

IL PREZZO NASCOSTO DELLA PIRATERIA

L'impatto sulla sicurezza degli utenti e sul futuro delle nuove generazioni

M. Cassoli, S. da Empoli, A. D'Amato, D. Salerno, G. Verolini

La pirateria danneggia i media che rivestono da sempre un ruolo centrale, non solo per il loro valore economico e produttivo, ma anche per la grande valenza qualitativa e culturale. La crescente diffusione della fruizione illegale di contenuti attraverso piattaforme pirata rappresenta oggi una minaccia che va ben oltre il perimetro industriale del settore media. Queste piattaforme, infatti, non sono semplici canali alternativi di accesso ai contenuti, ma ecosistemi opachi, spesso progettati per sottrarre dati personali, generare frodi e favorire attività di cybercriminalità. La pirateria digitale espone così un'ampia fascia di utenti a rischi informatici rilevanti, con impatti diretti sulla sicurezza individuale, e mette a repentaglio i tanti professionisti di oggi e di domani dell'industria creativa, nonché la sopravvivenza stessa delle aziende del settore.

- Nonostante il settore audiovisivo mobiliti miliardi di ricavi occupando decine di migliaia di persone, le aziende che lo popolano sono costantemente in lotta con una delle problematiche più subdole che affliggono questo genere di produzioni, la pirateria. Secondo gli ultimi dati disponibili, la fruizione illegale di contenuti è praticata da circa il 40% della popolazione adulta del nostro Paese.
- La pirateria mette a rischio anche chi la fa. Dall'analisi effettuata da I-Com sull'impatto economico delle minacce cibernetiche legate alla fruizione di contenuti illegali in rete e svolta sulla popolazione italiana over 16 è emerso che dal 2022 al 2024 vi è stato un incremento pari al 14,5%.
- I risultati mostrano che il danno economico pro capite è più elevato nella fascia 45-54 anni (1.507 €), seguita a breve distanza dagli individui tra i 55 e i 64 anni (1.505 €) e si mantiene per quasi tutte le altre classi di età al di sopra dei 1.000€. Difatti, il valore medio pro capite si attesta a €1.204 nel periodo considerato.
- Le piattaforme illegali non sono solo semplici canali per offrire la fruizione illegale di contenuti, ma sono spesso progettate anche per sottrarre dati, generare frodi e alimentare mercati paralleli di informazioni personali. In questi ambienti, estremamente vulnerabili, proliferano infatti malware, attacchi di phishing e altre minacce informatiche, oltre alla rivendita sistematica nei database del dark web dei dati personali sottratti.
- Guardando solamente al 2025, le stime I-Com indicano che la perdita di posti di lavoro nell'industria audiovisiva è di 3.399 posti di lavoro, di cui la maggior parte, con un dato pari a 2.677, imputabili all'attività economica 59.1, ovvero "Attività di produzione cinematografica, di video e di programmi televisivi".

- Nel complesso, ovvero considerando il periodo compreso tra il 2025 ed il 2030, si stima una perdita di ben 34.012 posti di lavoro, di cui 26.786 dovuti all'attività economica 59.1 "Attività di produzione cinematografica, di video e di programmi televisivi".

Il presente studio è aggiornato alla data del 10 febbraio 2026

SOMMARIO

PREMESSA	4
1. LA PIRATERIA AUDIOVISIVA IN ITALIA	5
1.1. <i>La fruizione di contenuti piratati in Italia.....</i>	5
1.2. <i>L'importanza del settore audiovisivo per l'economia italiana</i>	10
2. LA MINACCIA CYBER LEGATA ALLA FRUIZIONE DI CONTENUTI ILLEGALI.....	15
2.1. <i>I rischi per la sicurezza informatica legati alla pirateria digitale</i>	16
2.2. <i>Analisi I-Com sui rischi della fruizione di contenuti illegali online.....</i>	26
3. L'IMPATTO SOCIO-ECONOMICO DELLA PIRATERIA	32
3.1. <i>Introduzione metodologica.....</i>	32
3.2. <i>Stima dell'impatto della pirateria audiovisiva sulle prospettive occupazionali</i>	33
CONCLUSIONI E SPUNTI DI POLICY.....	39

PREMESSA

La pirateria audiovisiva rappresenta una minaccia non solo per chi fruisce di questi contenuti, ma anche per chi li produce e li trasmette. Da un lato, chi accede a contenuti pirata si espone a seri rischi legati alla cybersicurezza. Dall'altro, le aziende coinvolte nella creazione e distribuzione dei contenuti subiscono enormi perdite in termini di fatturato, valore economico e posti di lavoro, compromettendo la sostenibilità dell'intero ecosistema audiovisivo.

I fruitori di contenuti pirata si espongono innanzitutto a seri rischi legati alla cybersicurezza. Le piattaforme illegali, infatti, spesso nascondono malware, spyware e altre minacce informatiche che possono compromettere dati sensibili, esporre informazioni personali o persino consentire accessi non autorizzati ai dispositivi degli utenti.

Chi accede a questi contenuti, non fa un danno solo a sé stesso, ma sostiene anche circuiti illeciti e quindi contribuisce involontariamente alla perdita di opportunità lavorative per migliaia di professionisti del settore. Il danno all'ecosistema audiovisivo si manifesta in fasi diverse: inizialmente colpisce le aziende che distribuiscono i contenuti, compromettendone il fatturato e la capacità di investimento. Successivamente, l'impatto si estende anche alle aziende che producono i contenuti, mettendo a rischio la sostenibilità economica e i posti di lavoro nel settore creativo e tecnico. Inoltre, quello audiovisivo è un settore trainante che alimenta e interconnette numerosi altri comparti economici, come la produzione software o l'editoria. Alcuni di questi settori stanno già subendo i danni della pirateria, altri ne risentiranno fortemente nei prossimi anni.

