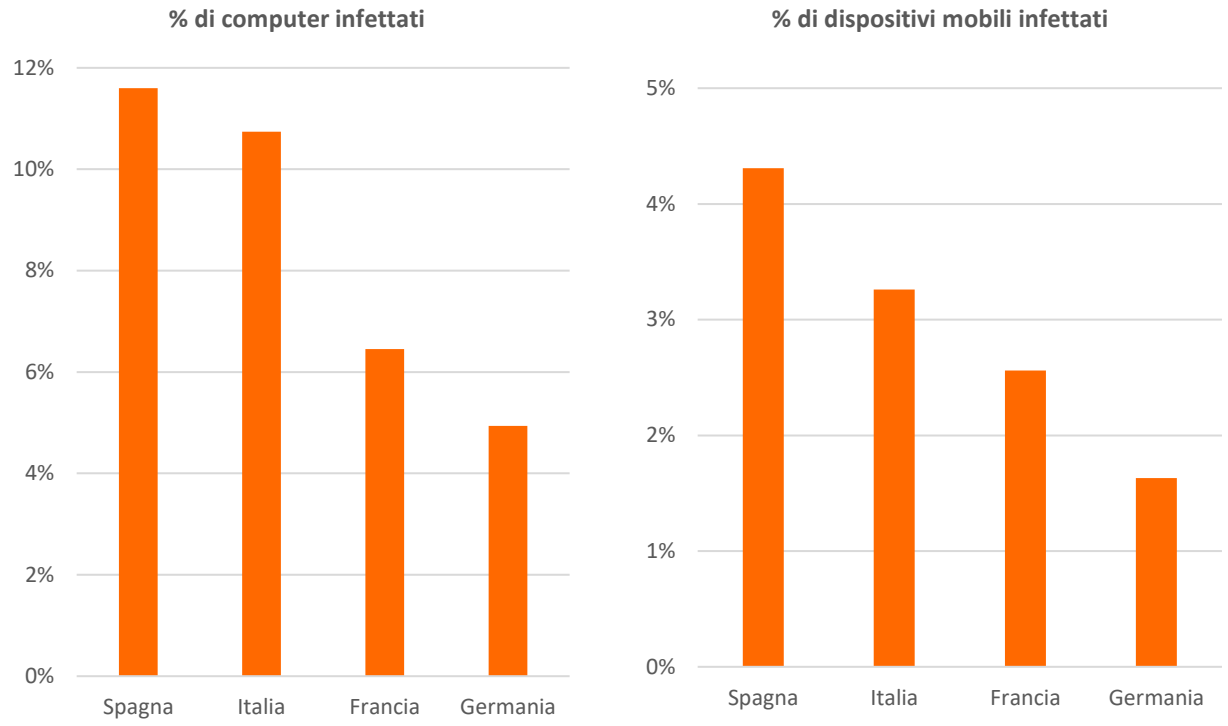



Se si osserva la quota di computer e dispositivi mobili infettati almeno una volta da *malware* nell'ambito del nostro Paese e nei principali partner europei (Fig. 4.9), i dati raccolti da Comparitech e aggiornati al 2022 vedono l'Italia in seconda posizione con il 10,7% di computer e il 3,3% di dispositivi mobili infettati, dietro solo alla Spagna (11,6% computer infettati; 4,3% dispositivi mobili infettati) e seguita invece da Francia (6,5% computer infettati; 2,6% dispositivi mobili infettati) e, infine, dalla Germania (4,9% computer infettati; 1,6% dispositivi mobili infettati).

*Se si osserva la quota di computer e dispositivi mobili infettati almeno una volta da malware nell'ambito del nostro Paese e nei principali partner europei, i dati raccolti da Comparitech e aggiornati al 2022 vedono l'Italia in seconda posizione con il 10,7% di computer e il 3,3% di dispositivi mobili infettati, dietro solo alla Spagna (11,6% computer infettati; 4,3% dispositivi mobili infettati)*

**Fig.4.9: Quota di computer e dispositivi mobili infettati almeno una volta da software malevoli (2022)**

Fonte: Comparitech

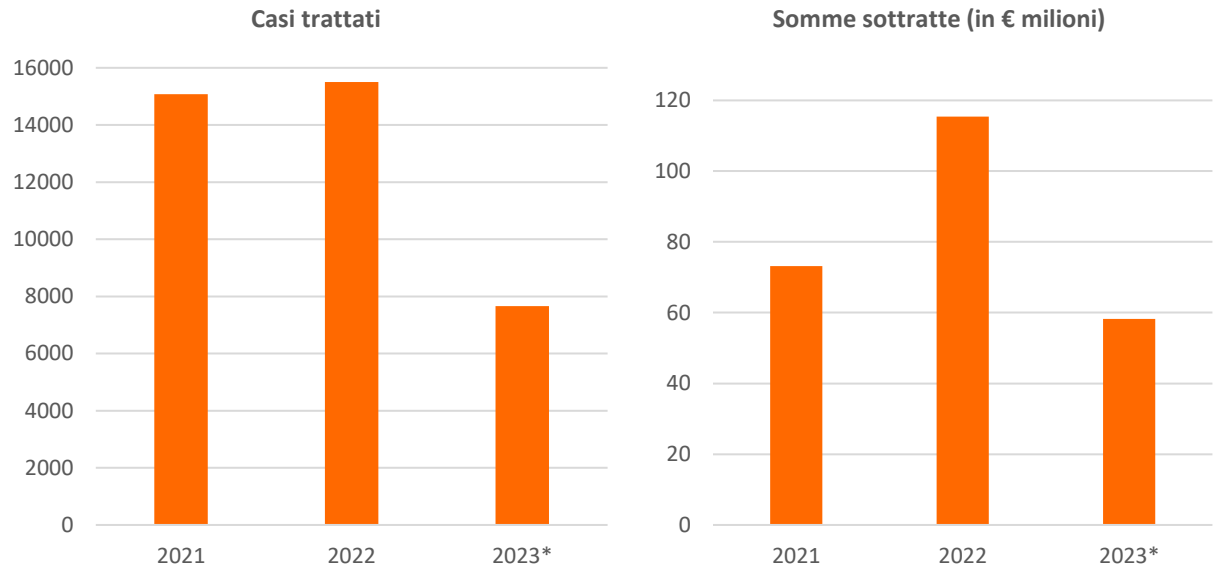



Le rilevazioni effettuate dalla Polizia Postale nell'ambito del resoconto delle rispettive attività, aggiornato al primo semestre del 2023 con i dati contenuti nell'ultimo rapporto Clusit (Fig.4.10), offrono una panoramica importante relativamente alle truffe online esperite in Italia. Sul punto, si evidenzia un incremento di 425 casi trattati nel 2022 rispetto all'anno precedente (+3%), per un totale complessivo di 15.508 truffe online registrate, che hanno comportato la sottrazione di oltre €115,4 milioni dalle vittime, segnando un aumento consistente del 58% rispetto al 2021. Peraltro, nel primo semestre del 2023 sono stati registrati nello specifico 7.661 episodi relativi a truffe informatiche, per un valore di somme sottratte pari a €58,2 milioni. Si tratta di risultati parziali che però sembrano in linea con il precedente periodo di rilevazione.

*Nel 2022 si evidenzia un aumento di truffe online rispetto all'anno precedente (+3%), per un totale complessivo di 15.508 truffe online registrate, che hanno comportato la sottrazione di oltre €115,4 milioni dalle vittime, segnando un aumento consistente del 58% rispetto al 2021. Peraltro, nel primo semestre del 2023 sono stati registrati nello specifico 7.661 episodi relativi a truffe informatiche, per un valore di somme sottratte pari a €58,2 milioni*

**Fig.4.10: Numero di casi trattati e somme sottratte con le truffe online in Italia**

Note: *I dati dell'anno 2023 fanno riferimento esclusivamente al primo semestre (gennaio-giugno).
Fonte: Resoconto attività 2022 della Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica; Clusit – Rapporto sulla Sicurezza Ict in Italia, ottobre 2023



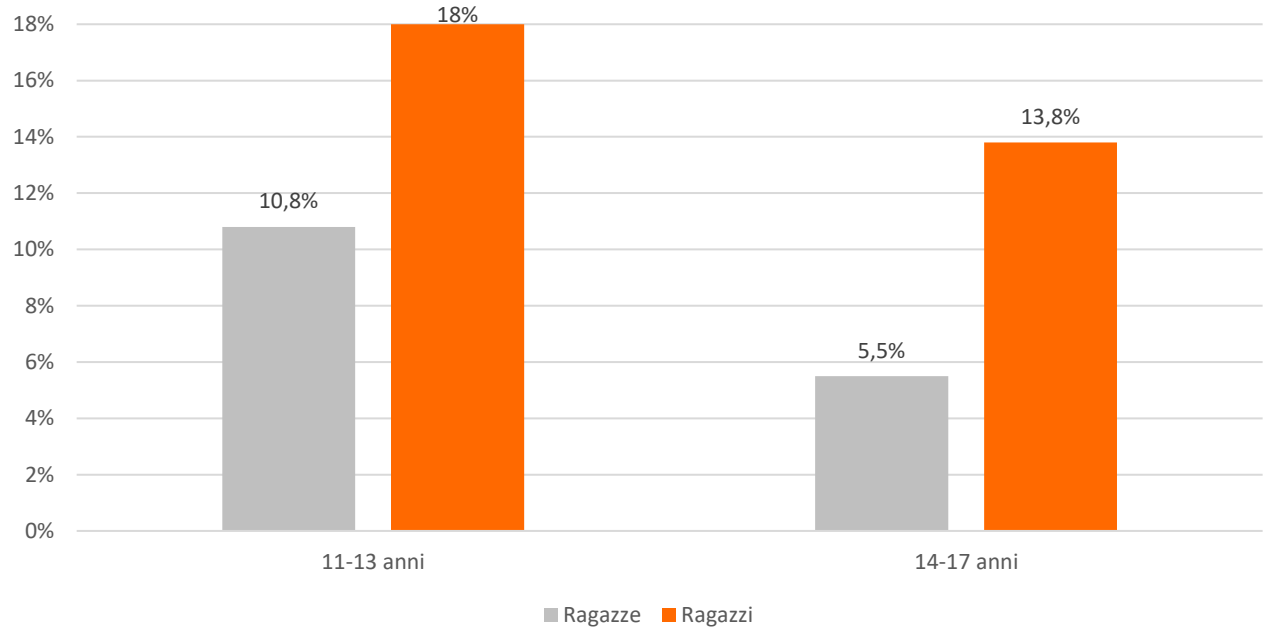

Un uso compulsivo della rete e delle nuove tecnologie da parte degli utenti può sfociare nel fenomeno della dipendenza da Internet. Tale terminologia descrive quei comportamenti nocivi online che provocano difficoltà nello svolgimento dell'attività lavorativa o scolastica, nei rapporti affettivi, interferendo con la normale pratica delle attività quotidiane. Attualmente, solo la dipendenza da gioco (*gaming disorder*) è stata inclusa nella classificazione delle malattie stilata dall'Organizzazione Mondiale della Sanità, ed è stata anche inserita nella Sezione III "Condizioni che necessitano di ulteriori studi" del DSM5 (*Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition*).

All'interno dello studio "Dipendenze comportamentali nella Generazione Z" dell'Istituto Superiore di Sanità (ISS), nell'autunno del 2022 sono stati intervistati più di 8.700 studenti, di cui circa 3.600 circa delle scuole secondarie di primo grado e 5.100 circa appartenenti alle secondarie di secondo grado (Fig.4.11). Le risultanze mostrano che il *gaming disorder* coinvolge il 12% degli studenti (circa 480.000). Il genere maschile è più colpito, con una percentuale che arriva al 18% negli studenti maschi dagli 11 ai 13 anni e al 13,8% in quelli tra i 14 e i 17 anni. Diversamente, il fenomeno interessa il 10,8% delle studentesse nella fascia 11-13 anni e il 5,5% in quella che va dai 14 ai 17 anni.

*Le risultanze mostrano che il gaming disorder coinvolge il 12% degli studenti (circa 480.000). Il genere maschile è più colpito, con una percentuale che arriva al 18% negli studenti maschi dagli 11 ai 13 anni e al 13,8% negli studenti tra i 14 e i 17 anni*

**Fig.4.11: Quota di adolescenti dipendenti da videogiochi per età e genere (2022)**

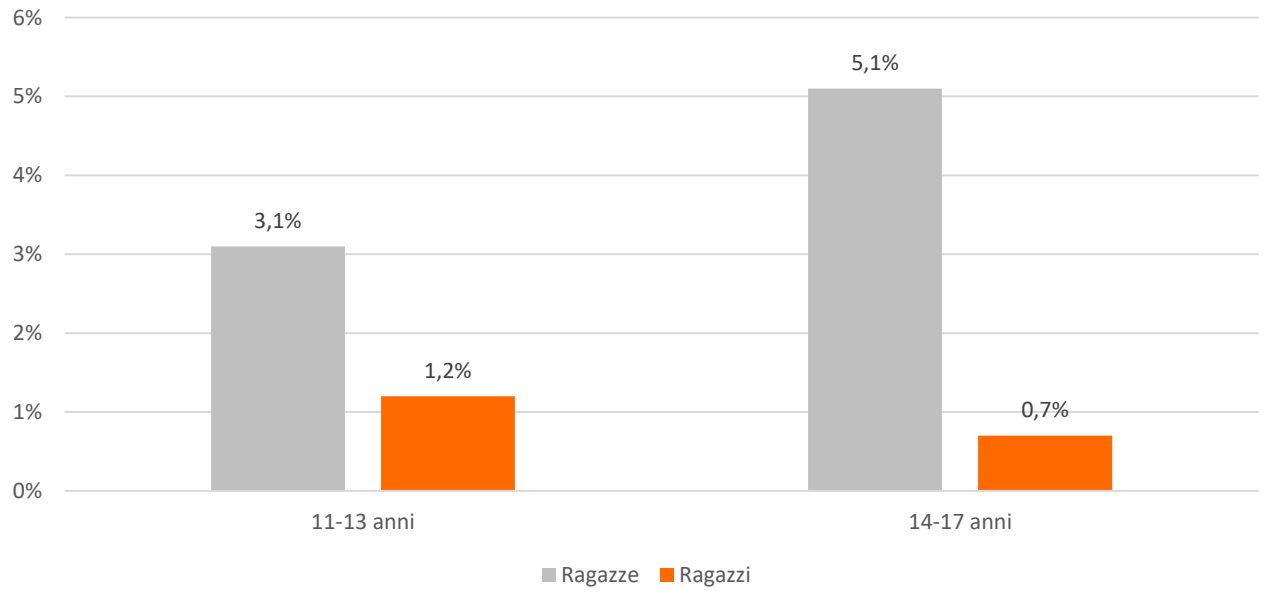
Fonte: ISS, "Dipendenze comportamentali nella Generazione Z", 2022




Anche la dipendenza da social media (Fig. 4.12) è diventata oggetto di attenzione per la comunità scientifica, ciò è inevitabile se si considera che il 2,5% del campione presenta caratteristiche compatibili con questo disturbo (circa 99.600 studenti), percentuale che raggiunge il 3,1% nelle studentesse di 11-13 anni e il 5,1% nella fascia 14-17 anni. Per quanto concerne i ragazzi, la dipendenza da social media interessa soltanto l'1,2% degli studenti dagli 11 ai 13 anni e lo 0,7% di coloro che hanno un'età compresa tra i 14 e i 17.

**Fig.4.12: Quota di adolescenti dipendenti da social media per età e genere (2022)**

Fonte: ISS, "Dipendenze comportamentali nella Generazione Z", 2022

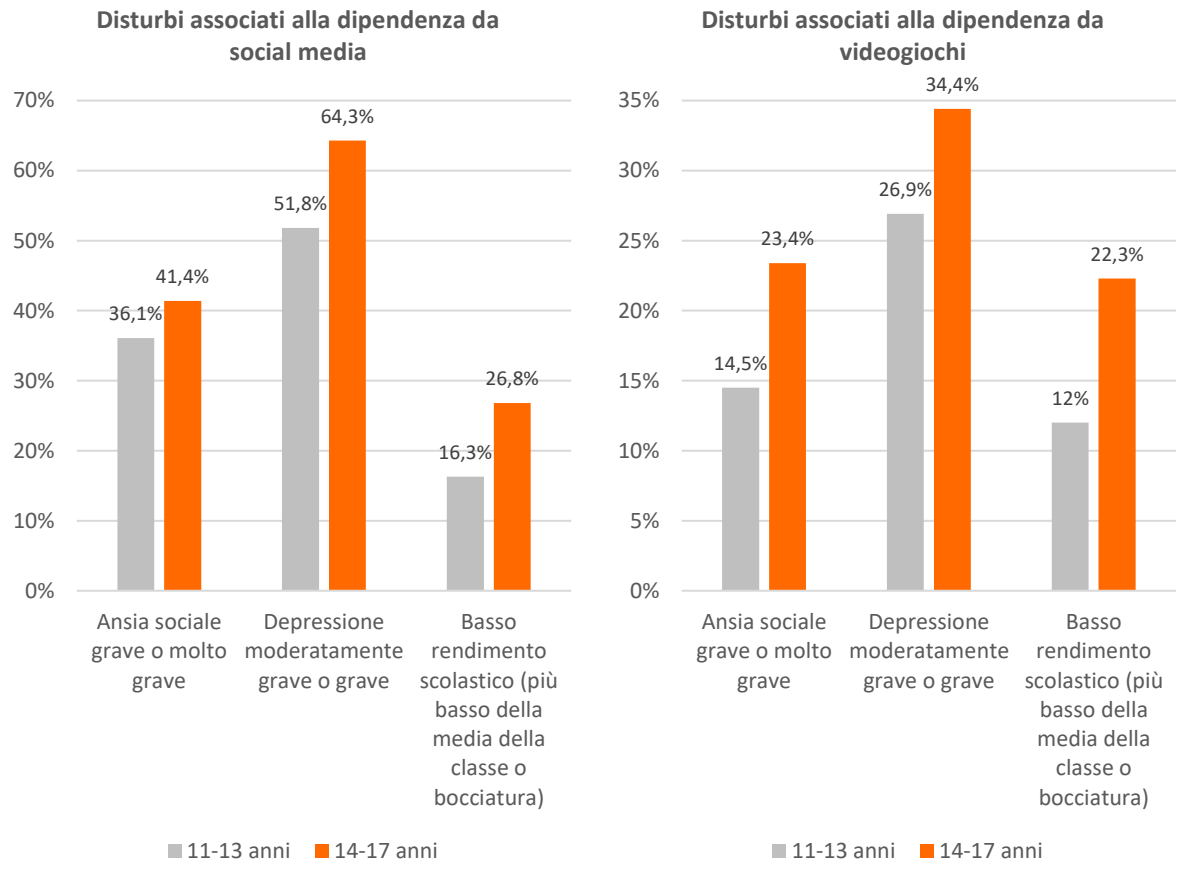


I principali disturbi legati alle suddette forme di dipendenza si sostanziano in (Fig. 4.13):

- ansia sociale grave o molto grave, di cui soffre il 36,1% di studenti e studentesse con dipendenza da social media tra gli 11 e i 13 anni e il 41,4% tra i 14 e i 17; il 14,5% nella fascia di età 11-13 e il 23,4% in quella 14-17 degli affetti da *gaming disorder*;
- depressione moderatamente grave o grave, con una percentuale del 51,8% (11-13 anni) e del 64,3% (14-17 anni) dei dipendenti da social media. Mentre tra i soggetti dipendenti da videogiochi si individua una percentuale del 26,9% (11-13 anni) e del 34,4% (14-17 anni);
- basso rendimento scolastico (più basso della media della classe o bocciatura), che si presenta come conseguenza della dipendenza da social media per il 16,3% (11-13 anni) e il 26,8% (14-17 anni) del campione e per il 12% (11-13 anni) e il 22,3% (14-17 anni) di coloro che dipendono dall'uso di videogame.