1. LA PIRATERIA AUDIOVISIVA IN ITALIA

L'obiettivo di questa prima parte della ricerca è dimostrare con chiarezza l'impatto della pirateria sul settore audiovisivo, che sarà approfondito più nel dettaglio all'interno del capitolo 3. È fondamentale evidenziare che le stime effettuate nel presente studio si basano sui dati di un periodo in cui strumenti di contrasto come Piracy Shield non erano ancora attivi. Tali iniziative hanno bisogno di tempo e di una collaborazione diffusa per portare ancora più risultati: pur rappresentando un passo fondamentale nella lotta contro la pirateria, Piracy Shield non può avere un impatto immediato sull'andamento di questo segmento industriale. Solo con un impegno continuativo, con l'evoluzione delle tecnologie di protezione e con il sostanziale allargamento del suo raggio d'azione dai soli eventi sportivi in diretta a tutta una serie di contenuti audiovisivi *live* (incluse opere cinematografiche, serie tv e musica), come stabilito lo scorso 30 luglio dall'Agcom, Piracy Shield potrà iniziare a dare risultati tangibili, i cui effetti si evidenzieranno nel lungo periodo, permettendo di ridurre progressivamente l'efficacia delle reti di pirateria.

I dati raccolti dimostrano che negli ultimi anni i primi a subire le conseguenze della pirateria sono stati i broadcaster, il cui calo di fatturato evidenzia l'impatto diretto della diffusione illegale dei contenuti. Ora gli impatti si stanno spostando anche su chi produce contenuti: la crescita registrata in questo comparto tra il 2020 e il 2024 (legata anche alla ripresa degli investimenti al termine del periodo Covid) è destinata a subire un'inversione, riflettendo anche il danno accumulato nel periodo in cui mancavano strumenti come Piracy Shield.

1.1. La fruizione di contenuti piratati in Italia

Nonostante il settore audiovisivo mobiliti, come si dirà meglio nel paragrafo successivo, miliardi di ricavi occupando decine di migliaia di persone, le aziende che lo popolano sono costantemente in lotta con una delle problematiche più subdole che affliggono questo genere di produzioni, la pirateria. La fruizione illegale di contenuti audiovisivi è una piaga che pesa su questo settore da decenni ma che ha ricevuto un notevole impulso in tempi recenti grazie allo sviluppo dei canali digitali.

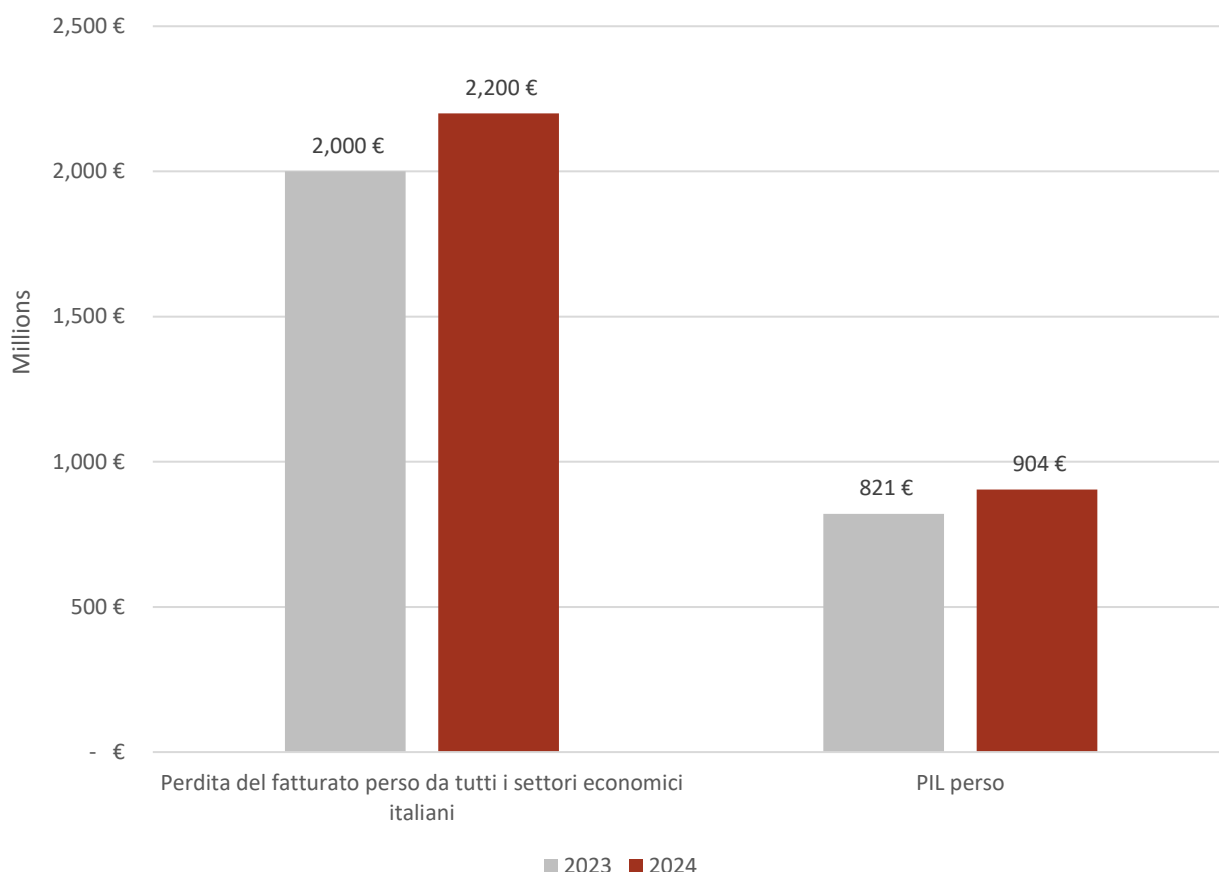
Nonostante il settore audiovisivo mobiliti miliardi di ricavi occupando decine di migliaia di persone, le aziende che lo popolano sono costantemente in lotta con una delle problematiche più subdole che affliggono questo genere di produzioni, la pirateria

Una chiara fotografia delle dimensioni di questo fenomeno ci arriva dal rapporto annuale realizzato da Fapav e Ipsos sulla pirateria audiovisiva in Italia. Lo studio mostra chiaramente come gli effetti negativi per l'economia nazionale derivanti dalla fruizione illegale di contenuti audiovisivi è preoccupantemente ampia e non si limita al solo comparto audiovisivo (Fig.1.1). La perdita di fatturato complessiva in tutti i settori economici, secondo le stime, ha superato nel 2024 i due miliardi di euro (+10% rispetto al 2023). Notevole è anche l'impatto sul PIL nazionale, pari a 904 milioni di euro (+10%).