**Fig.4.13: Frequenza di disturbi associati alla dipendenza da social media e da videogiochi per età (2022)**

Fonte: ISS "Dipendenze comportamentali nella Generazione Z", 2022



# 4. LE POLICY IN MATERIA DI BENESSERE DIGITALE: GLI INDIRIZZI EUROPEI E NAZIONALI

La diffusione di Internet a livello globale, nonché del c.d. "*user generated content*" e dei social media, ha prodotto due effetti contrastanti: da un lato, ha accelerato la circolazione di informazioni migliorando e arricchendo le interazioni sociali, la condivisione di conoscenza e lo scambio di opinioni tra soggetti connessi; dall'altro, ha inciso particolarmente sulla sicurezza e sul benessere di chi popola la rete, mettendo a dura prova gli equilibri del cyberspazio e facendo emergere nuove sfide ed esigenze regolatorie.

Al fine di arginare tutti quei fenomeni che possono minare il raggiungimento di una condizione comune di *digital wellbeing* , la strategia digitale dell'Unione Europea si è basata sull'adozione di un modello definito di "*public-private cooperation and co-optation*", che affida alle imprese che offrono servizi di condivisione di contenuti online la competenza nella regolamentazione dei servizi digitali, legittimando una forma di controllo e censura privata non sottoposta ad una previa valutazione parlamentare, amministrativa e giudiziaria, prevedendo allo stesso tempo una serie di obblighi a cui gli operatori devono rigorosamente sottostare. Lo scopo è quello di tutelare la sicurezza dei cittadini della rete e, contemporaneamente, salvaguardarne diritti e libertà fondamentali, tra cui quella di espressione. Tale approccio trova piena rappresentazione nel recente *Digital services package*, costituito dal *Digital Services Act* (DSA) e dal *Digital Markets Act* (DMA), di cui si parlerà più approfonditamente nel prossimo paragrafo.

*Tale approccio trova piena espressione nel recente Digital services package, costituito dal Digital Services Act (DSA) e dal Digital Markets Act (DMA), volto a regolare i servizi digitali inserendosi nel quadro della Strategia digitale dell'Unione Europea*

Ripercorrendo i passi del legislatore comunitario, una prima iniziativa volta a regolare il settore dei servizi digitali è rivista nella Direttiva n. 31/2000 inerente taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno, anche detta "Direttiva sul commercio elettronico o Direttiva *e-commerce*". A norma del considerando n. 8, essa "*si prefigge di creare un quadro giuridico inteso ad assicurare la libera circolazione dei servizi della società dell'informazione tra gli Stati membri, e non di armonizzare il settore del diritto penale in quanto tale*". In particolare, gli artt. 14 e 15, escludono la responsabilità dei provider di servizi online per *user generated content*, quando non siano effettivamente a conoscenza dell'illiceità e se, appurata quest'ultima, siano intervenuti immediatamente per rimuovere tali informazioni. Peraltro, la normativa non impone né un obbligo generale di sorveglianza sui dati che i provider trasmettono e memorizzano, né previsioni che prescrivano la ricerca attiva di fatti e circostanze che indichino la presenza di attività illecite. Nel 2010, la Corte di giustizia[4] ha chiarito più approfonditamente che suddetta esenzione da responsabilità deve essere applicata ai prestatori di servizi di *hosting* che non abbiano giocato alcun ruolo attivo sui dati caricati dagli

[4] *Sentenza della Corte (grande sezione) del 23 marzo 2010. Google France SARL e Google Inc. contro Louis Vuitton Malletier SA (C-236/08), Google France SARL contro Viaticum SA e Luteciel SARL (C-237/08) e Google France SARL contro Centre national de recherche en relations humaines (CNRRH) SARL e altri (C-238/08).*

utenti, ruolo che abbia consentito loro di conoscerne il contenuto materiale o di assumere il controllo dei medesimi, ad eccezione del caso in cui, essendo venuti a conoscenza della natura illecita di tali dati o dell'attività dell'utente, abbiano omesso di rimuoverli prontamente o disabilitarne l'accesso.

In tal modo, la direttiva *e-commerce* prevedeva limitatamente un obbligo per gli Stati di imporre alle società dell'informazione la rimozione di determinati contenuti per l'esclusione della loro responsabilità, ponendosi come principale punto di riferimento la necessità di creare un mercato dei servizi digitali libero. Va però considerato che, in virtù del ruolo sempre più significativo che le imprese in questione hanno assunto nell'odierno panorama economico e sociale, una simile disciplina è stata considerata insufficiente per inibire la diffusione dei contenuti illeciti, preferendo piuttosto l'adozione di un approccio che punti a una regolamentazione maggiormente specifica e settoriale, che ricorra all'impiego di atti di *soft law*, come accade nel caso dei codici di condotta.

*In virtù del ruolo sempre più significativo che le imprese in questione hanno assunto nell'odierno panorama economico e sociale, una simile disciplina è stata considerata insufficiente per inibire la diffusione dei contenuti illeciti, preferendo piuttosto l'adozione di un approccio che punti a una regolamentazione maggiormente specifica e settoriale, che ricorra all'impiego di atti di soft law, come accade nel caso dei codici di condotta*

Proprio sulla scia di quanto detto, il 31 maggio 2016 la Commissione europea ha promosso, in applicazione della decisione quadro 2008/913/GAI e dell'art. 16 della direttiva *e-commerce*, un Codice di condotta per il contrasto all'illecito incitamento all'*hate speech*, al quale hanno aderito i principali operatori privati di servizi online (tra cui Google, Instagram e Facebook). Il codice esorta le imprese aderenti a predisporre procedimenti di esame delle segnalazioni relative a discorsi d'odio che siano chiari ed efficaci e che possano condurre alla rimozione tempestiva dei contenuti illegittimi, oltre a dotarsi di linee guida che vietino la promozione e l'istigazione alla violenza e alla condotta odiosa, ad esaminare le richieste di rimozione nel rispetto delle linee guida adottate e delle normativa di recepimento della suddetta decisione quadro, mediante gruppi di lavoro a ciò specificamente deputati, e di far ciò entro 24 ore dalla conoscenza dell' illecito.

Successivamente, il 7 novembre 2022 la Commissione europea ha pubblicato i risultati della valutazione annuale del suddetto codice, da cui si evince che il numero di notifiche esaminate dalle società entro 24 ore è diminuito rispetto alle ultime due edizioni del monitoraggio, passando dal 90,4 % nel 2020, all'81 % nel 2021 e al 64,4 % nel 2022. In particolare, si rileva una quota del 69,6% dei contenuti che incitano violenza contro gruppi specifici, che scende al 63,6% per i contenuti pericolosi, mentre nel 59,3% dei casi vi è stata la cancellazione di immagini o nomi diffamatori, mostrando un andamento positivo nella prontezza di intervento delle piattaforme considerate. Inoltre, si è registrato un miglioramento dei *feedback* forniti agli utenti rispetto al 2021, soprattutto per TikTok e Instagram.

L'11 ottobre scorso la Commissione europea, nell'ambito del gruppo ad alto livello sulla lotta contro l'incitamento all'odio e i crimini d'odio e di intolleranza, ha discusso insieme ai firmatari del

codice, alle autorità nazionali e alle organizzazioni della società civile le previsioni del prossimo "Codice di Condotta", che verrà elaborato in osservanza della disciplina comunitaria sui servizi digitali. Tale atto rappresenterà uno strumento reattivo operante allo scopo di rimuovere i contenuti illeciti e incoraggiare le piattaforme online a rafforzare la prevenzione e ad anticipare le minacce che affliggono e limitano l'esperienza degli utenti.

*L'11 ottobre 2023 la Commissione europea, nell'ambito del gruppo ad alto livello sulla lotta contro l'incitamento all'odio e i crimini d'odio e di intolleranza, ha discusso insieme ai firmatari del codice, alle autorità nazionali e alle organizzazioni della società civile le previsioni del prossimo "Codice di Condotta"*

Altro profilo di rilievo per l'UE nell'ambito del benessere digitale è quello del contrasto alla diffusione online di fake news. Difatti, nell'ottobre 2018 i rappresentanti delle piattaforme online, delle principali imprese tecnologiche e degli operatori del settore pubblicitario hanno concordato il Codice di buone pratiche sulla disinformazione[5]. Questo ha rappresentato una novità a livello mondiale, riconoscendo norme di autoregolamentazione per combattere la disinformazione. Il Codice auspicava il conseguimento degli obiettivi espressi nella comunicazione della Commissione presentata nell'aprile 2018, stabilendo 21 impegni divisi in cinque aree, tra cui: permettere alla comunità di ricerca di accedere ai dati delle piattaforme per monitorare la disinformazione online attraverso modalità conformi alle norme sulla privacy; aumentare la trasparenza della pubblicità politica; interrompere le entrate pubblicitarie di determinati account e siti Web che diffondono disinformazione; affrontare la questione degli account falsi e dei bot online; facilitare l'accesso alle fonti d'informazione, migliorando la visibilità dei contenuti autorevoli, e rendere più facile la segnalazione di notizie false.

*Nell'ottobre 2018 i rappresentanti delle piattaforme online, delle principali imprese tecnologiche e degli operatori del settore pubblicitario hanno concordato il Codice di buone pratiche sulla disinformazione*

La Commissione europea ha eseguito una valutazione del suo primo periodo di attuazione e, nel maggio 2021, ha pubblicato orientamenti dettagliati per rimediare alle carenze del Codice del 2018, allo scopo di aumentare la sua efficacia. Successivamente, a seguito del processo di revisione avviato nel giugno 2021, è stato firmato da 34 soggetti aderenti e presentato, in data 16 giugno 2022, il Codice di Condotta Rafforzato sulla disinformazione. Quest'ultimo contiene 44 impegni e 128 misure specifiche per mettere in atto strategie di trasparenza che permettano di proteggere gli utenti mediante strumenti avanzati per riconoscere, comprendere e segnalare la disinformazione; ampliare la copertura della verifica dei fatti in tutti gli Stati membri e le lingue dell'UE; istituire una *task force* permanente composta da rappresentanti dei firmatari, il gruppo dei regolatori europei per i servizi di media audiovisivi, l'Osservatorio europeo dei media digitali e

[5] *I firmatari del codice furono le piattaforme online Facebook, Google, Twitter e Mozilla, nonché inserzionisti e altri operatori del settore pubblicitario. Microsoft ha aderito nel maggio 2019, mentre TikTok ha firmato il codice nel giugno 2020.*

il Servizio europeo per l'azione esterna; prevedere un quadro di monitoraggio rafforzato basato su elementi di rendicontazione qualitativa e indicatori a livello di servizio che misurano l'efficacia della sua attuazione da parte soprattutto delle "piattaforme online molto grandi" a norma del *DSA,* per cui la violazione degli obblighi assunti da tali piattaforme nell'ambito del presente Codice di Condotta possono integrare le gravose sanzioni previste dalla normativa sui servizi digitali; costituire un centro per la trasparenza che comunichi al pubblico le politiche messe in atto per adempiere agli impegni previsti.

*A seguito del processo di revisione avviato nel giugno 2021, è stato firmato da 34 soggetti aderenti e presentato, in data 16 giugno 2022, il Codice di Condotta Rafforzato sulla disinformazione*

Il cyberspazio è divenuto un palcoscenico particolarmente attrattivo anche per le organizzazioni criminali, che ad oggi utilizzano Internet per preparare o compiere reati, coinvolgendo utenti comuni grazie all'efficacia della comunicazione e alla forte persuasività della propaganda online. Per tale ragione, le istituzioni europee hanno adottato, nell'aprile 2021, il Reg. n. 784 il cui contenuto bersaglia la diffusione di registrazioni audio, video, comprese le trasmissioni in streaming, immagini, testi che impartiscono istruzioni su come commettere reati, specificamente consigliandone i metodi e le tecniche, o che istigano a prendere parte ad organizzazioni terroristiche. L'art. 3, co.3 3, prevede che: "*I prestatori di servizi di hosting rimuovono i contenuti terroristici o disabilitano l'accesso (…) in tutti gli Stati membri il prima possibile e in ogni caso entro un'ora dal ricevimento dell'ordine di rimozione*". L'ambito di applicazione del regolamento si estende a tutti i prestatori che offrono servizi nell'UE, a prescindere dal fatto che il loro stabilimento principale sia situato o meno in uno Stato dell'Unione[6]. Per ragioni di tempestività necessaria per assicurare l'efficacia dell'intervento, il Regolamento impone di eseguire l'ordine il prima possibile o, in ogni caso, entro un'ora dal ricevimento dall'ordine di rimozione[7]. I prestatori di servizi di hosting conservano i contenuti terroristici rimossi o il cui accesso è stato disabilitato per un periodo di almeno sei mesi, salvo specifiche proroghe previste dall'autorità competente o da un organo giurisdizionale, legittimate da un criterio di necessarietà e ammissibili per tutto il tempo richiesto per il procedimento di ricorso amministrativo o giurisdizionale in corso[8]. Inoltre, a norma dell'art. 9 è riconosciuta la possibilità agli ISP e al fornitore dei contenuti di impugnare la decisione dinanzi all'Autorità Giudiziaria per verificare la legittimità dell'ordine di rimozione e tutelare la libertà di espressione e di informazione. La lettura attenta del regolamento permette di comprendere l'importanza affidata alla collaborazione volontaria tra gli Stati membri e i prestatori di servizi di hosting, sottolineando la conformità all'approccio adottato dalla Commissione europea, a partire dal 2010, nell'ambito della strategia antiterrorismo, ossia agevolare forme di partenariato pubblico-privato per ridurre la diffusione di contenuti illeciti.

Va inoltre specificata l'importanza in questo contesto della disciplina sulla regolamentazione dell'intelligenza artificiale (IA) delineata all'interno dell'*Artificial Intelligence Act*[9], il quale si

[6] *Art. 4. Reg. UE 784/2021.*
[7] *Ivi, art. 3, co. 3.*
[8] *Ivi, art. 13.*
[9] *A seguito della proposta presentata il 21 aprile 2021 dalla Commissione europea, il 14 giugno 2023 il Parlamento europeo ha deliberato a favore dell'Artificial Intelligence Act, che avrà l'obiettivo di regolamentare l'IA nella piena osservanza dei diritti e dei valori dell'Unione Europea. L'approvazione definitiva di tale proposta di Regolamento dovrebbe avvenire entro fine 2023 a seguito della conclusione delle trattative tra il Consiglio, il Parlamento e la Commissione europea (il c.d. trilogo).*

caratterizza per l'adozione di un approccio basato sul rischio (*risk based*), stabilendo obblighi per i fornitori e gli utenti di IA in base al livello di rischio da essa producibile[10]. Ciò rileva se si considera che il procedimento di rimozione dei contenuti illeciti avviene mediante algoritmi utilizzati in prima battuta per individuare immagini, conversazioni, video che appaiono come potenzialmente illeciti e, in seguito, per la loro rimozione in ottemperanza alle policy interne alle singole società tecnologiche.

*Il procedimento di rimozione dei contenuti illeciti avviene mediante algoritmi utilizzati in prima battuta per individuare immagini, conversazioni, video che appaiono come potenzialmente illeciti e, in seguito, per la loro rimozione in ottemperanza alle policy interne alle singole società tecnologiche*

Come conseguenza della discriminazione online, il cyberbullismo appare un fenomeno sempre più diffuso, in quanto gli utenti mediante i social network e le app di messaggistica hanno l'opportunità di porre in essere atti di violenza nei confronti di soggetti fragili, tra cui i minori. In ambito nazionale la legge 29 maggio 2017, n. 71 ha previsto un sistema di enforcement nei confronti delle piattaforme digitali per intervenire prontamente sulla questione, offrendo un quadro normativo più specifico per regolamentare questa materia. L'art. 2 afferma che ciascun minore ultraquattordicenne, nonché ciascun genitore o soggetto esercente la responsabilità del minore, ha la possibilità di inoltrare al titolare del trattamento – secondo la definizione fornita dal GDPR – o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco di dati personali del minore. Se entro il termine di ventiquattro ore il soggetto responsabile non ha comunicato di avere assunto l'incarico di provvedere all'oscuramento, alla rimozione o al blocco richiesto, l'interessato può presentare la medesima istanza al Garante per la protezione dei dati personali che, entro quarantotto ore dalla sua ricezione, deve provvedere in osservanza della disciplina sulle decisioni di reclamo e sulle segnalazioni prevista dal Codice Privacy.