La perdita di fatturato complessiva in tutti i settori economici, secondo le stime, ha superato nel 2024 i due miliardi di euro (+10% rispetto al 2023). Notevole è anche l'impatto sul PIL nazionale, pari a 904 milioni di euro (+10%)

Fig.1.1: Stima dei danni economici della pirateria audiovisiva in Italia (€milioni)

Fonte: Ricerca Fapav/Ipsos sulla pirateria audiovisiva in Italia (giugno 2025)

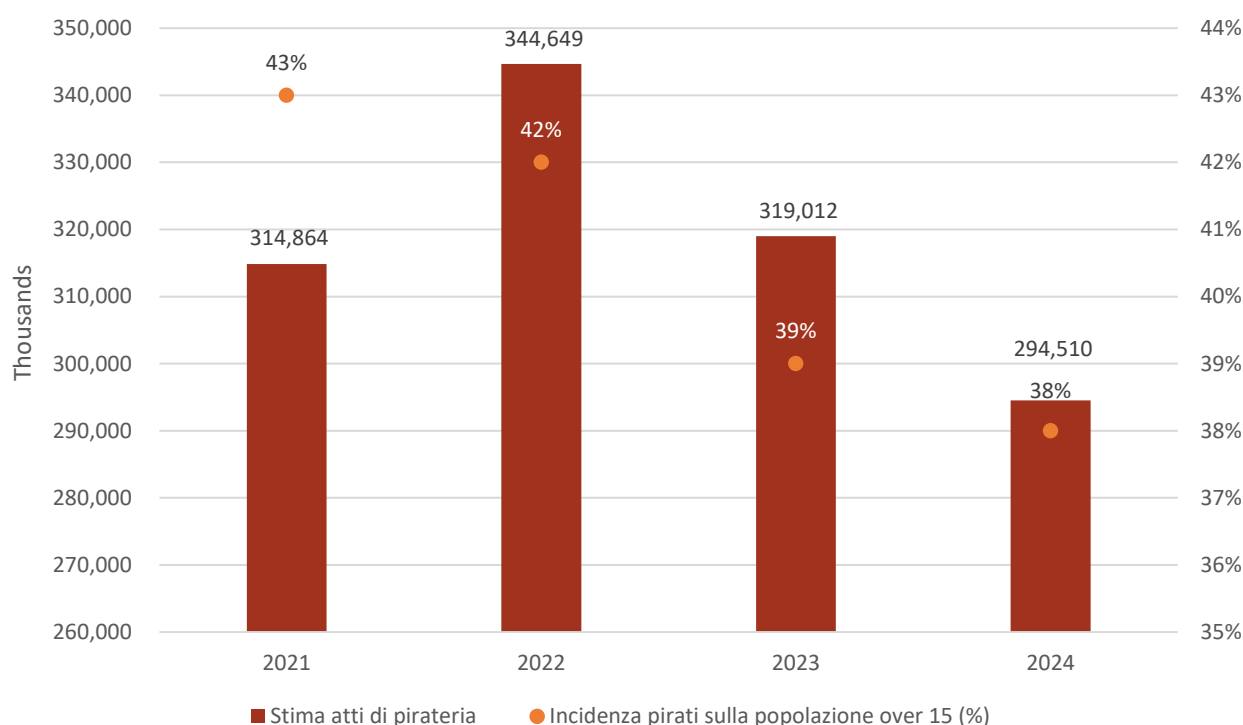


Scendendo nel dettaglio dei contenuti dello studio, il primo dato interessante da analizzare è quello relativo al numero di fruizioni di contenuti illegali e all'incidenza di questo sulla popolazione. Il numero di atti di pirateria realizzati in Italia annualmente supera costantemente le 290 milioni di unità e coinvolge circa il 40% della popolazione adulta nel nostro Paese (Fig.1.2).

Il numero di atti di pirateria realizzati in Italia annualmente supera costantemente le 290 milioni di unità e coinvolge circa il 40% della popolazione adulta nel nostro Paese

Fig.1.2: Incidenza della pirateria audiovisiva in Italia tra la popolazione adulta

Fonte: Ricerca Fapav/Ipsos sulla pirateria audiovisiva in Italia (giugno 2025)



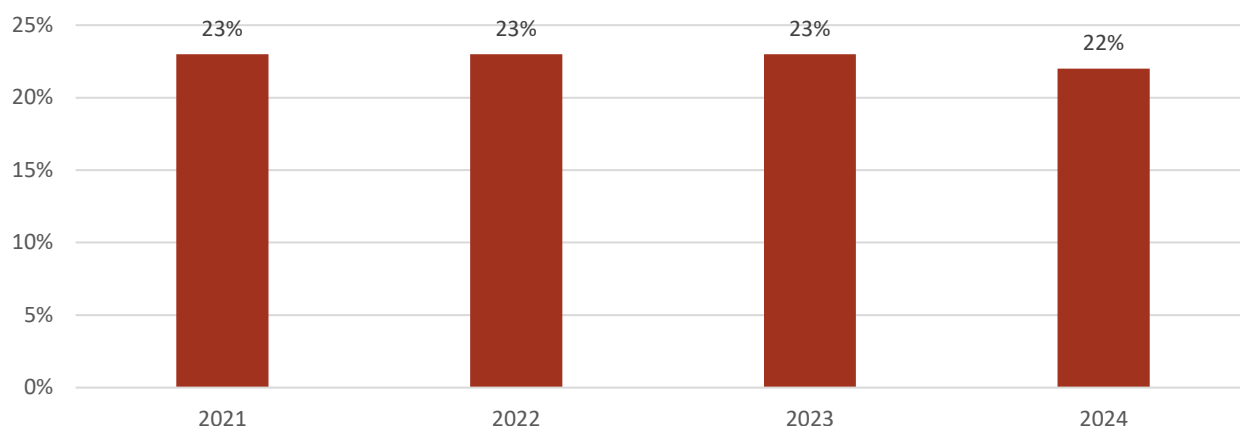
Uno degli strumenti più problematici legati al mondo delle pirateria sono le IPTV (*Internet Protocol Television*) illecite. Questi sistemi permettono agli utenti della rete di fruire di programmi televisivi in diretta attraverso i propri device grazie ad una connessione ad internet. Nonostante siano pensati per trasmettere contenuti leciti e vengano largamente utilizzati in maniera regolare, purtroppo questi strumenti sono diventati una delle armi più potenti in mano a chi pirata contenuti audiovisivi. Le IPTV permettono infatti di diffondere su canali paralleli e illegali prodotti audiovisivi di vario genere, dai film e le serie tv allo sport live, in molti casi facendosi pagare dall'utenza un abbonamento parallelo che drena notevoli risorse al legittimo proprietario dei diritti di trasmissione.

Le IPTV permettono infatti di diffondere su canali paralleli e illegali prodotti audiovisivi di vario genere, dai film e le serie tv allo sport live, in molti casi facendosi pagare dall'utenza un abbonamento parallelo che drena notevoli risorse al legittimo proprietario dei diritti di trasmissione

Secondo le rilevazioni effettuate da Fapav e Ipsos, l'incidenza di utilizzo delle IPTV illecite tra la popolazione adulta italiana rimane sostanzialmente stabile negli anni. La quota di individui che utilizza questi sistemi è infatti pari al 22% nel 2024, in leggero decremento rispetto a quanto registrato negli anni precedenti (-1%) (Fig.1.3).

Fig.1.3: Incidenza di utilizzo delle IPTV illecite tra la popolazione adulta

Fonte: Ricerca Fapav/Ipsos sulla pirateria audiovisiva in Italia (giugno 2025)

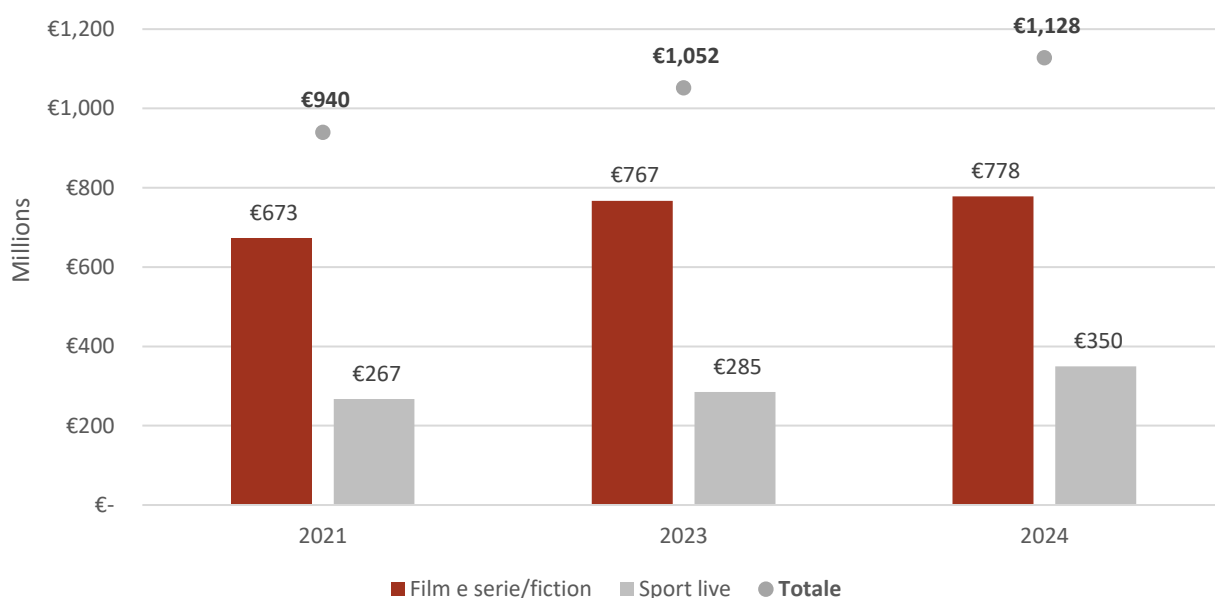


La conseguenza del fenomeno della pirateria è inevitabilmente un danno economico per le aziende del settore e, di conseguenza, per l'intero Paese. Il Rapporto Fapav/Ipsos stima che il danno economico diretto per le attività che caratterizzano questo comparto sia ammontato nel 2024 a 1,12 miliardi di euro, in crescita di quasi l'8% rispetto alla rilevazione precedente (Fig.1.4).

Il danno economico diretto della pirateria è ammontato nel 2024 a 1,12 miliardi di euro, in crescita di quasi l'8% rispetto alla rilevazione precedente

Fig.1.4: Danno potenziale in termini di fatturato perso direttamente a causa della mancata fruizione legale di film, serie/fiction e sport live a causa della pirateria

Fonte: Ricerca Fapav/Ipsos sulla pirateria audiovisiva in Italia (giugno 2025)