Nel 2017, il legislatore italiano ha emanato le "Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo", allo scopo di consentire ai dirigenti, ai docenti e agli operatori scolastici di comprendere, ridurre e contrastare i fenomeni negativi che colpiscono gli studenti, ricorrendo all'uso di strumenti e strategie efficaci. Tra queste, con l'aggiornamento del 2021, si è data enfasi alla creazione e al rafforzamento della piattaforma ELISA, che consente un percorso di formazione gratuita rivolto agli insegnanti designati come referenti per il cyberbullismo, affinché acquisiscano utili competenze psico-pedagogiche e sociali. In aggiunta, il 6 settembre scorso la Camera ha approvato il testo unificato delle proposte di legge 536, 891 e 910, intervenendo sulla legge n. 71/2017, incrementando le risorse a disposizione per campagne informative di sensibilizzazione e prevedendo l'adozione, da parte di ciascun istituto scolastico, di un codice interno per la prevenzione e il contrasto del bullismo e del cyberbullismo, nonché la predisposizione per gli istituti scolastici, da parte delle regioni, di servizi di sostegno psicologico. Fra l'altro, viene disposta l'implementazione del numero pubblico di emergenza 114 e l'obbligo di richiamare espressamente nei contratti con i fornitori di servizi di comunicazione elettronica le

[10] *Il Titolo II inerisce le pratiche di IA vietate seguendo l'approccio basato sul rischio e differenziando quest'ultimo in quattro categorie: 1) rischio inaccettabile; 2) rischio alto; 3) rischio limitato; 4) rischio basso o minimo.*

disposizioni in materia di responsabilità dei genitori per i danni cagionati dai figli minori e le norme del regolamento europeo in materia di servizi digitali.

*Il 6 settembre scorso la Camera ha approvato il testo unificato delle proposte di legge 536, 891 e 910, intervenendo sulla legge n. 71/2017*

## 4.1. La tutela dell'utente online tra *Digital Services Package* e GDPR

L'approccio dell'UE in tema di benessere digitale non è rimasto immutato nel tempo in quanto in virtù della perdita di efficacia delle misure di *soft law,* si è fatta viva la necessità di uniformare il quadro legislativo sui servizi digitali, allo scopo di garantire libertà e sicurezza a chi ne fruisce direttamente. Perciò, come precedentemente anticipato[11], la Commissione europea ha presentato nel dicembre 2020 il *Digital Services package*, ossia due proposte di regolamento inerenti la concorrenza equa dei mercati digitali (*Digital Markets Act*)[12] e il mercato unico dei servizi digitali (*Digital Services Act*)[13]. Gli atti sono entrati in vigore nel 2022 con applicazione, rispettivamente, dal 2 maggio 2023[14] e 17 febbraio 2024[15].

Il *Digital Markets Act* (DMA), in particolare, è uno strumento normativo che ha l'obiettivo di contrastare eventuali abusi di posizione dominante nei mercati digitali. Esso opera *ex ante*, in quanto regola condotte e obblighi prima che sia compiuto l'abuso, differenziandosi dalla normativa antitrust che agisce *ex post*, sanzionando solo dopo il comportamento di concorrenza sleale. La Commissione ha valutato come, attualmente, la dominanza di poche e grandi piattaforme nel mercato digitale determini una carenza di contendibilità dei mercati delle piattaforme, con una conseguente debolezza nella concorrenza e il verificarsi di pratiche commerciali scorrette[16]. Per cui, l'art. 1, par. 1 designa la finalità del DMA sostenendo che esso "*stabilisce norme armonizzate volte a garantire che i mercati nel settore digitale nei quali sono presenti gatekeeper (controllori dell'accesso) siano equi e contendibili in tutta l'Unione*". Quando si parla di *gatekeeper* si fa riferimento, come noto, alle VLoPs (*Very Large Online Platforms*) che per una serie di motivi quantitativi e qualitativi assumono tale qualifica. Tra i primi rientrano la copertura delle quote di mercato, il numero di utenti della piattaforma, il tempo di utilizzo per utente della stessa e i ricavi annuali; mentre, tra i secondi vanno considerati la capacità di fungere da intermediario tra la concorrenza e gli utenti, oltre che la capacità di gestire i dati degli stessi a scopi analitici per poter competere anche su mercati differenti. I tre parametri con cui questi fornitori di piattaforma di base vengono individuati sono: la dimensione dell'impresa, il controllo

[11] *Si v. supra, par. 4.*
[12] *Regolamento (UE) 2022/1925 del Parlamento Europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali).*
[13] *Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali).*
[14] *Articolo 54 «Entrata in vigore e applicazione» - «Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione Europea. Si applica a decorrere dal 2 maggio 2023. Tuttavia, l'articolo 3, paragrafi 6 e 7, e gli articoli 40, 46, 47, 48, 49 e 50 si applicano a decorrere dal 1° novembre 2022 e gli articoli 42 e 43 si applicano a decorrere dal 25 giugno 2023. Tuttavia, se la data del 25 giugno 2023 precede la data di applicazione di cui al secondo comma del presente articolo, l'applicazione degli articoli 42 e 43 è rimandata fino alla data di applicazione di cui al secondo comma».*
[15] *Articolo 93 «Entrata in vigore e applicazione» - «Il presente regolamento entra in vigore in ventesimo giorno successivo alla pubblicazione in Gazzetta ufficiale dell'Unione Europea. Si applica a decorrere dal 17 febbraio 2024. Tuttavia, l'articolo 24, paragrafi 2, 3 e 6, l'articolo 33, paragrafi da 3 a 6, l'articolo 37, paragrafo 7, l'articolo 40, paragrafo 13, l'articolo 43 e il capo IV, sezioni 4, 5 e 6, si applicano a decorrere dal 16 novembre 2022».*
[16] *Considerando n. 3, Regolamento (UE) 2022/1925.*

del *gateway* di accesso ai dati degli utenti e una posizione stabile sul mercato[17]. Questo processo consta di tre fasi: 1) la società verifica i requisiti quantitativi e deve comunicare l'esito dell'operazione eseguita alla Commissione; 2) quest'ultima, in base alle risultanze ottenute o all'avvio di indagini, designa il *gatekeeper*; 3) entro un termine di sei mesi da questa data, la società deve osservare le prescrizioni dettate dal DMA[18].
Inoltre, la Commissione può riconsiderare, modificare o revocare in qualsiasi momento, su richiesta o di propria iniziativa, la decisione adottata[19]. In aggiunta, attraverso una serie di norme vengono disciplinati gli obblighi affidati alle piattaforme, la sospensione degli stessi, l'esenzione dall'osservanza degli obblighi per motivi imperativi di interesse pubblico e una serie di poteri di controllo, indagine, sanzione e monitoraggio affidati alla Commissione. I vantaggi che potranno derivare dall'applicazione del Regolamento si sostanziano nella maggiore trasparenza rispetto ai meccanismi di funzionamento del mercato digitale e delle piattaforme, nella garanzia dell'interoperabilità con servizi di aziende di piccole dimensioni, nella maggiore libertà di scelta per i consumatori a cui verranno offerti servizi migliori a costi più concorrenziali.

*L'art. 1, par. 1 designa la finalità del DMA sostenendo che esso "stabilisce norme armonizzate volte a garantire che i mercati nel settore digitale nei quali sono presenti gatekeeper (controllori dell'accesso) siano equi e contendibili in tutta l'Unione"*

Il *Digital Services Act* (DSA), a norma dell'art. 1, par. 1, vuole "*contribuire al corretto funzionamento del mercato interno dei servizi intermediari stabilendo norme armonizzate per un ambiente online sicuro, prevedibile e affidabile che faciliti l'innovazione e in cui i diritti fondamentali sanciti dalla Carta, compreso il principio della protezione dei consumatori, siano tutelati in modo effettivo*". Tra gli aspetti principali dell'atto normativo in esame vi è l'obbligo per i prestatori di servizi di hosting di intervenire immediatamente per la rimozione o l'oscuramento di contenuti illeciti appena essi ne siano venuti a conoscenza. Nel suo testo, il Regolamento afferma l'esonero di responsabilità in capo agli intermediari digitali[20] per i contenuti online, l'assenza di obblighi di sorveglianza e accertamento attivo, imponendo obblighi di *due diligence*[21] e prevedendo regole[22] di attuazione, cooperazione, sanzione ed esecuzione volte a contrastare una serie di rischi riconosciuti nel dettato normativo.

Questi ultimi si rivedono: nella diffusione di contenuti illegali; negli effetti reali o prevedibili sull'esercizio dei diritti fondamentali, in particolare la dignità umana, la vita privata e familiare, la tutela dei dati personali, la libertà di espressione e informazione, la libertà e il pluralismo dei media, la non discriminazione; nei rischi derivanti dagli effetti negativi reali o prevedibili sui processi democratici, sul dibattito civico, sulla sicurezza pubblica; nei rischi per la salute pubblica derivanti dall'uso di piattaforme e motori di ricerca di grandi dimensioni[23].

[17] *Art. 3, Regolamento (UE) 2022/1925.*
[18] *Ibidem.*
[19] *Art. 4, Regolamento (UE) 2022/1925.*
[20] *Artt. 4-10, Regolamento (UE) 2022/2065.*
[21] *Artt. 11-48, Regolamento (UE) 2022/2065.*
[22] *Artt. 49-88, Regolamento (UE) 2022/2065.*
[23] *Artt. 34, 35; considerando nn. 3 e 4, Regolamento (UE) 2022/2065.*

*Il Regolamento afferma l'esonero di responsabilità in capo agli intermediari digitali per i contenuti online, l'assenza di obblighi di sorveglianza e accertamento attivo, imponendo obblighi di due diligence e prevedendo norme di attuazione, cooperazione, sanzione ed esecuzione volte a contrastare una serie di rischi riconosciuti nel dettato normativo*

Entro la data di entrata in vigore della normativa sui servizi digitali, gli Stati membri dovranno designare una o più Autorità Competenti incaricate della vigilanza dei fornitori di servizi intermediari e dell'esecuzione del DSA, l'Autorità potrà anche essere dichiarata *Digital Services Coordinator*, figura che sorveglia in maniera indipendente l'applicazione del DSA sottostando a doveri di trasparenza, tempestività, imparzialità e rendicontazione.
Tale organismo ha il compito di gestire i reclami contro i provider e di indagare sulla presenza di illeciti con pieno potere di ispezione. Una volta accertato l'illecito, il *Digital Services Coordinator* è tenuto a imporre la cessazione della violazione con sanzioni e penalità di mora, fino a chiedere alle autorità giudiziarie dello Stato la temporanea restrizione dell'accesso dei destinatari al servizio.
L'Autorità Competente e i Coordinatori dei servizi digitali cooperano tra loro e sono tenuti ad informare la Commissione delle operazioni svolte, soprattutto per evitare che la stessa condotta sia sanzionata più di una volta per la violazione degli obblighi stabiliti nel regolamento. Inoltre, è istituito il Comitato europeo per i servizi digitali**,** composto dai Coordinatori nazionali dei servizi digitali di tutti gli Stati membri e presieduto dalla Commissione europea, che supporta la direzione e la vigilanza delle grandi piattaforme, fornendo anche attività di consulenza. Ebbene, in Italia, con ben tre mesi di anticipo rispetto al termine del 17 febbraio 2024 fissato dal comma 3 dell'art. 49 per la designazione da parte dei singoli Stati membri, la scelta è caduta sull'Autorità per le garanzie nelle comunicazioni (AGCom) designata coordinatore dei servizi digitali con l'art. 15 del D.L. 23/2023 convertito con modificazioni dalla legge n. 159/23.

Le piattaforme online e i motori di ricerca hanno rivisto l'obbligo di pubblicare il proprio numero di utenti attivi entro il 17 febbraio 2023, al fine di essere riconosciuti dalla Commissione, in caso di quota superiore a 45 milioni (10 % della popolazione in Europa), con la definizione di VLOPs e VLOSEs (*Very Large Online Search Engines*). Inoltre, sono stati concessi quattro mesi di tempo a tali servizi per potersi conformare agli obblighi del DSA, tra cui appare fondamentale quello relativo all'esecuzione e alla trasmissione alla Commissione della valutazione annuale dei rischi.
A norma dell'art. 37 viene richiamata l'importanza degli *audit* indipendenti, che costituiscono strumenti fondamentali per verificare i rischi "sistemici" prodotti dagli algoritmi. Pertanto, il 20 ottobre scorso la Commissione ha adottato un regolamento delegato in cui vengono stabilite le fasi e i principi fondamentali da rispettare nell'esecuzione di tali operazioni di valutazione, l'atto sarà applicabile entro tre mesi dalla sua presentazione al Consiglio e al Parlamento, nel caso in cui questi non solleveranno obiezioni.

*Il 20 ottobre scorso la Commissione ha adottato un regolamento delegato in cui vengono stabilite le fasi e i principi fondamentali da rispettare nell'esecuzione di tali operazioni di valutazione*

In caso di violazioni del *Digital Services Act*, l'art. 52 prevede che le sanzioni possano ammontare al 6% del fatturato annuo totale e i destinatari dei servizi digitali possano richiedere un risarcimento per i danni o le perdite subite. Tra i motivi sanzionatori vi sono anche l'aver prestato informazioni scorrette, incomplete o fuorvianti; la mancata rettifica delle informazioni presentate e il mancato assoggettamento ai sopralluoghi, per cui in tali circostanze i provvedimenti dovranno essere inferiori all'1% del reddito o del fatturato annuo. Peraltro, gli Stati Membri provvedono in caso di penalità di mora affinché l'importo massimo giornaliero sia pari al 5 % del fatturato giornaliero medio mondiale o del reddito del fornitore di servizi intermediari interessato nell'esercizio finanziario precedente. In base a quanto fin qui esposto, dalla lettura del DSA risulta evidente l'intento dell'UE che, mediante questa normativa, mette in pratica il tentativo di bilanciare sia l'interesse legato alla tutela dei diritti fondamentali e del principio democratico, tangibile dall'imposizione di ordini di rimozione e di obblighi di *due diligence*, sia di salvaguardare la libera iniziativa e lo sviluppo economico, grazie all'esonero delle responsabilità e all'assenza degli obblighi di sorveglianza o accertamento attivo.

Un profilo critico da non sottovalutare è quello inerente all'impegno da parte delle piattaforme digitali di dati personali resi pubblici dall'utente. Difatti, l'accessibilità del dato può esporlo a numerose finalità di trattamento come l'estrazione, la diffusione, l'utilizzo per scopi diversi ed ulteriori o, ancor di più, per ragioni di *marketing*. Va sottolineato che per definire un trattamento lecito, sarà necessario tener conto del regime delle basi giuridiche individuato all'interno del Reg. 679/ 2016 (GDPR), il quale, nel caso di specie, potrebbe vedere applicata sia la condizione di liceità dell'adempimento di un obbligo legale cui è soggetto il titolare del trattamento ai sensi dell'art. 6, par. 1, lett. c (si pensi agli albi professionali), sia la necessarietà per l'esecuzione del contratto di servizio ai sensi dell'art. 6 par. 1, lett. b (in caso di iscrizione ad un social network), o anche il consenso espresso dall'interessato rispetto alle finalità predisposte, inteso come qualsiasi manifestazione di volontà libera, specifica, informata ed inequivocabile con la quale egli manifesta il proprio assenso mediante dichiarazione o azione positiva. Peraltro, il trattamento deve avvenire nel pieno rispetto del principio di limitazione delle finalità, indicato all'art. 5, par. 1, lett. b, poiché il consenso può riferirsi solo agli scopi determinati, espliciti, legittimi che siano stati dichiarati. In tale contesto, un ruolo fondamentale è affidato all'informativa, la quale deve essere presentata dalla piattaforma online all'interessato in forma coincisa, chiara, facilmente accessibile ed intellegibile, in particolare quando è rivolta ai minori. Inoltre, deve essere resa per iscritto o con altri mezzi, difatti, è ammessa la possibilità di pubblicare l'informativa su un sito web, inserendo il collegamento ipertestuale alla pagina di riferimento.

In aggiunta, l'art. 22 tutela gli interessati vietando forme di trattamento automatizzato di dati personali che possano produrre effetti giuridici che li riguardino o che incidano in modo analogo significativamente sulla loro persona, compresa la profilazione, ossia qualsiasi forma di trattamento volto a valutare determinati aspetti personali relativi ad un individuo, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica. Ciò appare rilevante se si considera che da queste analisi, rafforzate mediante l'uso di sistemi di IA, le aziende di grandi dimensioni possano accrescere il loro potere sui mercati digitali, fornendo all'utente messaggi ed esperienze personalizzate, che lo fidelizzano in cambio di una moneta di scambio spesso poco visibile, ma molto preziosa: il dato personale.

## 4.2. Il rafforzamento delle tutele a favore dei minori: il decreto Caivano

La tutela dei minori online rappresenta uno degli ambiti di maggior interesse per i policy maker e le autorità di regolamentazione nazionali. Sono ampie e variegate, infatti, le iniziative che si sono succedute anche sulla spinta della disciplina europea, tra cui spicca, per l'attualità e la rilevanza del dibattito che l'ha accompagnata, l'adozione del D.L. n. 123/23 convertito dalla legge n. 159/23 (c.d. "decreto Caivano") nell'immediatezza delle efferate violenze subite dalle minori di Caivano.

Si tratta di un'iniziativa importante che fissa, tra l'altro, regole specifiche ed individua strumenti tesi a garantire la sicurezza dei minori online. In particolare, il Capo IV (art. 13 e ss.) detta disposizioni per la sicurezza dei minori in ambito digitale e disciplina lo strumento del parental control, fissando l'obbligo per i produttori di dispositivi di comunicazione elettronica - definizione che include smartphone, computer, tablet e, ove compatibili, console di videogiochi, e altri possibili oggetti connessi che consentano l'accesso ai browser, come televisioni, orologi, assistenti vocali, sistemi di domotica e di IoT - di garantire sistemi operativi che consentano l'utilizzo e includano la disponibilità di applicazioni di controllo parentale, di informare gli utenti sulla possibilità e l'importanza di utilizzare applicazioni di controllo parentale (anche tramite l'inserimento nelle confezioni di vendita di uno specifico foglio illustrativo o tramite l'apposizione sulla confezione di uno specifico supporto adesivo) e prescrive il principio di gratuità per il servizio di attivazione delle applicazioni di controllo parentale. A ciò si aggiunge, nel frattempo, l'obbligo per i fornitori di servizi di comunicazione elettronica di assicurare la disponibilità di applicazioni di controllo parentale nell'ambito dei contratti di fornitura nei servizi di comunicazione elettronica. Un obbligo di implementazione di sistemi di controllo parentale a carico degli operatori di TLC era stato peraltro già fissato dall'art. 7-bis del d.l. 28/2020, in attuazione del quale AGCom ha adottato la delibera 9/23/CONS recante linee guida in materia di "sistemi di protezione dei minori dai rischi del cyberspazio".