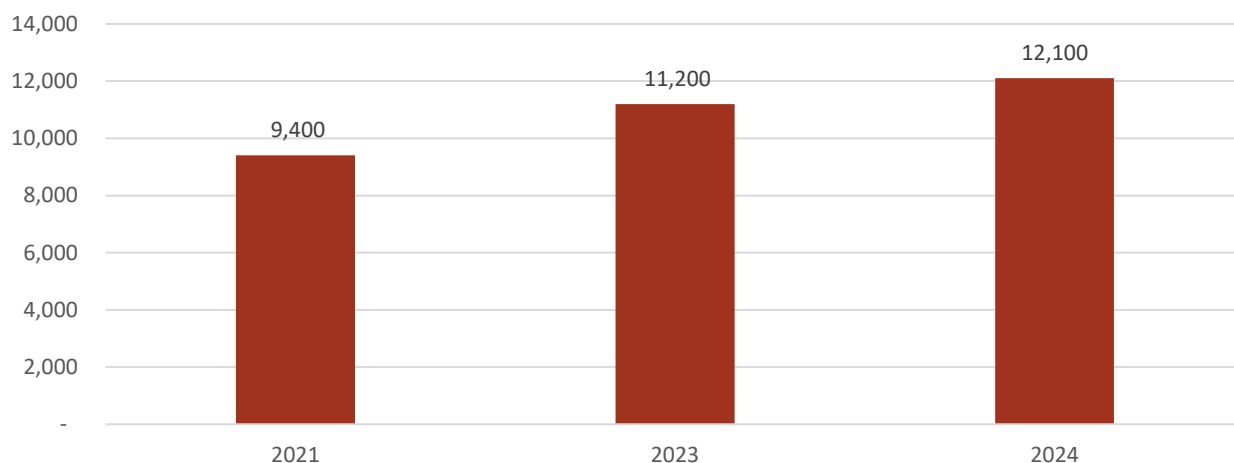


La perdita economica derivante dalla pirateria non può non avere un effetto sull'occupazione. I ritorni economici persi a causa della mancata fruizione legale dei prodotti audiovisivi risultano sia in un peggioramento delle performance economiche delle aziende del settore che in minori risorse da investire nella realizzazione di nuovi prodotti. Ipsos e Fapav stimano per il 2024 circa 12.100 posti di lavoro a rischio a causa della pirateria audiovisiva in tutti i settori dell'economia italiana, in crescita dell'8% rispetto al 2023 (Fig.1.5).

Ipsos e Fapav stimano per il 2024 circa 12.100 posti di lavoro a rischio a causa della pirateria audiovisiva in tutti i settori dell'economia italiana, in crescita dell'8% rispetto al 2023

Fig.1.5: Stima potenziale dei posti di lavoro a rischio in tutti i settori economici a causa della pirateria audiovisiva

Fonte: Ricerca Fapav/Ipsos sulla pirateria audiovisiva in Italia (giugno 2025)



Nell'analisi della pirateria audiovisiva in Italia è senza dubbio utile analizzare anche le misure intraprese per arginare questo preoccupante fenomeno. In particolare, lo strumento principe adottato in Italia per contrastare la fruizione illegale di contenuti audiovisivi è la piattaforma *Piracy Shield*. Questa è stata istituita con la legge 14 luglio 2023, n. 93, che ha attribuito all'AgCom più ampi poteri per una più efficace e tempestiva azione a contrasto degli atti di pirateria on line.

Lo strumento principe adottato in Italia per contrastare la fruizione illegale di contenuti audiovisivi è la piattaforma Piracy Shield

Nella sostanza, i titolari dei diritti delle opere piratate segnalano sulla piattaforma gli indirizzi IP che stanno trasmettendo i contenuti in maniera illecita. Dopo l'inserimento i fornitori di servizi internet hanno 30 minuti per bloccare l'accesso a tali siti. Secondo i dati diffusi nella Relazione Annuale Agcom 2025, tra il 1° maggio 2024 e il 30 aprile 2025 sono stati disabilitati 28.041 domini e 6.104 indirizzi IP che diffondevano in maniera illecita eventi sportivi in diretta.

1.2. L'importanza del settore audiovisivo per l'economia italiana

Fin dall'invenzione del cinematografo nel 1895 la produzione audiovisiva ha catalizzato l'attenzione di intere generazioni di individui. I prodotti audiovisivi si sono rivelati nel corso del tempo sia una delle più importanti forme di intrattenimento della storia umana che uno strumento fondamentale per la diffusione e la valorizzazione della cultura. Attraverso una modalità facilmente accessibile e comprensibile per gran parte della popolazione globale, le produzioni audiovisive hanno contribuito alla diffusione della conoscenza in numerosi ambiti come la storia, la società, la politica, l'arte, la letteratura, la musica, lo sport, ecc.

Il comparto audiovisivo genera nel nostro paese un importantissimo indotto economico e occupazionale

L'importanza di questo settore non si esaurisce esclusivamente nell'aspetto culturale. Infatti, il comparto audiovisivo genera nel nostro Paese un importantissimo indotto economico e occupazionale.

Secondo gli ultimi dati resi disponibili dall'Istat, le aziende che si occupano di audiovisivo in Italia, ovvero afferenti ai 6 codici Ateco a tre cifre contenuti nella categoria J, generano ricavi per oltre 21,6 miliardi di euro e occupano quasi 80 mila addetti (Fig.1.6). I principali pilastri di quest'industria sono l'edizione di libri, periodici ed altre attività editoriali (58.1), le attività di produzione cinematografica, di video e di programmi televisivi (59.1) e l'attività di programmazione e trasmissioni televisive (60.2), che generano ricavi rispettivamente per 7,6, 6,3 e 6,3 miliardi di euro.

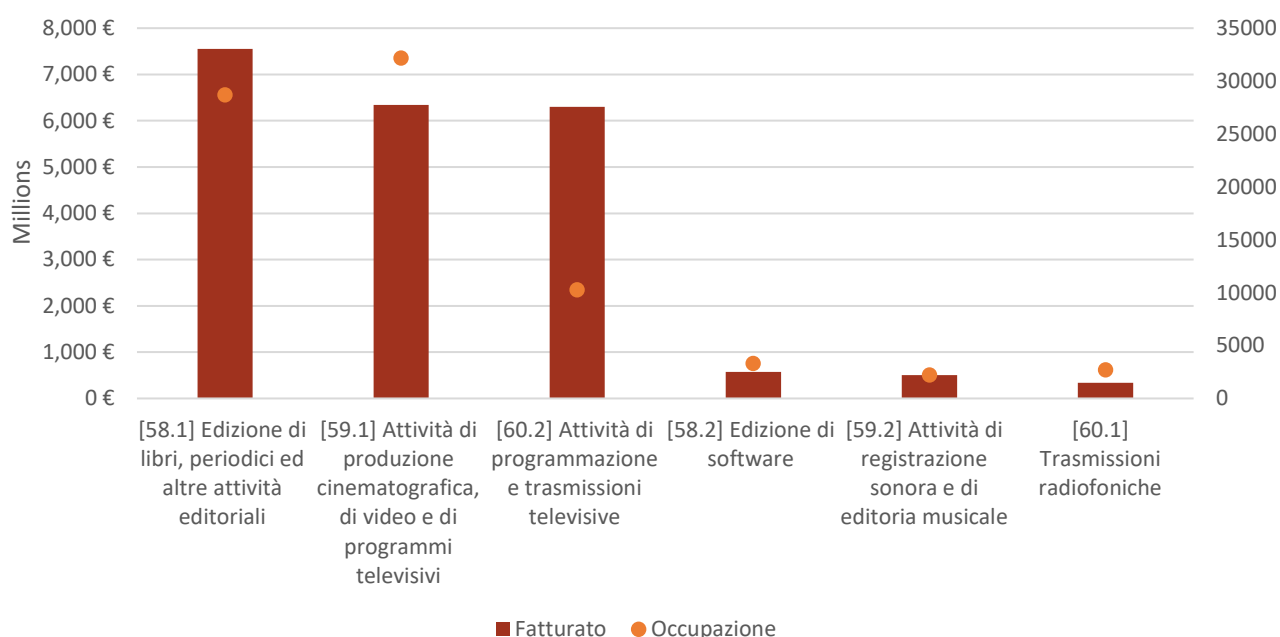
I medesimi tre codici Ateco sono quelli che prevalgono per livelli occupazionali. In questo caso, a primeggiare è il versante della produzione cinematografica, che coinvolge oltre 32 mila addetti, seguito da l'editoria tradizionale (28,7 mila) e dalla trasmissione (10,2 mila). I restanti tre codici Ateco considerati nel comparto risultano molto distaccati in termini dimensionali dai primi tre, generando complessivamente un fatturato di 1,4 miliardi e un'occupazione di circa 8,2 mila unità.

L'importanza di questo settore non si esaurisce esclusivamente nell'aspetto culturale. Infatti, il comparto audiovisivo genera nel nostro Paese un importantissimo indotto economico e occupazionale.

Secondo gli ultimi dati resi disponibili dall'Istat, le aziende che si occupano di audiovisivo in Italia, ovvero afferenti ai 6 codici Ateco a tre cifre contenuti nella categoria J, generano ricavi per oltre 21,6 miliardi di euro occupando quasi 80 mila addetti

Fig.1.6: Fatturato e occupazione del settore audiovisivo in Italia (2023)

Fonte: Istat



I principali pilastri di quest'industria sono l'edizione di libri, periodici ed altre attività editoriali (58.1), le attività di produzione cinematografica, di video e di programmi televisivi (59.1) e l'attività di programmazione e trasmissioni televisive (60.2) che generano ricavi rispettivamente per 7,6, 6,3 e 6,3 miliardi di euro

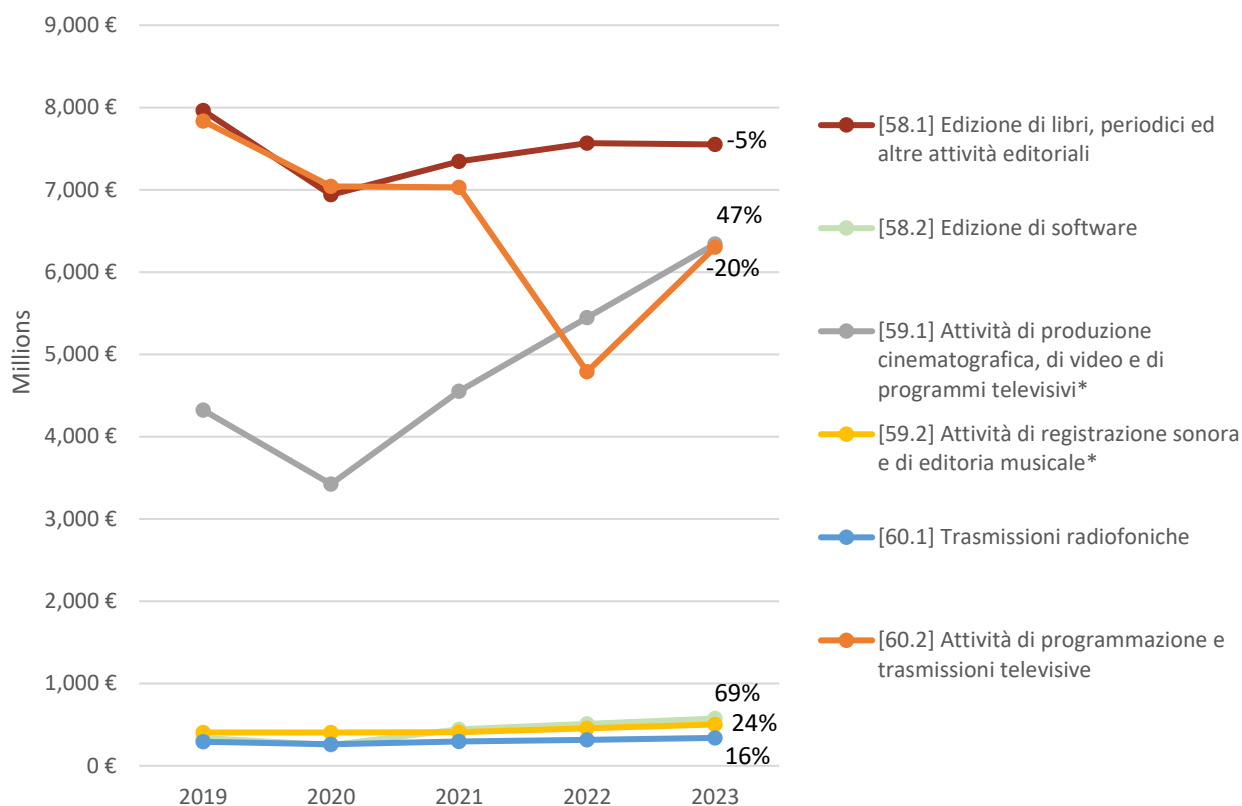
Passando all'analisi degli andamenti delle singole variabili del settore negli ultimi anni, si osserva invece come sia sul versante del fatturato che su quello dell'occupazione vi siano notevoli differenze tra i vari codici Ateco considerati in quest'analisi (Fig.1.7). Per quanto riguarda il fatturato, due delle attività principali del comparto, l'editoria tradizionale e le trasmissioni televisive, mostrano segnali di difficoltà, con una contrazione rispettivamente del 5% e del 20% rispetto ai livelli del 2019.