*Un obbligo di implementazione di sistemi di controllo parentale a carico degli operatori di TLC era stato peraltro già fissato dall'art. 7-bis del d.l. 28/2020, in attuazione del quale AGCom ha adottato la delibera 9/23/CONS recante linee guida in materia di "sistemi di protezione dei minori dai rischi del cyberspazio"*

Specifici obblighi di controllo dell'età sono posti a carico dei gestori di siti web e dei fornitori delle piattaforme di condivisione video, al fine di evitare la fruizione da parte di minori di contenuti di carattere pornografico, mentre l'AGCom è chiamata a stabilire, entro sessanta giorni dalla data di entrata in vigore della legge di conversione, con proprio provvedimento, sentito il Garante per la protezione dei dati personali, le modalità tecniche e di processo che i soggetti sono tenuti ad adottare per l'accertamento della maggiore età degli utenti, assicurando un livello di sicurezza adeguato al rischio e il rispetto della minimizzazione dei dati personali raccolti in ragione dello scopo nonché a vigilare sull'osservanza della disciplina in esame. La stessa AGCom è chiamata a predisporre, entro il 31 gennaio di ciascun anno, una relazione sull'uso delle applicazioni di controllo parentale (sulla base anche di tale relazione, entro il 31 maggio di ciascun anno, l'Autorità politica con delega alle politiche per la famiglia presenta una relazione annuale al Parlamento).

Il tema dell'alfabetizzazione digitale e mediatica a tutela dei minori e delle campagne informative è al centro di disposizioni che affidano alla Presidenza del Consiglio dei ministri - Dipartimento per le politiche della famiglia, la promozione di studi e l'elaborazione di linee guida rivolte ai fruitori di dispositivi di comunicazione elettronica e di applicazioni di controllo parentale, con particolare attenzione agli educatori, alle famiglie e ai minori stessi, nonché l'organizzazione, insieme al MIMIT, di campagne annuali di informazione sull'uso consapevole della rete e sui rischi connessi.

I Centri per la famiglia sono invece chiamati ad offrire consulenza e servizi in merito alla alfabetizzazione mediatica e digitale dei minori, con particolare attenzione alla loro tutela rispetto all'esposizione a contenuti pornografici e violenti.

Quanto esposto dimostra l'assoluta centralità assunta, anche nel contesto nazionale, dalla tutela dei minori nel contesto digitale. Si tratta di un interesse che ha registrato, inevitabilmente, una crescente rilevanza in conseguenza della crescente diffusione dei servizi digitali e del sempre più massiccio utilizzo dei device da parte di tali categorie di soggetti.

*Quanto esposto dimostra l'assoluta centralità assunta, anche nel contesto nazionale, dalla tutela dei minori nel contesto digitale. Si tratta di un interesse che ha registrato, inevitabilmente, una crescente rilevanza in conseguenza della crescente diffusione dei servizi digitali e del sempre più massiccio utilizzo dei device da parte di tali categorie di soggetti*

In particolare, con DM 21 giugno 2021 è stato istituito un tavolo tecnico sulla tutela dei diritti dei minori nel contesto dei social networks, dei servizi e dei prodotti digitali in rete i cui lavori sono culminati nella pubblicazione, il 10 maggio 2022, della relazione finale nella quale sono state individuate quattro possibili aree di intervento, e nello specifico, *age verification*, lotta al fenomeno dei baby influencer**,** promozione di campagne di comunicazione e sensibilizzazione sul corretto uso delle risorse online da parte dei minori e del rapporto tra genitori e minori e nuova governance per il coordinamento degli attori istituzionali aventi finalità di protezione dei minori, con istituzione di una unità di coordinamento interistituzionale sulla tematica.

# 5. SURVEY: LA PERCEZIONE DEI RISCHI DIGITALI DA PARTE DI STUDENTI E DOCENTI

Nel mese di novembre 2023 l'Istituto per la Competitività (I-Com) – con il supporto dei *laFabbrica.net*[24] e *wonderwhat.it* – ha avviato un'indagine campionaria volta a comprendere il grado di consapevolezza degli studenti italiani rispetto ai principali rischi collegati all'utilizzo degli strumenti informatici, nonché sulle possibili iniziative utili a potenziare conoscenze e competenze necessarie ad affrontare le sfide dell'ecosistema digitale.

L'indagine si è articolata su due assi principali: il primo ha previsto la somministrazione di un questionario di 15 domande agli studenti di scuola secondaria e ad universitari, al fine di identificare le loro abitudini di utilizzo degli strumenti digitali e la loro preparazione nel rispondere alle minacce informatiche; il secondo si è sostanziato nella somministrazione di un questionario ai docenti composto da 8 domande volte a comprendere il grado di consapevolezza dei propri studenti, delle scuole primarie e secondarie, rispetto ai principali rischi collegati all'utilizzo degli strumenti informatici, nonché sul possibile ruolo della scuola e della famiglia nell'acquisizione delle conoscenze e competenze necessarie ad affrontare le sfide dell'ecosistema digitale.

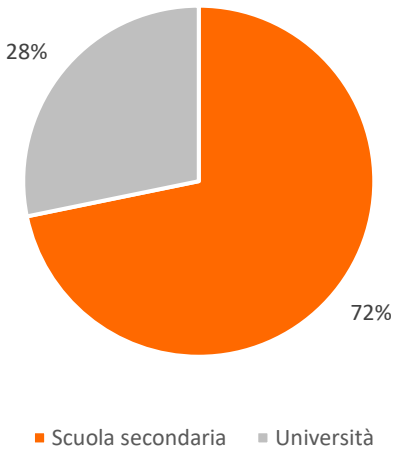
Lo studio ha coinvolto un campione di 280 studenti e 235 docenti e la raccolta dati è avvenuta tramite metodo CAWI (Computer Assisted Web Interview), ovvero attraverso l'auto compilazione da parte degli intervistati di un questionario somministrato via web.

## 5.1. Gli studenti di scuola secondaria e gli universitari

Sul versante degli studenti il campione è composto per il 72% da soggetti che frequentano la scuola secondaria e per il 28% da universitari (Fig.5.1).

**Fig.5.1: Distribuzione del campione degli studenti per istituto frequentato**

Totale rispondenti: 280 su 280
Fonte: Elaborazioni I-Com

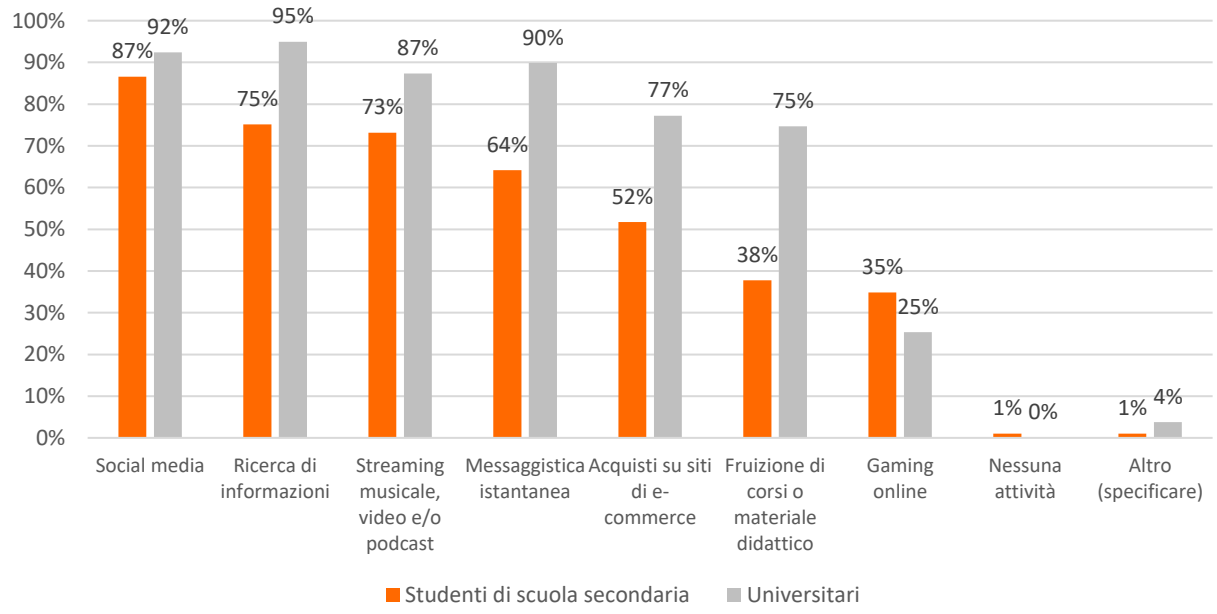



[24] *Società Benefit*

In merito alle attività svolte online, osservando le risposte è possibile notare come solo l'1% degli studenti di scuola superiore non utilizza i canali digitali per nessuna finalità, mentre tra gli universitari invece nessuno ha selezionato questa opzione (Fig.5.2). Tra le attività maggiormente svolte, spiccano i social media (fruiti dall'87% degli studenti di scuola secondaria e del 92% degli universitari) e la ricerca di informazioni (rispettivamente il 75% e il 95%).

**Fig.5.2: Quali delle seguenti attività online svolgi con regolarità?**

Totale rispondenti: 280 su 280
Fonte: Elaborazioni I-Com

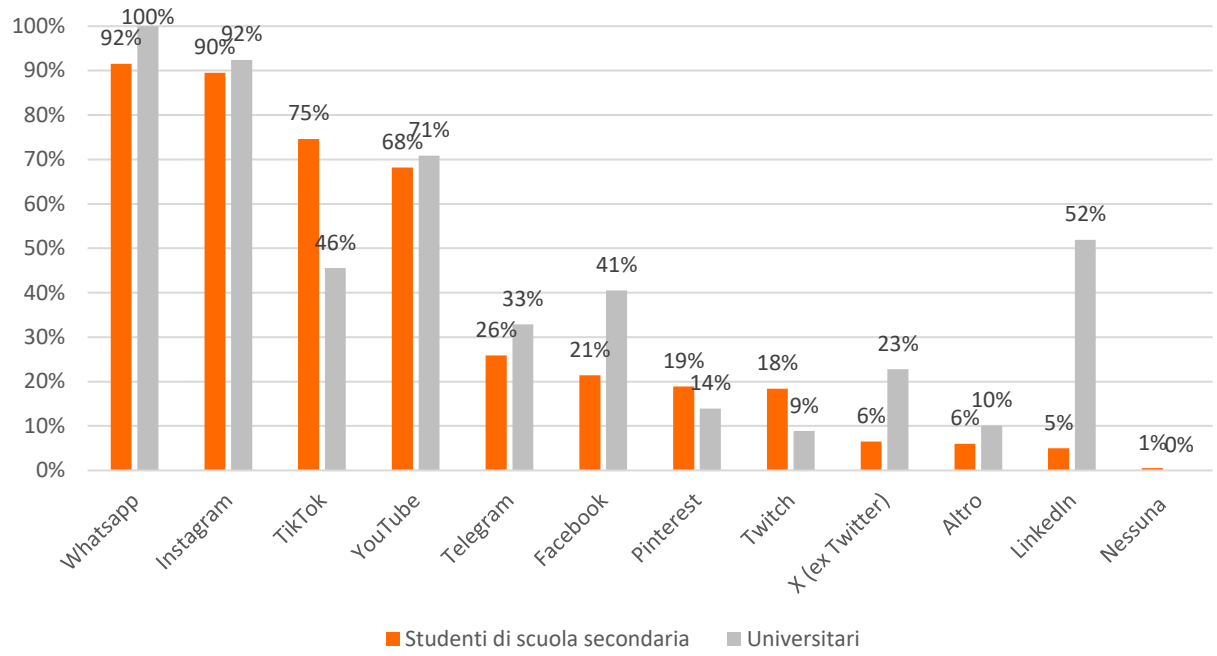



Osservando la distribuzione delle risposte nei due gruppi possiamo vedere come gran parte degli intervistati utilizzi più di una piattaforma digitale con regolarità, in particolare la quasi totalità fruisce di Whatsapp e Instagram (Fig.5.3). Altre piattaforme molto diffuse sono TikTok e YouTube: in particolare, la prima è molto diffusa fra gli studenti più giovani (il 75% rispetto al 46%), mentre sulla seconda vi è un sostanziale equilibrio. Un divario importante si riscontra nell'uso di LinkedIn, con solo il 5% degli studenti di scuola secondaria che lo utilizza contro il 52% degli universitari. Ciò riflette l'orientamento di LinkedIn verso il networking professionale, rendendolo più rilevante per gli individui più prossimi ad entrare nel mondo del lavoro.

*Osservando la distribuzione delle risposte nei due gruppi possiamo vedere come gran parte degli intervistati utilizzi più di una piattaforma digitale con regolarità, in particolare la quasi totalità fruisce di Whatsapp e Instagram*

**Fig.5.3: Quali delle seguenti piattaforme utilizzi con regolarità?**

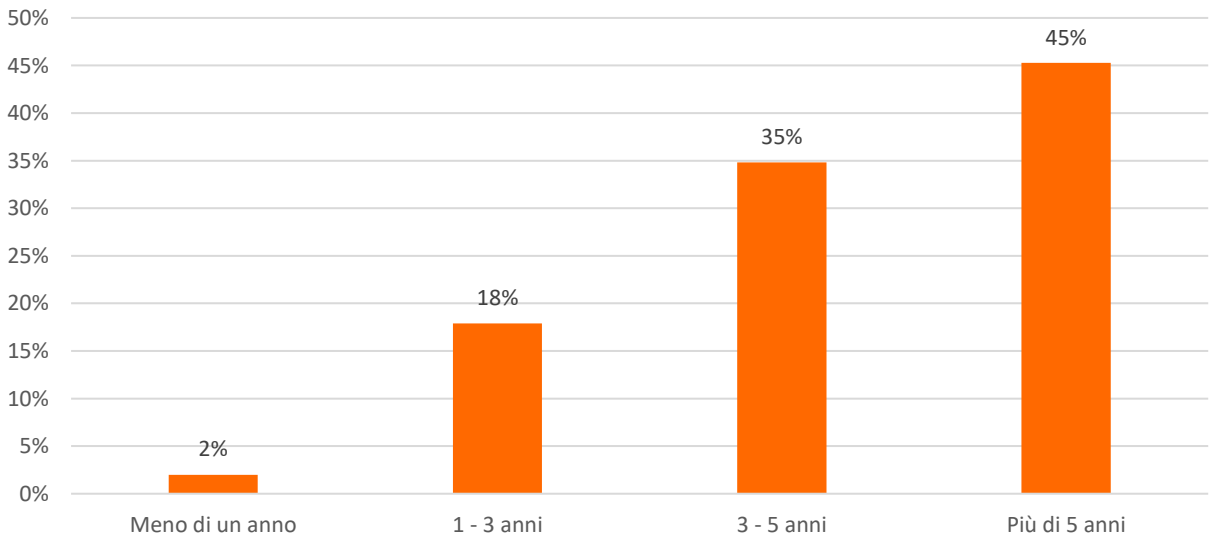
Totale rispondenti: 280 su 280
Fonte: Elaborazioni I-Com




Agli studenti delle scuole secondarie è stato inoltre chiesto da quanti anni utilizzassero i social network (Fig.5.4). Si è scelto di somministrare questa domanda solo a questa categoria di studenti in virtù della giovane età di questa classe di rispondenti. Considerando ciò, è particolarmente interessante notare come la maggioranza dei rispondenti (45%) abbia affermato di utilizzare i social da più di 5 anni, quindi con tutta probabilità da prima del limite legale previsto in Italia di 14 anni (decreto legislativo 101 del 2018).

**Fig.5.4: Da quanti anni utilizzi i social media con regolarità?**

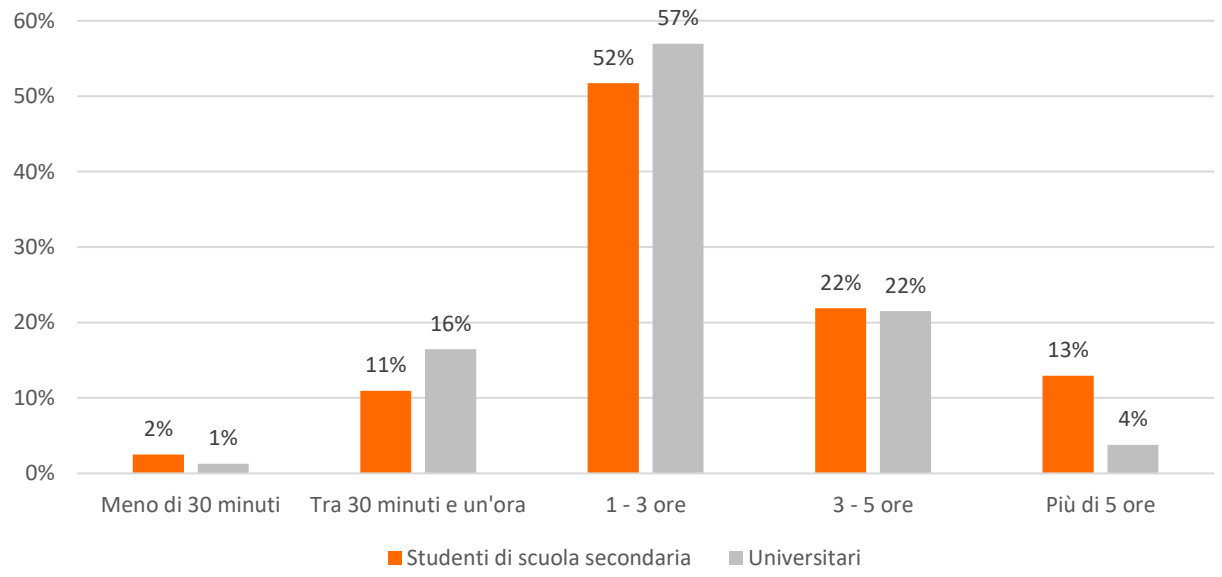
Totale rispondenti: 201 su 201
Fonte: Elaborazioni I-Com



Relativamente al tempo trascorso sui social media la distribuzione delle risposte è pressoché la stessa (Fig.5.5). Infatti, la maggior parte degli intervistati, il 52% degli studenti di scuola secondaria e il 57% degli universitari, dichiara di trascorrervi fra una e tre ore. Una parte ristrettissima degli intervistati si colloca agli estremi: solo il 2% degli studenti di scuola secondaria e l'1% degli universitari passa meno di mezz'ora sui social media; invece afferma di trascorrere più di 5 ore online il 13% degli studenti di scuola secondaria e il 4% degli studenti universitari.