A trainare i ricavi complessivi del settore è stata invece la produzione cinematografica, unica dei tre pilastri principali a registrare una crescita significativa nel periodo analizzato (+47% rispetto al 2019). Relativamente agli altri codici Ateco, tutte e tre le attività considerate presentano un incremento rispetto al 2019. Particolarmente rilevante è la crescita del comparto software (+69%), che, pur mantenendosi su valori assoluti ancora contenuti, rappresenta un segmento in rapida espansione all'interno del settore.

Fig.1.7: Andamento fatturato delle aziende del comparto audiovisivo nel periodo 2019-2023

*i dati per il 2022 delle attività 59.1 e 60.2 sono stati stimati in mancanza di dati ufficiali pubblicati da ISTAT

Fonte: Istat

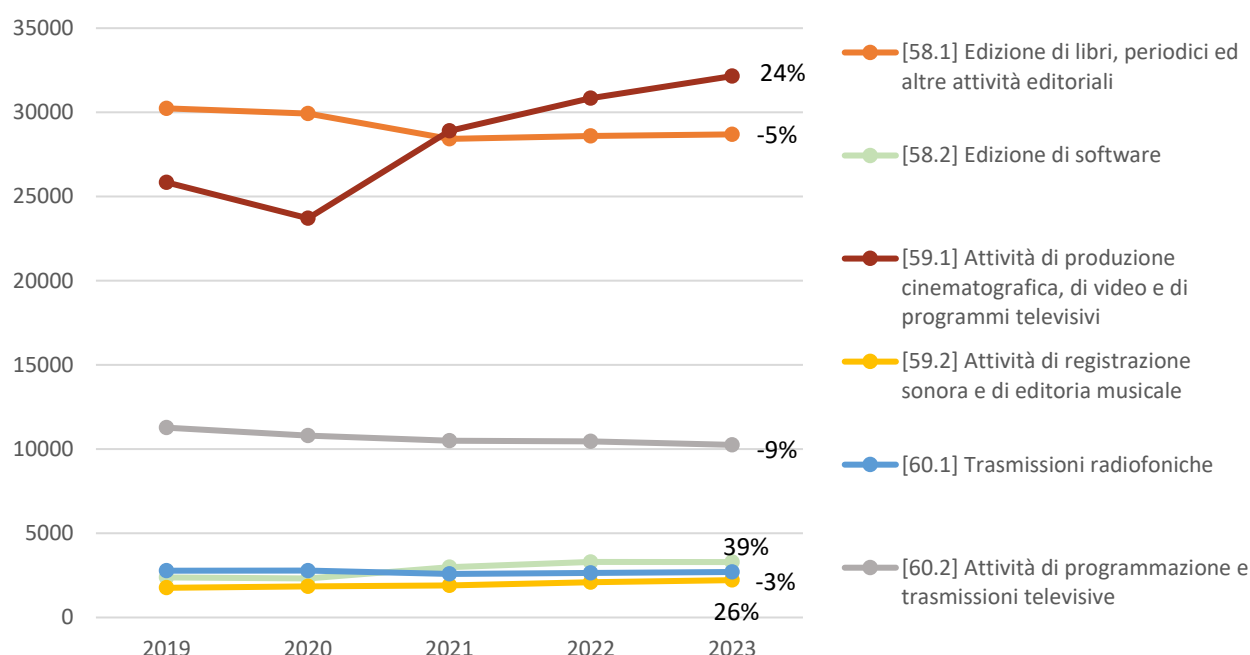


Per quanto riguarda il fatturato, due delle attività principali del comparto, l'editoria tradizionale e le trasmissioni televisive, mostrano segnali di difficoltà, con una contrazione rispettivamente del 5% e del 20% rispetto ai livelli del 2019. A trainare i ricavi complessivi del settore è stata invece la produzione cinematografica, unico dei tre pilastri principali a registrare una crescita significativa nel periodo analizzato (+47% rispetto al 2019)

Relativamente all'occupazione, analizzando i dati relativi al periodo 2019-2023 è possibile notare come anche in questo caso l'unico dei pilastri del settore a presentare una variazione positiva sia la produzione cinematografica (+24%). L'editoria e le trasmissioni televisive mostrano ancora una volta un andamento discendente (rispettivamente -5% e -9% rispetto al 2019) (Fig.1.8). Tra le ragioni più importanti che hanno portato a questo calo, come vedremo maggiormente nel dettaglio nel capitolo 3, spicca certamente la pirateria, fattore che non permette alle aziende di realizzare il pieno valore potenziale delle opere prodotte e distribuite. I settori più vicini al consumatore sono infatti i primi a sperimentare gli effetti negativi dei mancati ricavi derivanti dalla fruizione illegale dei contenuti.

Fig.1.8: Numero di occupati nelle aziende appartenenti al comparto audiovisivo italiano (2019-2023)