**Fig.5.5: In media, quanto tempo trascorri al giorno utilizzando i social media?**

Totale rispondenti: 280 su 280
Fonte: Elaborazioni I-Com

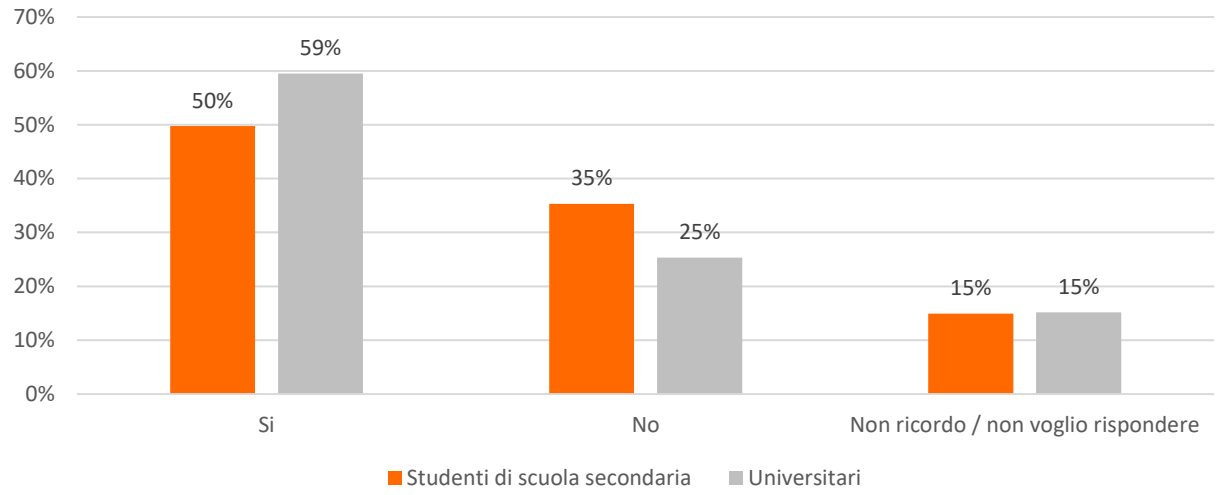



*Il 52% degli studenti di scuola secondaria e il 57% degli universitari dichiarano di trascorrervi fra una e tre ore. Una parte ristrettissima degli intervistati si colloca agli estremi: solo il 2% degli studenti di scuola secondaria e l'1% degli universitari passa meno di mezzora sui social media; invece afferma di trascorrere più di 5 ore online il 13% degli studenti di scuola secondaria e il 4% degli studenti universitari*

Sono molto alte le percentuali di coloro che affermano di aver ricevuto una richiesta di informazioni personali (Fig.5.6), rispettivamente il 50% degli studenti di scuola secondaria e il 59% degli universitari. Considerevoli sono anche le percentuali di studenti che dichiarano di non voler rispondere, il 15% sia di quelli di scuola secondaria che di universitari. Da ciò emerge chiaramente quanto i ragazzi possano essere vulnerabili, se non correttamente informati, tramite queste piattaforme.

**Fig.5.6: Ti hanno mai chiesto informazioni personali tramite mail/messaggi sui social o sulle applicazioni di instant messaging?**

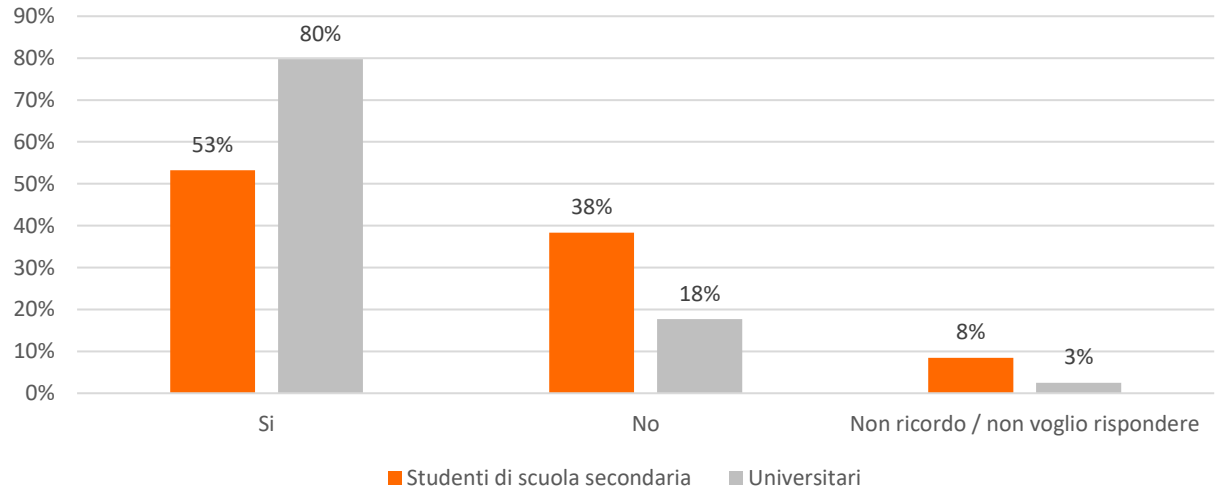
Totale rispondenti: 280 su 280
Fonte: Elaborazioni I-Com




Ciò detto, desta preoccupazione anche la quota di coloro che affermano di aver ricevuto messaggi o mail da soggetti malintenzionati (Fig.5.7), ossia l'80% degli universitari, dato che scende di ben 27 punti percentuali, al 53%, per gli studenti di scuola secondaria, che però in virtù della giovane età possono certamente essere considerati più vulnerabili. Allo stesso tempo è da segnalare come, ancora una volta, l'8% di questi non abbia voluto rispondere.

**Fig.5.7: Hai mai ricevuto mail/messaggi da soggetti apparentemente malintenzionati o sospetti sui social media o sulle applicazioni di instant messaging?**

Totale rispondenti: 280 su 280
Fonte: Elaborazioni I-Com



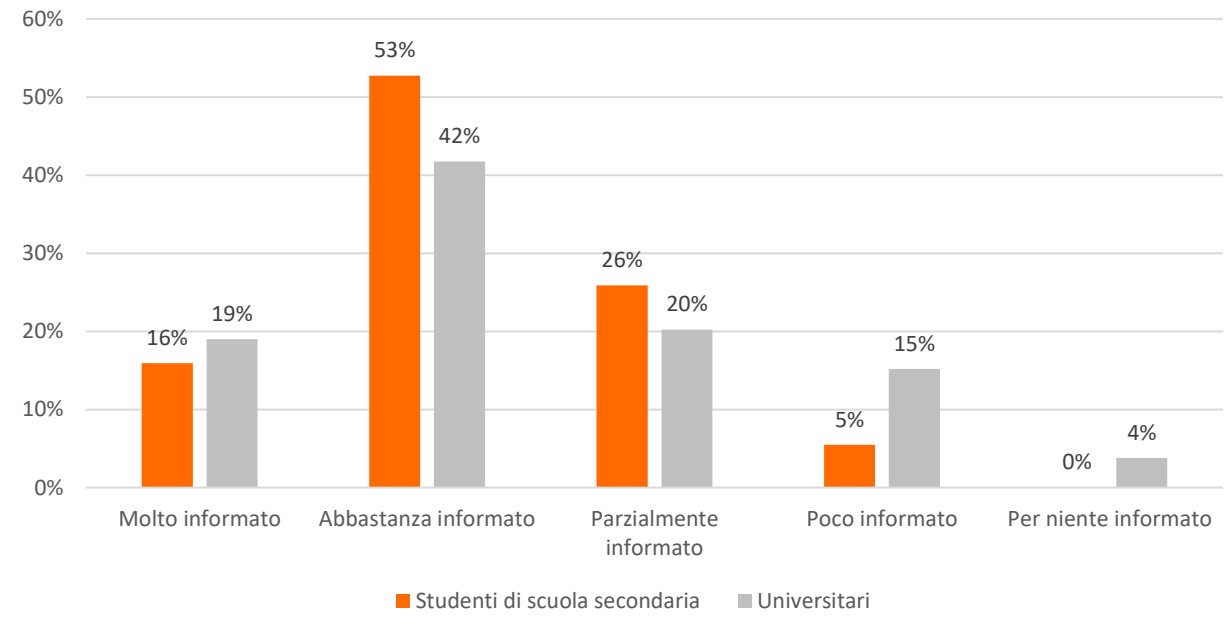

Dal sondaggio inoltre emerge che, almeno nella percezione degli studenti, vi è una buona diffusione delle informazioni relative a come proteggersi dai pericoli della rete (Fig.5.8). La quota maggiore di rispondenti afferma infatti di essere abbastanza informato, con una percentuale

leggermente maggiore negli studenti di scuola secondaria, il 53% contro il 42% degli universitari. Quest'ultimi, sempre secondo un giudizio personale, sono in media meno informati degli studenti di scuola secondaria, infatti dice di essere poco informato rispettivamente il 15% e il 5%. Tale dato potrebbe essere condizionato dalla maggiore consapevolezza degli individui anagraficamente più grandi.

*Almeno nella percezione degli studenti, vi è una buona diffusione delle informazioni relative a come proteggersi dai pericoli della rete. La quota maggiore di rispondenti afferma infatti di essere abbastanza informato, con una percentuale leggermente maggiore negli studenti di scuola secondaria, il 53% contro il 42% degli universitari*

**Fig.5.8: Quanto ritieni di essere informato su come proteggerti dai pericoli in cui potresti imbatterti in rete (ad esempio, phishing, furto di identità, cyberbullismo, incontri indesiderati online o ricezione di contenuti dannosi)?**

Totale rispondenti: 280 su 280
Fonte: Elaborazioni I-Com

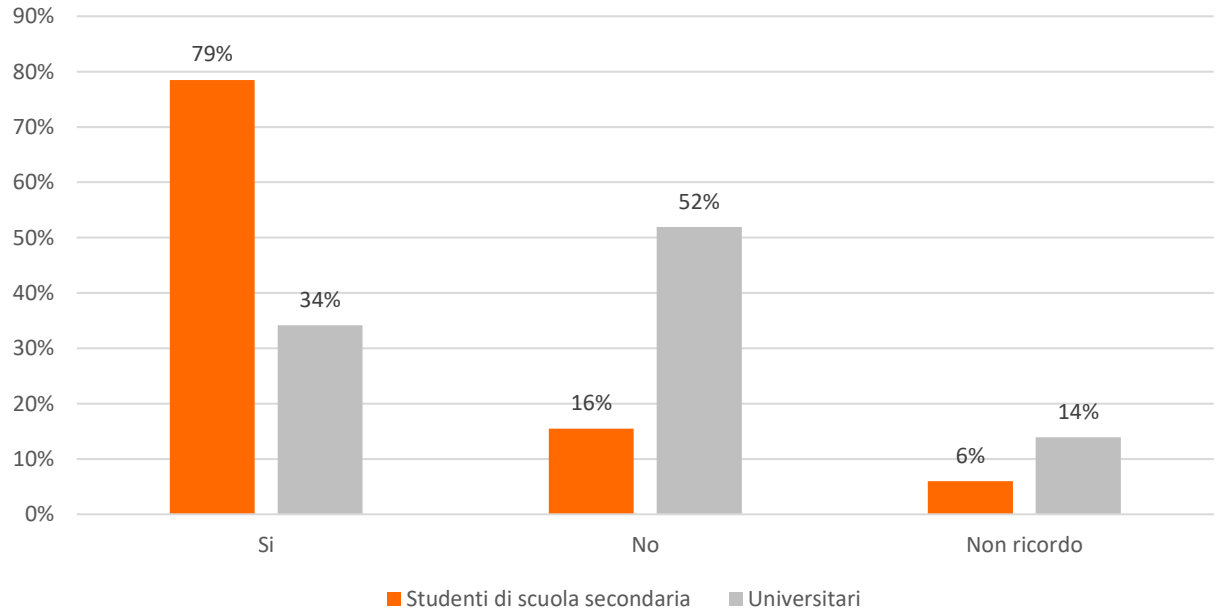



Emerge anche che una quota rilevante di universitari, il 52% (Fig.5.9), non ha mai ricevuto informazioni su come proteggersi in rete. La diffusione di informazioni in ambito di sicurezza digitale sembra apparentemente differenziarsi per fasce d'età e grado di istruzione. Infatti, di converso, la larga maggioranza degli studenti di scuola secondaria hanno dichiarato di aver ricevuto informazioni a proposito, ben l'79%, contro il 34% degli universitari. Questo potrebbe dimostrare una maggiore sensibilità anche delle istituzioni scolastiche verso tali tematiche che sfocia in una maggiore diffusione di iniziative dedicate a tali tematiche.

*La larga maggioranza degli studenti di scuola secondaria hanno dichiarato di aver ricevuto informazioni a proposito, ben il 79%, contro il 34% degli universitari. Questo potrebbe dimostrare una maggiore sensibilità anche delle istituzioni scolastiche verso tali tematiche che sfocia in una maggiore diffusione di iniziative dedicate a tali tematiche*

**Fig.5.9: Hai mai ricevuto spiegazioni o informazioni su come proteggerti dai pericoli in rete (escludendo le volte in cui ti sei informato autonomamente)?**

Totale rispondenti: 280 su 280
Fonte: Elaborazioni I-Com

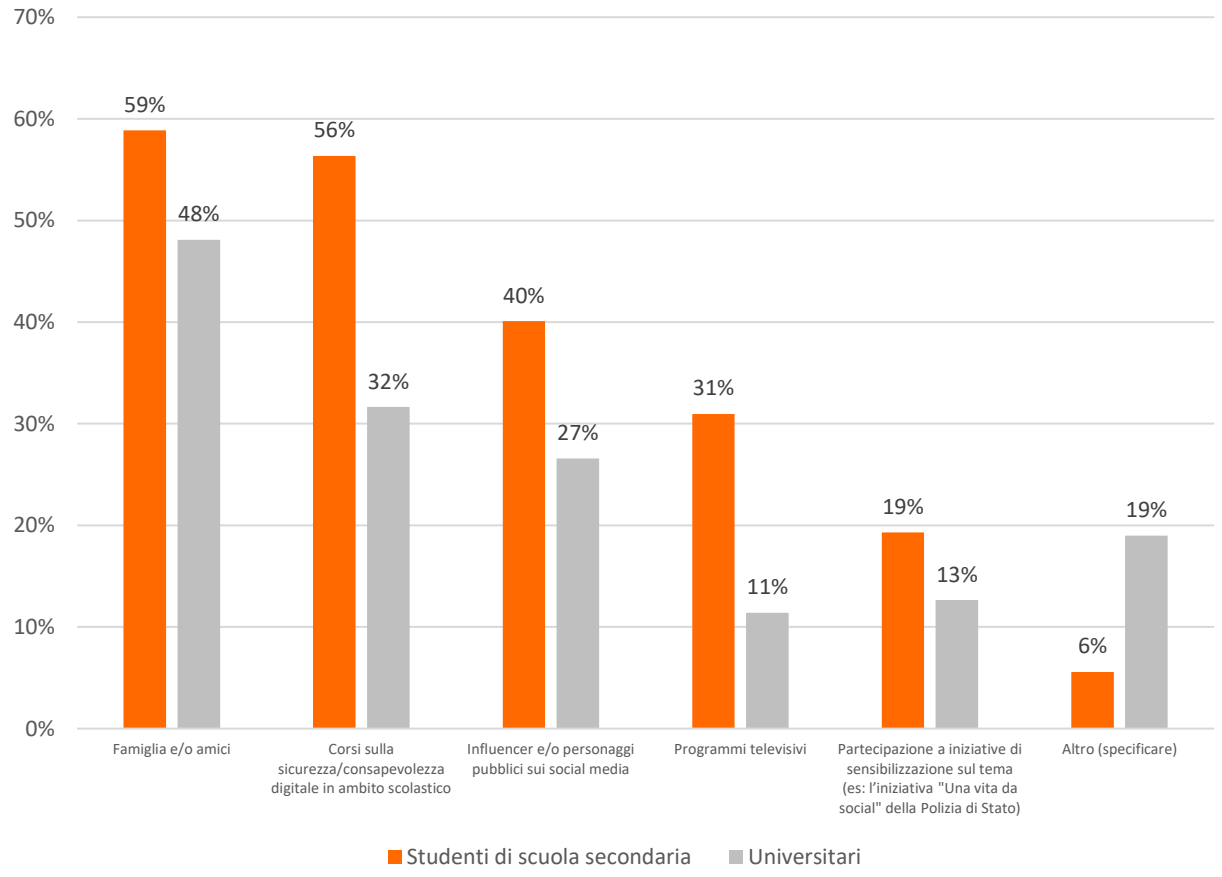



La tesi esposta precedentemente trova conferma nella domanda seguente, infatti, fra le fonti principali delle informazioni su come proteggersi dai rischi, risaltano al secondo posto i corsi sulla sicurezza digitale in ambito scolastico, preceduti solo dalle nozioni ricevute da famiglia e amici. Giocano un ruolo rilevante anche gli influencer e i personaggi pubblici: dichiarano infatti di aver ricevuto da queste informazioni in ambito di sicurezza digitale il 40% degli studenti di scuola secondaria e il 27% degli universitari (Fig.5.10).

*Giocano un ruolo rilevante anche gli influencer e i personaggi pubblici: dichiarano infatti di aver ricevuto da queste informazioni in ambito di sicurezza digitale il 37% degli studenti di scuola secondaria e il 27% degli universitari*

**Fig.5.10: Da quali fonti hai ricevuto queste informazioni? (sono possibili più risposte)**

Totale rispondenti: 280 su 280
Fonte: Elaborazioni I-Com

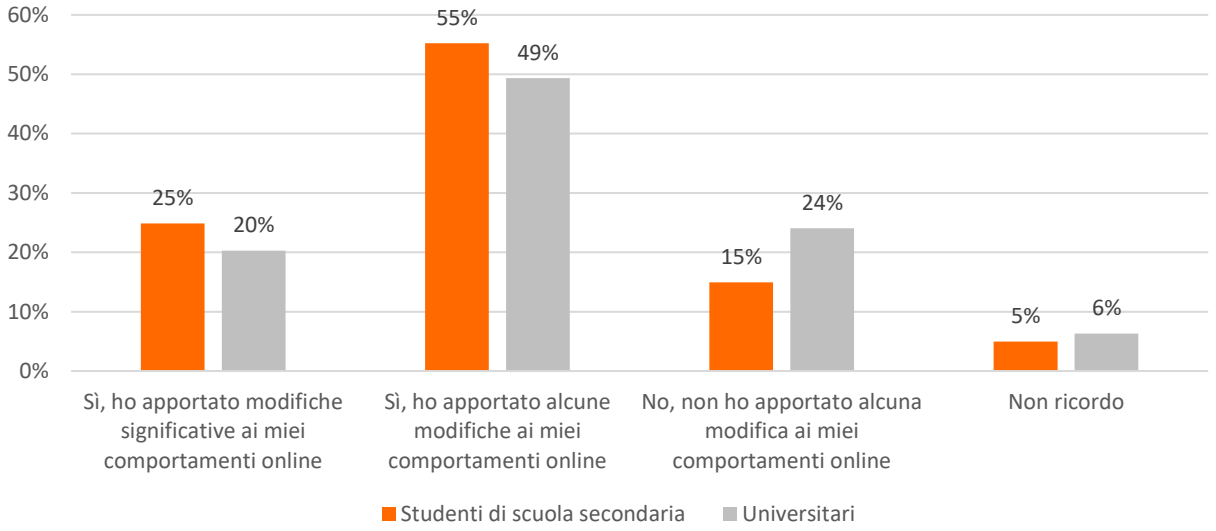



Larga parte degli intervistati ha percepito come utili le informazioni di sicurezza ricevute. In risposta alle stesse una quota importantissima, il 55% e il 49% rispettivamente di studenti di scuola secondaria e universitari, ha apportato alcune modifiche ai propri comportamenti digitali (Fig.5.11). Di converso, purtroppo c'è una quota di minoranza ma non irrilevante (15% degli studenti di scuola secondaria e 24% degli universitari) che a seguito di queste informazioni non ha modificato le proprie abitudini.

*Larga parte degli intervistati ha percepito come utili le informazioni di sicurezza ricevute. In risposta alle stesse una quota importantissima, il 55% e il 49% rispettivamente di studenti di scuola secondaria e universitari, ha apportato alcune modifiche ai propri comportamenti digitali*

**Fig.5.11: Hai apportato modifiche ai tuoi comportamenti online (come cambio di impostazioni di privacy sui social media, cambio regolare delle password, uso di VPN, ecc.) in risposta alle informazioni che hai ricevuto per proteggerti dai pericoli in rete?**

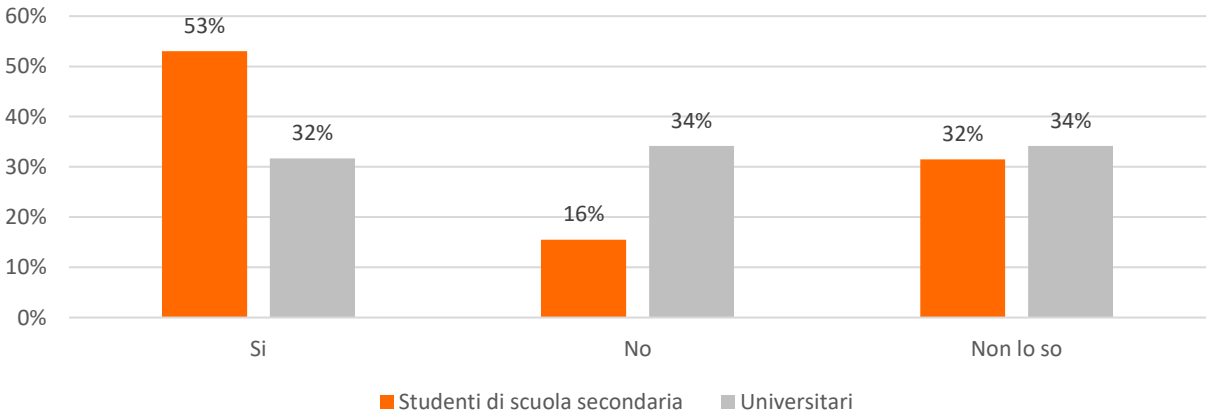
Totale rispondenti: 280 su 280
Fonte: Elaborazioni I-Com




È da sottolineare comunque la diffusione di incertezza sulla sufficienza o meno dei propri comportamenti per proteggersi dai pericoli digitali (Fig.5.12). Infatti, un terzo degli intervistati non riesce a dare una risposta precisa a questo proposito, mentre un quarto degli stessi crede che questi comportamenti non siano sufficienti. Parimenti a quanto visto in precedenza, dalle risposte pervenute gli studenti di scuola secondaria sembrerebbero essere più sicuri degli universitari rispetto alle proprie capacità di autodifesa digitale. Questo però potrebbe spingerli ad adottare comportamenti meno prudenti rispetto a potenziali minacce.

**Fig.5.12: Ritieni che le misure e i comportamenti da te adottati per proteggere la tua privacy online siano sufficienti?**

Totale rispondenti: 280 su 280
Fonte: Elaborazioni I-Com

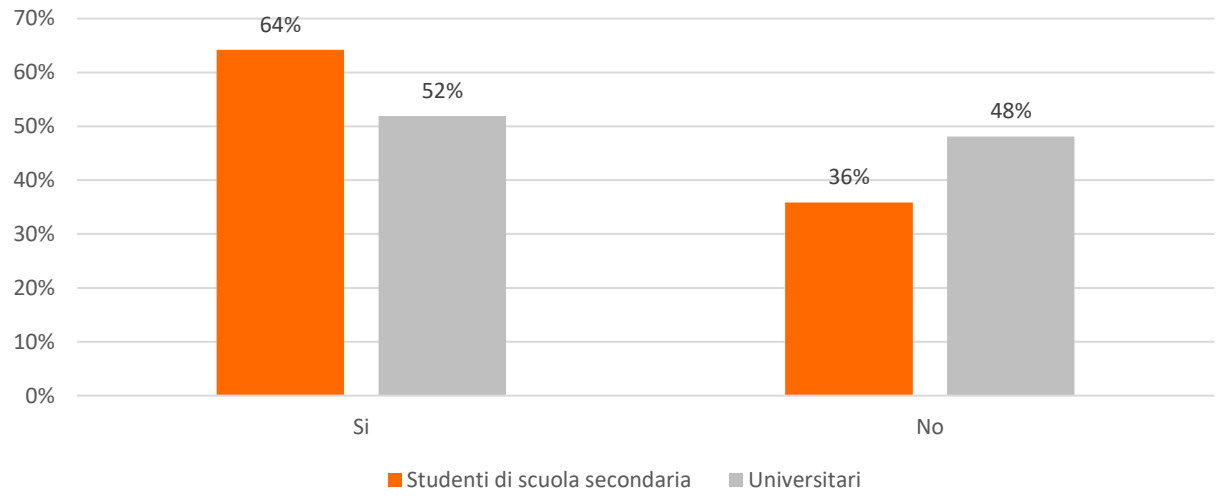


*Dalle risposte pervenute gli studenti di scuola secondaria sembrerebbero essere più sicuri degli universitari rispetto alle proprie capacità di autodifesa digitale. Questo però potrebbe spingerli ad adottare comportamenti meno prudenti rispetto a potenziali minacce*

Si palesa un'incertezza diffusa anche riguardo ai soggetti da contattare in caso di problematiche online, come phishing o furto d'identità (Fig.5.13). Il 48% degli studenti di scuola secondaria e il 36% degli universitari non sa a chi rivolgersi; ciò accentua la necessità di identificare un punto di riferimento noto a cui gli studenti (e non) possono appellarsi in caso incorrano in situazioni di pericolo online.

**Fig.5.13: Sai a chi rivolgerti in caso di problemi online (ad esempio, phishing, furto di identità, cyberbullismo, incontri indesiderati online o ricezione di contenuti dannosi)?**

Totale rispondenti: 280 su 280
Fonte: Elaborazioni I-Com

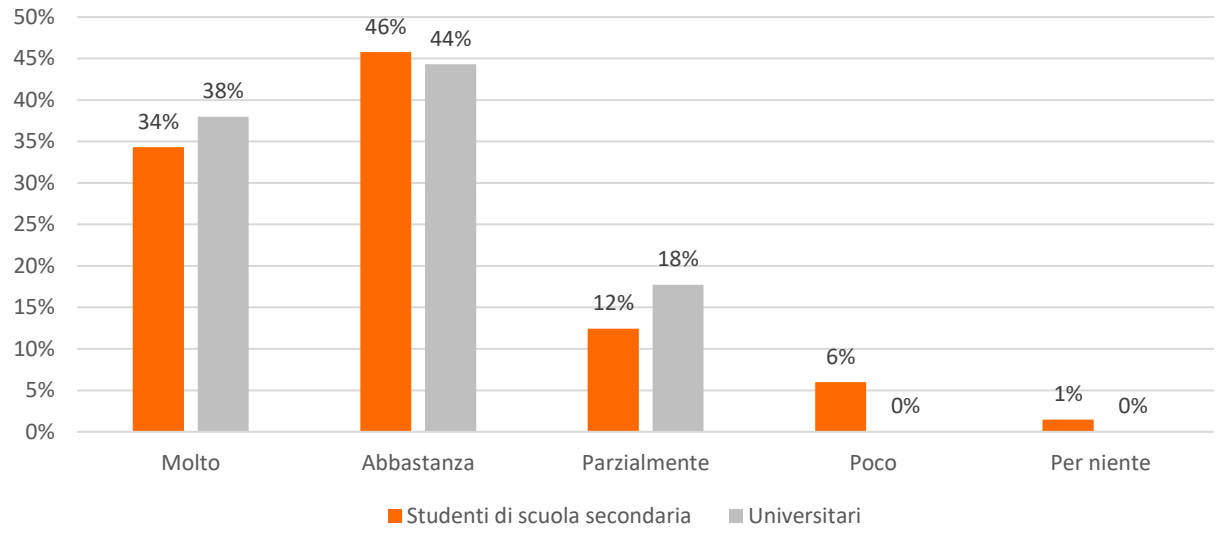



Infine, un segnale positivo viene dall'ultima domanda: la larghissima maggioranza dei partecipanti alla survey ha definito come molto (34% degli studenti di scuola secondaria e 38% degli universitari) o abbastanza importanti (46% e 44%) le iniziative per accrescere la consapevolezza digitale (Fig.5.14). Da ciò si può desumere che la quasi totalità dei giovani comprendono che l'ecosistema digitale abbia dei punti oscuri da cui sia necessario difendersi e che possedere un adeguato bagaglio di skill è lo strumento più importante per agire in tal senso.

*La larghissima maggioranza dei partecipanti alla survey ha definito come molto (34% degli studenti di scuola secondaria e 38% degli universitari) o abbastanza importanti (46% e 44%) le iniziative per accrescere la consapevolezza digitale*

**Fig.5.14: Quanto riterresti utile partecipare a iniziative per accrescere la tua consapevolezza rispetto ai pericoli della rete?**

Totale rispondenti: 280 su 280
Fonte: Elaborazioni I-Com

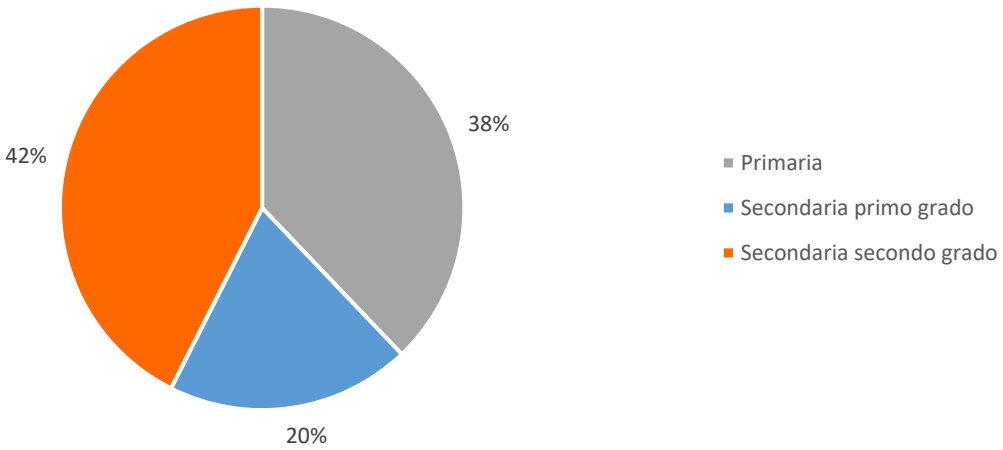



## 5.2. Il punto di vista dei docenti

Analizzare la prospettiva dei docenti rispetto al livello di awareness digitale dei propri studenti è fondamentale per delineare un quadro coerente in merito al tema, poiché non è scontato che il punto di vista dei primi coincida pacificamente con quello dei secondi. Come precedentemente accennato, l'Istituto per la Competitività ha rivolto una specifica survey agli insegnanti, al fine di conoscere la loro esperienza e il loro impegno in termini di prevenzione e contrasto ai rischi derivanti dall'impiego di strumenti digitali, che effettivamente incombono sui discenti.

**Fig.5.15: In che tipologia di istituto insegna?**

Totale rispondenti: 235 su 235
Fonte: Elaborazioni I-Com

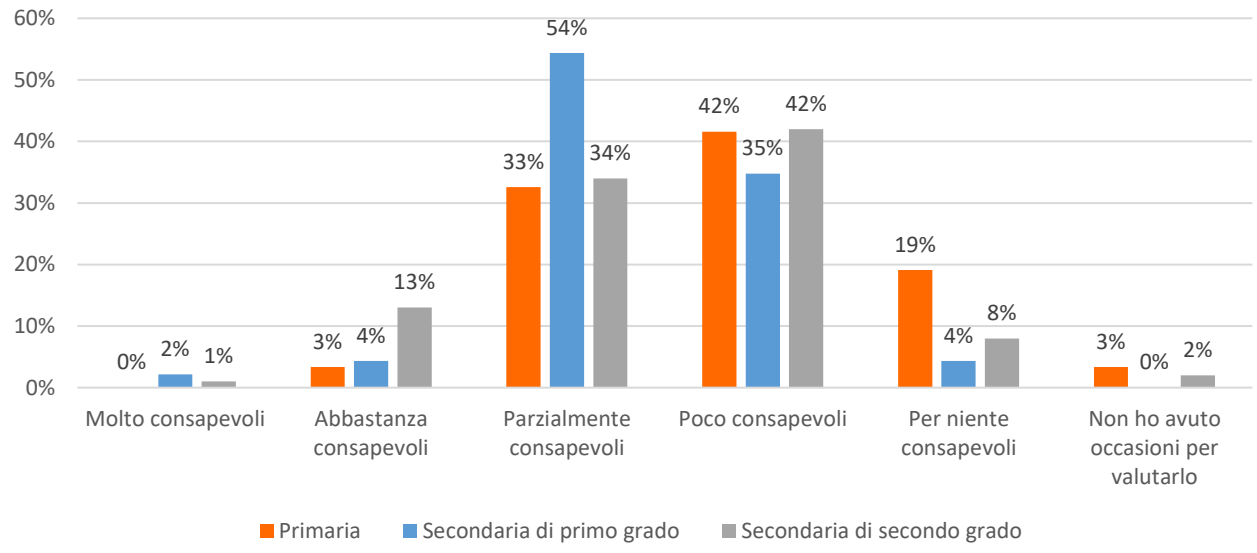


Nello specifico (Fig.5.15), i dati fanno riferimento a quanto indicato da 235 rispondenti, la maggior parte provenienti da scuole secondarie di secondo grado (42%), oltre che da scuole primarie (38%) e scuole secondarie di primo grado (20%).

Innanzitutto, è stato chiesto al campione di riferimento di valutare il livello di consapevolezza dei propri studenti circa i rischi connessi all'utilizzo di strumenti digitali (Fig.5.16) ed è emerso che per la maggioranza di docenti appartenenti alle scuole secondarie di secondo grado (42%) e alle scuole primarie (42%) c'è poca consapevolezza, mentre viene valutata come parziale da chi insegna in scuole secondarie di primo grado (35%). I risultati si mostrano preoccupanti se si considera che complessivamente solo il 3% e il 20% dei docenti affermano che i propri studenti sono, rispettivamente, molto o abbastanza consapevoli dei pericoli connessi alla rete. Inoltre, secondo il 31% degli insegnanti (il 19% tra quelli appartenenti alle primarie; il 4% tra i docenti delle secondarie di primo grado e l'8% tra i professori delle secondarie di secondo grado) vi è una totale assenza di awareness in merito alla tematica, aspetto che invece non è stato per niente valutato dal 5% docenti.

**Fig.5.16: In base alla sua esperienza, come valuterebbe il livello di consapevolezza dei suoi studenti circa i rischi connessi all'utilizzo di strumenti digitali?**

Totale rispondenti: 235 su 235
Fonte: Elaborazioni I-Com



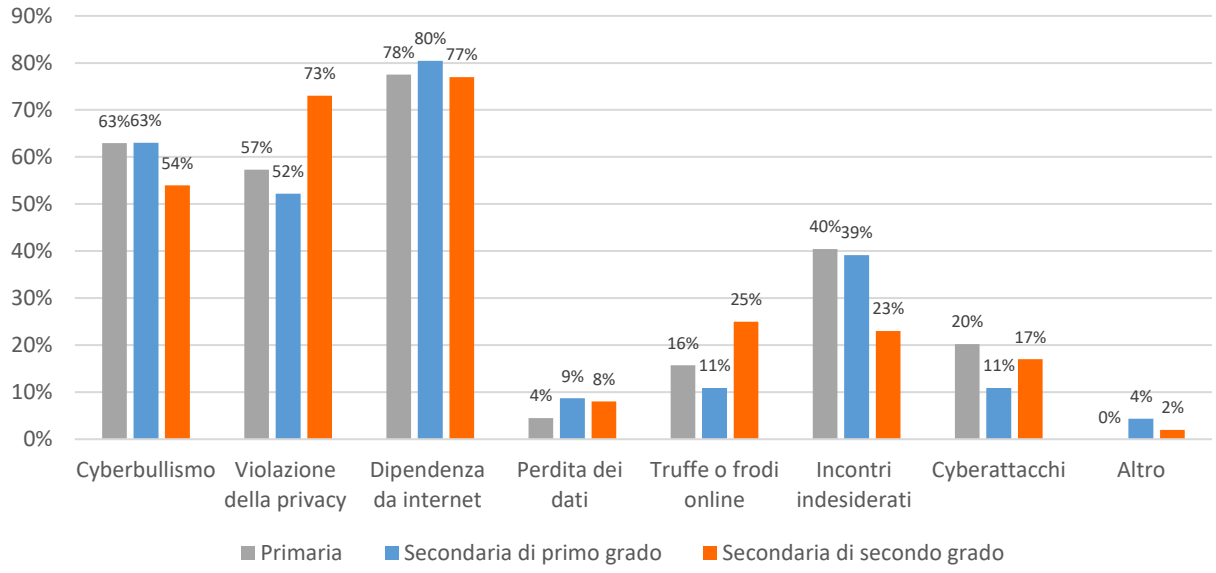

*Per la maggioranza di docenti appartenenti alle scuole secondarie di secondo grado (42%) e alle scuole primarie (42%) c'è poca consapevolezza, mentre viene valutata come parziale da chi insegna in scuole secondarie di primo grado (35%)*

Dalla survey emerge che i principali pericoli in cui rischiano di imbattersi i giovani nell'ottica degli insegnanti sono: la dipendenza da Internet (secondo il 77% dei docenti delle scuole secondarie di secondo grado, il 78% delle scuole primarie e l'80% delle scuole secondarie di primo grado); la

violazione della privacy secondo il 73% degli insegnanti delle scuole secondarie di secondo grado; il cyberbullismo per il 63% delle primarie e, in egual misura, delle secondarie di primo grado (Fig. 5.17). Diversamente, sembra che la perdita di dati personali non colpisca particolarmente i discenti, essendo rilevante solo per il 9% dei docenti delle secondarie di primo grado, per l'8% di quelli appartenenti alle secondarie di secondo grado e per il 4% di coloro che insegnano alle primarie. Oltre ai pericoli esplicitamente indicati nelle domande, tra le risposte libere vengono individuati anche la pornografia, la disinformazione, la propaganda e l'imitazione di modelli che producono influenze negative legate allo sviluppo di comportamenti violenti e alla percezione distorta dell'aspetto fisico.

**Fig.5.17: Secondo lei, quali sono i principali pericoli in cui rischiano di imbattersi i giovani nell'utilizzo degli strumenti digitali?**

Note: Possibilità di più risposte
Totale rispondenti: 235 su 235
Fonte: Elaborazioni I-Com



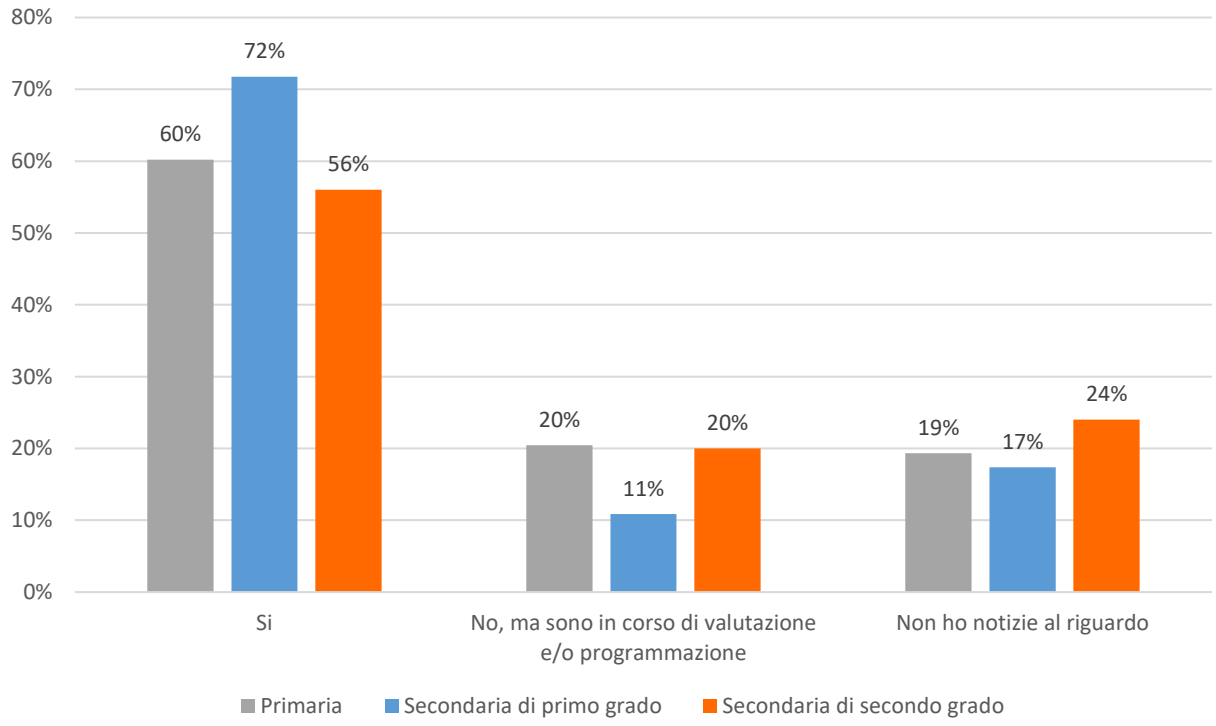

*I principali pericoli in cui rischiano di imbattersi i giovani nell'ottica degli insegnanti sono: la dipendenza da Internet (secondo il 77% dei docenti delle scuole secondarie di secondo grado, il 78% delle scuole primarie e l'80% delle scuole secondarie di primo grado); la violazione della privacy secondo il 73% degli insegnanti delle scuole secondarie di secondo grado; il cyberbullismo per il 63% delle primarie e, in egual misura, delle secondarie di primo grado*

In virtù del fatto che le competenze digitali fungono da scudo rispetto alla tutela di aspetti fondamentali come la privacy, l'integrità fisica e morale, la salute e la sicurezza informatica, è necessario promuovere programmi che sensibilizzino i discenti. Sul punto (Fig.5.18), si riscontra che dall'esperienza del 72% dei docenti delle scuole secondarie di primo grado, del 60% delle

primarie e del 56% delle scuole secondarie di secondo grado, siano state attivate iniziative di questo genere, mentre il 51% del totale dei docenti (ossia il 20% delle secondarie di primo e secondo grado e l'11% delle primarie) riferiscono che sono in corso di valutazione e/o programmazione. Peraltro, il 60% degli educatori afferma di non avere notizie al riguardo, con una prevalenza di quelli delle scuole secondarie di secondo grado.

**Fig.5.18: Nella scuola in cui lavora sono presenti programmi e/o iniziative di sensibilizzazione degli studenti rispetto ai pericoli della rete?**

Totale rispondenti: 234 su 235
Fonte: Elaborazioni I-Com

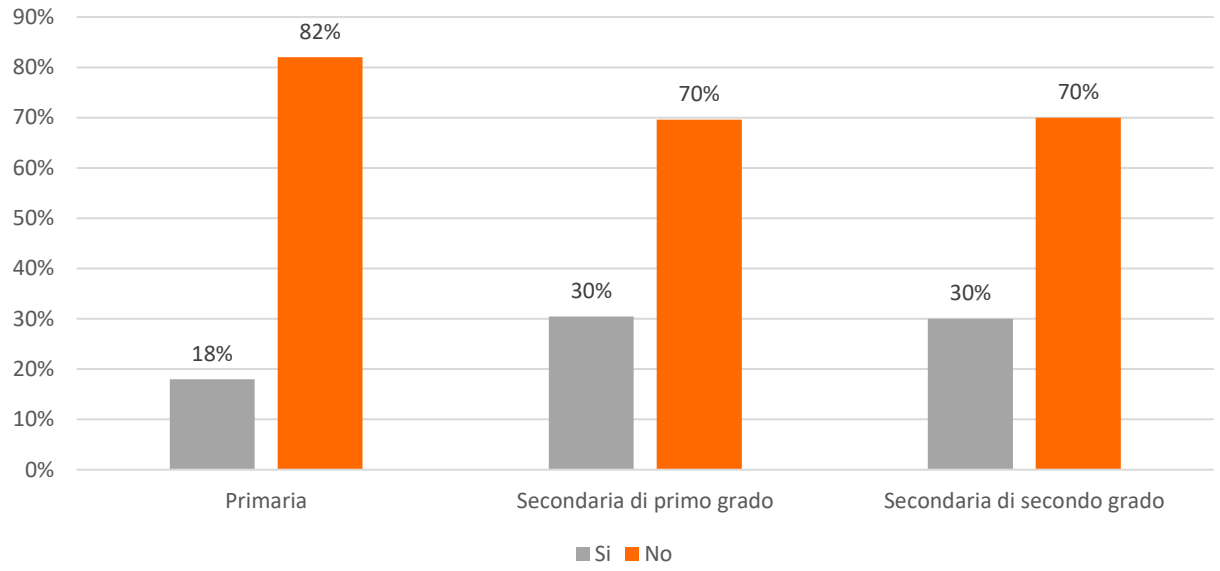



Il grafico successivo (Fig.5.19) consente di affermare che gli studenti dalla primaria fino alla secondaria di secondo grado tendono mediamente a rivolgersi ai docenti per problematiche legate all'utilizzo di strumenti digitali. In particolare, gli studenti delle primarie sembrano affidarsi agli insegnanti prevalentemente per questioni legate al cyberbullismo, contenuti offensivi online e video di istigazione a comportamenti pericolosi. Tra i discenti di entrambi i gradi della scuola secondaria emergono principalmente le medesime problematiche: cyberbullismo, diffusione online non autorizzata di dati, foto e video privati (violazione della privacy), incontri indesiderati sui social e chiarimenti sui pericoli della rete.

*Gli studenti dalla primaria fino alla secondaria di secondo grado tendono mediamente a rivolgersi ai docenti per problematiche legate all'utilizzo di strumenti digitali*

**Fig.5.19: I suoi studenti si sono mai rivolti a lei per problematiche in cui sono incorsi nell'utilizzo di strumenti digitali?**

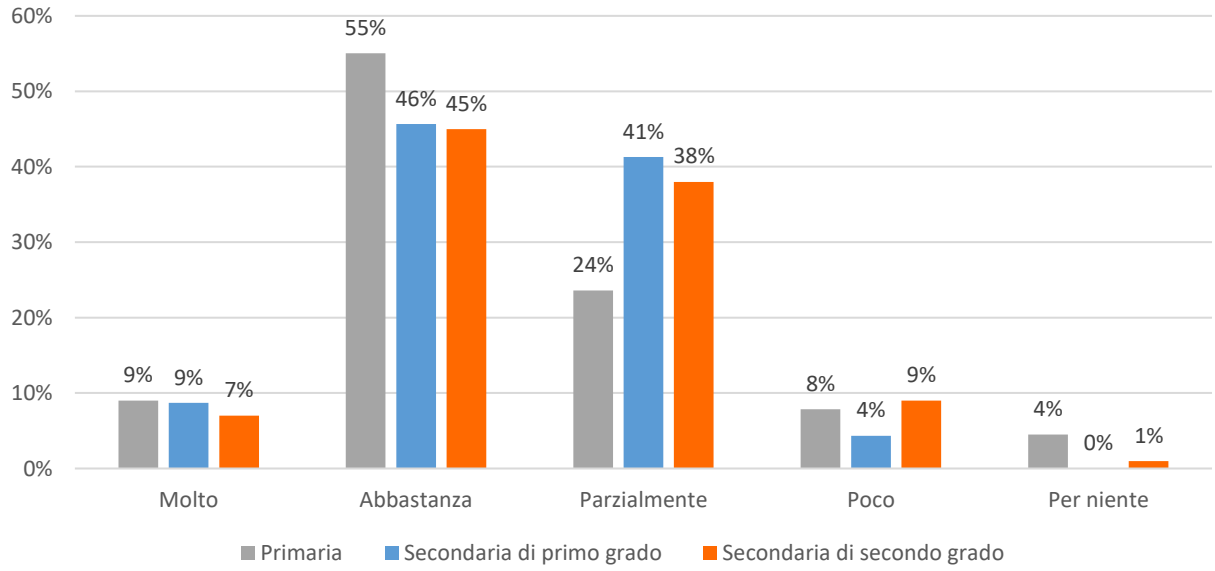
Totale rispondenti: 235 su 235
Fonte: Elaborazioni I-Com




Con riguardo al grado di competenza nel consigliare i propri studenti in termini di prevenzione e risposta alle minacce informatiche (Fig.5.20), la maggior quota di docenti della primaria (55%), della secondaria di primo (46%) e secondo grado (45%) ritengono di esserne abbastanza in grado. Al contrario il 12% degli insegnanti della primaria, il 4% della secondaria di primo grado e il 10% di quella di secondo grado si ritengono poco o per niente preparati.

**Fig.5.20: Quanto si sente competente nel consigliare i suoi studenti su come prevenire e/o affrontare le minacce informatiche?**

Totale rispondenti: 235 su 235
Fonte: Elaborazioni I-Com

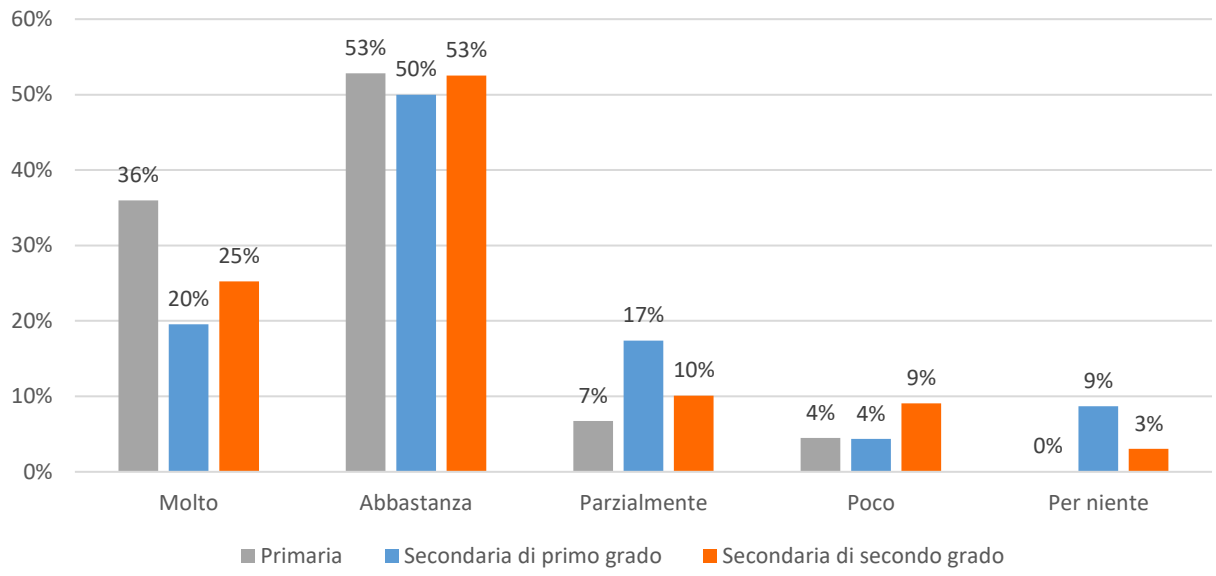


*Con riguardo al grado di competenza nel consigliare i propri studenti in termini di prevenzione e risposta alle minacce informatiche, la maggior quota di docenti della primaria (55%), della secondaria di primo (46%) e secondo grado (45%) ritengono di esserne abbastanza in grado*

Inoltre (Fig.5.21), la stragrande maggioranza dei docenti ritiene molto o abbastanza utile partecipare a iniziative per accrescere la propria consapevolezza e competenza rispetto ai pericoli della rete. Preoccupante, invece, che resiste una sacca di minoranza ma comunque consistente di insegnanti che considerano poco o per niente utile essere coinvolti in tali iniziative formative, in particolare nei due gradi della scuola secondaria.

**Fig.5.21: Quanto riterrebbe utile partecipare a iniziative per accrescere la sua consapevolezza e competenza rispetto ai pericoli della rete?**

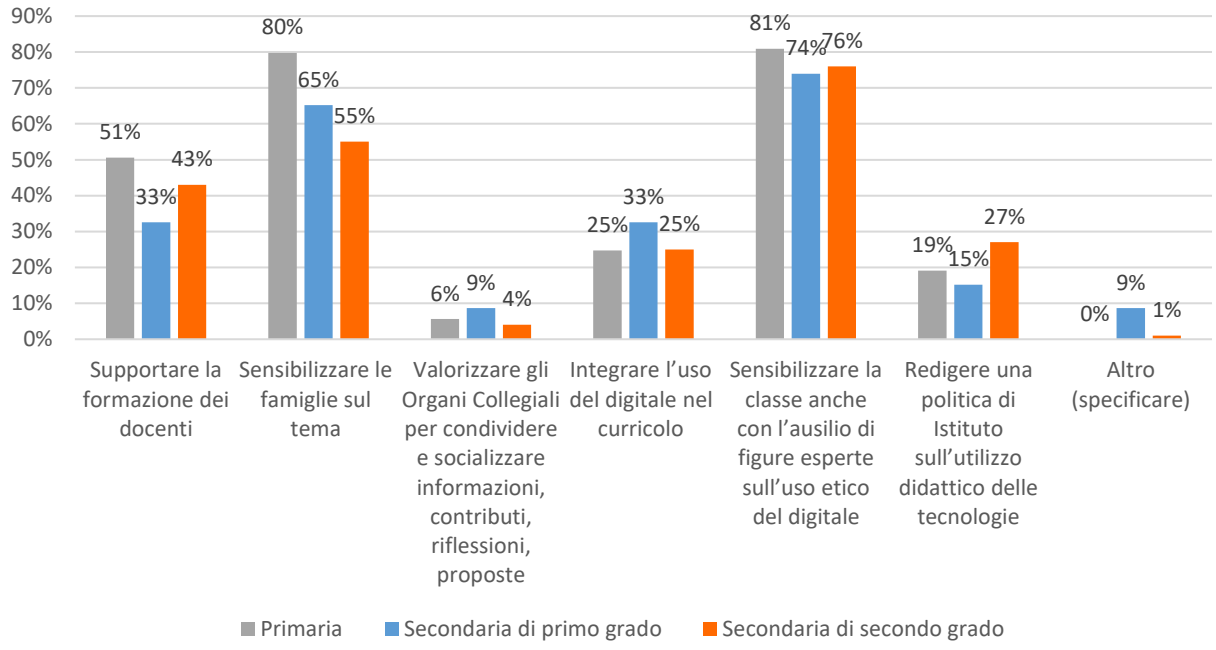
Totale rispondenti: 234 su 235
Fonte: Elaborazioni I-Com




Come ultima domanda (Fig.5.22), è stato chiesto ai docenti del campione di selezionare le iniziative che ritengono idonee a promuovere la consapevolezza digitale dei propri discenti ed è emerso che la maggioranza degli insegnanti di tutte le tipologie di istituti considera particolarmente importante sensibilizzare il gruppo classe con l'ausilio di esperti nell'uso etico delle tecnologie digitali. A seguire, la seconda voce maggiormente selezionata dai docenti afferma di non sottovalutare il ruolo delle famiglie, anch'esse da formare da questi temi. In terza posizione tra le preferenze espresse si colloca il supporto alla formazione dei docenti. Appare interessante evidenziare che l'opzione meno selezionata in assoluto concerne una maggiore valorizzazione degli organi collegiali per condividere e socializzare informazioni, contributi, riflessioni e proposte. Inoltre, tra le risposte in "altro" figura la proposta di aumentare le ore di didattica dedicate, in particolar modo, all'educazione civica e all'informatica.

**Fig.5.22: Quali iniziative, a suo avviso, può attivare la scuola per promuovere efficacemente in studentesse e studenti la consapevolezza digitale?**

Note: Possibilità di più risposte
Totale rispondenti: 235 su 235
Fonte: Elaborazioni I-Com




*La maggioranza degli insegnanti di tutte le tipologie di istituti considera particolarmente importante sensibilizzare il gruppo classe con l'ausilio di esperti nell'uso etico delle tecnologie digitali*

# CONCLUSIONI E SPUNTI DI POLICY

La digitalizzazione ha impattato fortemente sul cambiamento delle abitudini degli individui che utilizzano Internet quotidianamente per scopi differenti, come quello ludico, formativo o lavorativo. La pandemia da Covid-19 ha messo ancor di più in luce le risorse della rete e delle nuove tecnologie, che possono essere impiegate per riprodurre dinamiche tipiche della vita offline, spesso con uguale o maggiore efficacia. I dispositivi di accesso ad Internet sono fondamentali, in quanto questi permettono agli utenti di entrare nella dimensione virtuale e di farlo in maniera smart. Per questa ragione, la maggior parte di essi utilizza device mobili per navigare in rete, limitando sempre di più l'impiego dei PC.

Grazie ad Internet anche la ricerca informativa rivede un particolare miglioramento, soprattutto in virtù del potenziale offerto dai social network e dalle loro fonti aperte. Peralto, va evidenziato che il cambiamento delle abitudini quotidiane degli italiani traspare in maniera chiara anche dalle scelte di consumo che essi fanno, le quali risultano semplificate dal mezzo digitale.
Se è chiara la rivoluzione in atto e l'enorme potenziale che si accompagna all'utilizzo delle tecnologie digitali in quanto strumenti abilitatori ormai indispensabili, non sfuggono i rischi ed i pericoli che imperversano nell'ecosistema digitale e nel mondo di internet in particolare.
A livello generale, infatti, è evidente la pervasività di strumenti come gli smartphone che accompagnano ininterrottamente ciascuno individuo nelle quotidiane attività lavorative e ricreative e la continua, e spesso pressante, stimolazione che da ciò ne discende con tutte le conseguenze che ne derivano e la difficoltà, piuttosto diffusa, di orientarsi in un contesto che richiede specifiche conoscenze e competenze.
A tale riguardo, appare certamente preoccupante e da non sottovalutare la situazione inerente il livello di competenze digitali in Italia, cruciali per la transizione digitale. Rispetto a tale indicatore, il nostro Paese è infatti relegato negli ultimi posti delle classifiche europee (per competenze digitali avanzate è penultima) e non può sottovalutarsi come fattori quali il divario di genere, di età, di istruzione e occupazionale, determinino differenze significative nello sviluppo favorevole di dette competenze.

Appare dunque fondamentale puntare sull'aumento dell'accessibilità rispetto a percorsi di formazione personalizzati che includano ogni individuo, compresa la popolazione più adulta. Solo in tal modo sarà possibile rendere il cyberspazio un luogo sicuro e caratterizzato da una partecipazione maggiormente consapevole.

*Appare preoccupante e da non sottovalutare la situazione inerente il livello di competenze digitali in Italia, in quanto esse sono cruciali per la transizione digitale. Rispetto a tale indicatore, il nostro Paese è relegato negli ultimi posti delle classifiche europee (per competenze digitali avanzate è penultima)*

Promuovere un utilizzo responsabile delle tecnologie e sfruttare il digitale per la sostenibilità ambientale rappresenta un obiettivo comune per la costruzione di un futuro più equilibrato, dove l'innovazione tecnologica e il benessere umano camminano di pari passo. La diminuzione degli spostamenti, la dematerializzazione dei processi, la gestione domotica dei consumi energetici sono solo alcuni degli esempi che evidenziano come il digitale semplifichi la vita delle persone e contribuisca a ridurre le emissioni, producendo un impatto positivo sulla società e un vantaggio significativo in termini di sostenibilità ambientale. Inoltre, il diritto all'accesso a forme di connettività evoluta rappresenta un fattore di inclusione sociale per tutte le fasce di popolazione e il territorio, producendo effetti positivi sulla medicina, sull'educazione, sul lavoro e sulla gestione del settore finanziario. Pertanto, investimenti volti a migliorare le nuove tecnologie come l'IoT, le reti 5G e i dispositivi mobili contribuiscono ad agevolare il cammino verso nuove forme di benessere sia per l'uomo che per l'ambiente.

L'uso problematico della rete può generare effetti gravosi sulla società, sia per l'individuo inteso come singolo, sia nei rapporti tipici che questo instaura con altri soggetti. Se consideriamo l'importanza che le piattaforme digitali e le nuove tecnologie hanno assunto a seguito della pandemia da Covid-19, è inevitabile far luce anche sui rischi che ne sono derivati. Uno dei più significativi è rivisto nelle campagne di disinformazione che avvengono mediante la diffusione di *fake news*. Queste possono essere amplificate quando il mezzo con cui vengono trasmesse ha caratteristiche digitali. Difatti, da anni l'UE conduce un'importante battaglia al fine di contrastare tale fenomeno, anche mediante la piattaforma online "EUvsDisinfo", nata nel 2015 per raccogliere a livello internazionale i casi di *disinformation* a cui il pubblico ha libero accesso. Anche l'*hate speech* desta considerevoli preoccupazioni, poiché incita e genera sentimenti discriminatori che possono essere sintomo di atti di violenza motivati da ragioni etniche, sociali, religiose o economiche. Dinanzi a questi rischi il ruolo delle piattaforme digitali è rilevante e *social network* come Facebook, Instagram e YouTube si impegnano a disporre policy interne volte a rimuovere prontamente contenuti illeciti o valutati come inadeguati. Va però detto che tali operazioni, spesso eseguite mediante algoritmi di IA, possono rivedere errori nella fase di valutazione della rimozione, per cui è prevista la possibilità di ripristinare quanto è stato eliminato o oscurato precedentemente.

Se tali rischi sembrano non risparmiare nessuno, certamente assumono straordinaria rilevanza rispetto ai minori che approcciano sempre più precocemente internet - soprattutto nei contesti sociali più vulnerabili - trovandosi a fronteggiare rischi e pericoli inediti senza essere attrezzati della necessaria consapevolezza, delle indispensabili competenze e spesso anche dell'indispensabile guida da parte degli adulti. In questo contesto, pur essendo in vigore strumenti normativi in grado di tutelare i minori (si pensi all'age verification e al parental control) appare elevata l'elusione della normativa e la conseguente necessità di mettere in atto iniziative di self regulation, come ad esempio, l'adozione di "patti sociali" che vedano coinvolte *in primis* le famiglie e magari anche le istituzioni per regolamentare innanzitutto l'età a partire dalla quale consentire l'utilizzo degli smartphone e l'accesso ad internet da parte dei minori. Iniziative siffatte consentirebbero, infatti, di garantire un percorso graduale e controllato dagli adulti (anche attraverso una sorta di sandbox in cui sperimentare in ambiente controllato le potenzialità del digitale) che consenta l'acquisizione del bagaglio di consapevolezza, conoscenza e competenze prodromiche per approcciare, in sicurezza, un ambiente certamente non progettato per i bambini. Uno dei fenomeni sicuramente più gravi e preoccupanti, seppur ancora limitatamente denunciato, è il cyberbullismo, che si presenta soprattutto tra i più giovani. Questi, infatti, attraverso l'uso della

tastiera e dello schermo, vivono una separazione dalla vittima, una sorta di virtualizzazione dei comportamenti che ostacola la percezione dei reali effetti della propria condotta. Perciò, è necessario che accanto alle famiglie, prime responsabili dell'educazione dei minori, le Istituzioni, soprattutto scolastiche, organizzino attività di sensibilizzazione, riconoscendo e monitorando le vittime, gli autori e puntando sull'aumento delle competenze del personale scolastico per affrontare in maniera più consapevole le reali problematiche degli studenti.
Le caratteristiche che rendono attrattivi i social media e i videogame possono generare un sovraccarico cognitivo, per cui l'utente riceve troppi stimoli dalla fonte e ciò può causare una vera e propria dipendenza dalla stessa. Si assiste ad una "bulimia informativa" che può provocare sintomi di ansia sociale, depressione, disturbi del sonno e basso rendimento scolastico. Per queste ragioni, le dipendenze da Internet e il *gaming disorder* oggi sono all'attenzione della comunità scientifica, che non punta a disincentivare l'impiego delle nuove tecnologie, ma piuttosto ne sollecita un utilizzo maggiormente consapevole, obiettivo fondamentale perpetrato anche mediante l'aumento del livello di sicurezza informatica all'interno della popolazione del web, a cui può conseguire una diminuzione del numero di attacchi mirati ad opera dei cybercriminali.

*Le dipendenze da Internet e il gaming disorder oggi sono all'attenzione della comunità scientifica, che non punta a disincentivare l'impiego delle nuove tecnologie, ma piuttosto ne sollecita un utilizzo maggiormente consapevole, obiettivo fondamentale perpetrato anche mediante l'aumento del livello di sicurezza informatica all'interno della popolazione del web*

Le strategie regolatorie individuate sia a livello nazionale che comunitario sul tema del benessere digitale si sono inizialmente incentrate sulla produzione di atti di *soft law*, tra i quali spicca il ricorso a codici di condotta e linee di orientamento inerenti specifiche materie come la disinformazione, il cyberbullismo, l'*hate speech* e la diffusione di contenuti criminali. Un simile approccio è divenuto insufficiente nel tempo, soprattutto data la necessità di uniformare il quadro legislativo sui servizi digitali, che appariva estremamente frammentato. La presentazione da parte della Commissione europea del *Digital Services package* ha reso concreto questo obiettivo, delineando un *framework* normativo idoneo a tutelare i cittadini della rete. In esso, la cooperazione pubblico-privata assume un ruolo centrale, poiché affida alle imprese che offrono servizi di condivisione di contenuti online la competenza nella regolamentazione dei servizi digitali, legittimando una forma di controllo e censura privata non sottoposta ad una previa valutazione parlamentare, amministrativa e giudiziaria, ma prevedendo allo stesso tempo una serie di obblighi a cui gli operatori devono rigorosamente sottostare. Ciò emerge particolarmente dalla lettura dei due regolamenti, che hanno finalità diverse ma dipendenti, in quanto il DMA vuole supportare l'equità e la contendibilità nei mercati digitali in cui sono presenti i *gatekeeper*, ossia le VLoPs (*Very Large Online Platforms*); mentre il DSA mira a rendere l'ambiente online sicuro, prevedibile e affidabile, incentivando l'innovazione e il progresso. Va evidenziato che queste norme non si applicheranno solo alle grandi piattaforme, ma verranno estese anche ad imprese di piccole e medie dimensioni che, seppur destinatarie di misure di semplificazione, saranno tenute a partecipare al mantenimento degli equilibri designati dalla disciplina sui servizi digitali. Inoltre, con queste iniziative prende forma l'intento dell'UE che, in particolare mediante il DSA, mette in pratica il tentativo di bilanciare sia l'interesse legato alla tutela dei diritti fondamentali e del

principio democratico, tangibile dall'imposizione di ordini di rimozione e di obblighi di *due diligence*, sia di salvaguardare la libera iniziativa e lo sviluppo economico, grazie all'esonero delle responsabilità e all'assenza degli obblighi di sorveglianza o accertamento attivo.

*Con queste iniziative prende forma l'intento dell'UE che, in particolare mediante il DSA, mette in pratica il tentativo di bilanciare sia l'interesse legato alla tutela dei diritti fondamentali e del principio democratico, tangibile dall'imposizione di ordini di rimozione e di obblighi di due diligence, sia di salvaguardare la libera iniziativa e lo sviluppo economico, grazie all'esonero delle responsabilità e all'assenza degli obblighi di sorveglianza o accertamento attivo*

Nella logica di assicurare tutele efficaci soprattutto in favore dei minori a livello nazionale è stata crescente l'attenzione, da ultimo con l'adozione del decreto Caivano, che ha imposto obblighi specifici in capo ai produttori di device e, nel frattempo a carico dei fornitori di servizi di TLC in materia di parental control, nella logica di diffondere e potenziare uno strumento che offre enormi opportunità in termini di efficacia.

Su questi temi I-Com ha effettuato a novembre 2023 due survey ad hoc.

Alla prima hanno risposto 280 studenti, di cui 201 delle scuole secondarie e 79 universitari. In sintesi, i dati evidenziano un livello elevato di attività online da parte degli studenti, con particolare riguardo ai social media e alle app di messaggistica. Gli stessi si ritengono molto informati in ambito di consapevolezza digitale, ciononostante vi sono comunque percentuali elevate di coloro che non saprebbero a chi rivolgersi in caso di pericoli digitali. A riguardo un'amplissima platea è stata contattata da soggetti apparentemente malintenzionati. Ciò evidenzia la necessità di sforzi maggiori per informare gli studenti rispetto alla sicurezza digitale. Nonostante il ruolo comunque fondamentale delle famiglie, rappresentano uno strumento importante le iniziative specifiche per accrescere la consapevolezza digitale. Queste sono fondamentali specialmente secondo i potenziali partecipanti, gli studenti, che hanno dichiarato in larga maggioranza di aver modificato i propri comportamenti dopo aver ricevuto maggiori informazioni sulla sicurezza in rete.

Alla seconda rilevazione hanno partecipato in totale 235 docenti, la maggior parte provenienti da scuole secondarie di secondo grado (42%), oltre che da scuole primarie (38%) e scuole secondarie di primo grado (20%). Tra i risultati più interessanti che sono emersi vi è il dato preoccupante circa il grado di consapevolezza in materia di rischi digitali, in quanto solo il 23% dei rispondenti ritiene che i propri studenti siano molto o abbastanza consapevoli sul punto. La dipendenza da Internet dei discenti sembra un pericolo percepito in maniera abbastanza diffusa tra gli insegnanti intervistati, così come la violazione della privacy e il cyberbullismo. Queste ultime due sono anche le problematiche per cui, più frequentemente, gli studenti si sono rivolti ai loro insegnanti. Preoccupante, invece, che il 29% degli insegnanti considerino poco o per niente utile essere coinvolti in iniziative formative sui pericoli della rete. Appare incoraggiante che la maggioranza dei rispondenti di tutte le tipologie di istituti consideri particolarmente importante sensibilizzare il gruppo classe con l'ausilio di esperti nell'uso etico delle tecnologie digitali, mentre la seconda voce

maggiormente selezionata pone l'attenzione sulle attività di sensibilizzazione indirizzate alle famiglie.

In conclusione, emerge che gli studenti di scuola secondaria sembrerebbero essere più sicuri degli universitari rispetto alle proprie capacità di autodifesa digitale. Questo però potrebbe spingerli ad adottare comportamenti meno prudenti rispetto a potenziali minacce. Infatti, solo una quota marginale dei docenti intervistati sostiene che i propri alunni siano sufficientemente consapevoli in ambito digitale. Tuttavia, è opportuno sottolineare come la principale fonte di informazione per gli studenti delle scuole secondarie siano proprio le iniziative in ambito scolastico, a differenza di quanto dichiarato dagli studenti universitari. Ciò potrebbe indicare una maggiore offerta negli ultimi anni di occasioni di sensibilizzazione e formazione su temi correlati al benessere digitale. Inoltre, sia gli studenti che i docenti segnalano un ruolo cruciale in capo alle famiglie. Ciononostante, una parte significativa di studenti segnala di non sapere a chi rivolgersi in caso di pericoli online e infatti larga parte dei docenti afferma che i propri discenti si rivolgono a loro per questioni legate, prevalentemente, alla privacy e al cyberbullismo.

*Una parte significativa di studenti segnala di non sapere a chi rivolgersi in caso di pericoli online e infatti larga parte dei docenti afferma che i propri discenti si rivolgono a loro per questioni legate, prevalentemente, alla privacy e al cyberbullismo*

**Lo studio I-Com – Join Group è stato realizzato nell'ambito di Futur#Lab, il progetto promosso da I-Com e WINDTRE, in collaborazione con Join Group e con la partnership di Ericsson e INWIT.**