Fonte: Istat



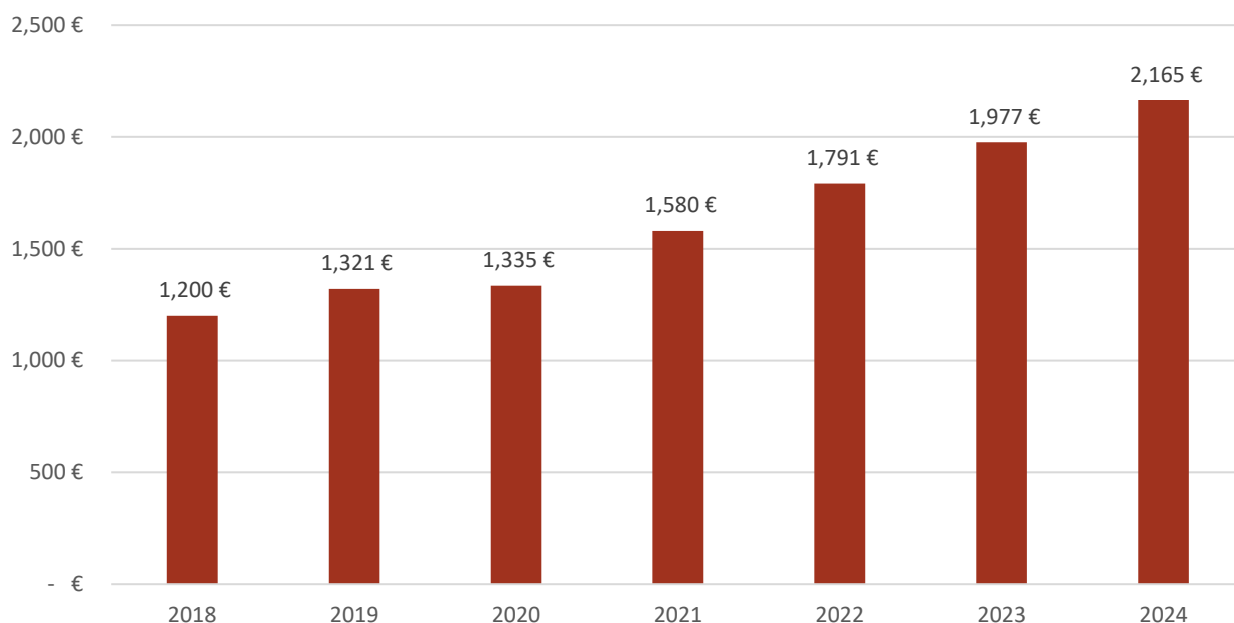
Tra le ragioni più importanti che hanno portato a questo calo, spicca certamente la pirateria, fattore che non permette alle aziende di realizzare il pieno valore potenziale delle opere prodotte e distribuite. I settori più vicini al consumatore sono infatti i primi a sperimentare gli effetti negativi dei mancati ricavi derivanti dalla fruizione illegale dei contenuti

Nonostante performance economiche non sempre brillanti, le aziende che popolano il settore audiovisivo in Italia hanno continuato negli anni ad accrescere i propri investimenti in opere audiovisive originali (Fig.1.9). In particolare, osservando i dati contenuti all'interno dell'ultimo "Rapporto sulla Produzione Audiovisiva Nazionale", realizzato da APA, si può notare come la spesa per creare nuove produzioni sia quasi raddoppiata nel periodo 2018-2024 (+80%).

Nonostante performance economiche altalenanti, le aziende che popolano il settore audiovisivo in Italia hanno continuato negli anni ad accrescere i propri investimenti in opere audiovisive originali. In particolare, osservando i dati contenuti all'interno dell'ultimo "Rapporto sulla Produzione Audiovisiva Nazionale", realizzato da APA, si può notare come la spesa per creare nuove produzioni sia quasi raddoppiata nel periodo 2018-2024 (+80%)

Fig.1.9: Volume complessivo degli investimenti in opere audiovisive originali (€milioni)

Fonte: 7° Rapporto sulla Produzione Audiovisiva Nazionale – APA

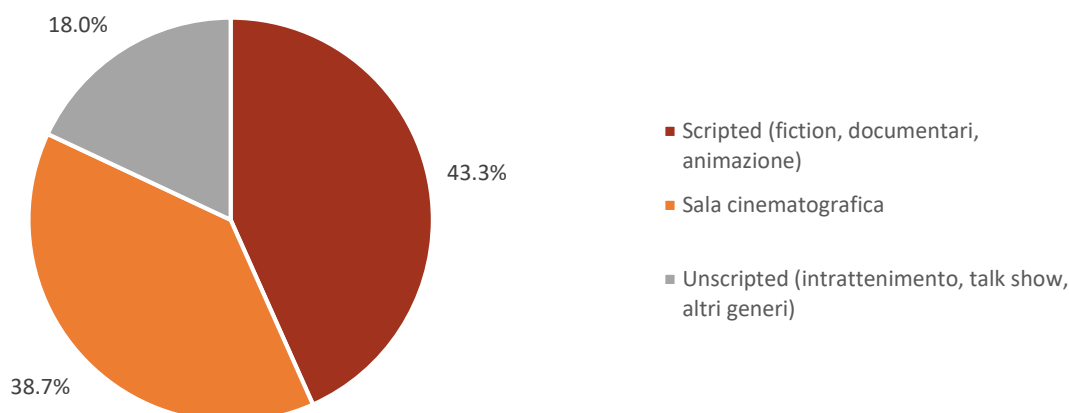


Da notare anche la varietà dell'offerta di opere originali prodotte in Italia. I dati APA ci restituiscono, infatti, uno scenario che si articola in tre principali componenti. Le tipologie di opere che assorbono larga parte delle risorse investite sono fiction, documentari e animazione (43,3%), seguite con un breve distacco dai film in sala (38,7%). Una minore incidenza hanno invece i prodotti di intrattenimento, talk show e altri generi residuali, che comunque insieme mobilitano oltre il 18% delle risorse investite, pari a 390 milioni di euro (Fig.1.10).

Fig.1.10: Quota di investimenti per tipologia di opera prodotta (2024)

Note: I valori sono da considerarsi stimati

Fonte: 7° Rapporto sulla Produzione Audiovisiva Nazionale – APA



2. LA MINACCIA CYBER LEGATA ALLA FRUIZIONE DI CONTENUTI ILLEGALI

Negli ultimi anni, la diffusione di contenuti digitali ha subito una crescita esponenziale, con un incremento significativo nell'accesso a film, musica, software e trasmissioni in streaming live e on demand attraverso canali non autorizzati. La fruizione di questi contenuti tramite modalità non consentite dalla legge può condurre a un grave rischio per la sicurezza informatica degli utenti, sia nel caso in cui il servizio sia gratuito, sia - a maggior ragione - nell'ipotesi di servizi pirata in abbonamento, poiché l'utente - soprattutto nei casi in cui abbia un livello basso in termini di consapevolezza digitale - tende a fornire le proprie informazioni personali, inclusi i dati relativi al metodo di pagamento.

In questo scenario, un report ha rilevato che nel Regno Unito il 76% dei siti pirata più visitati nel Paese sta attivamente esponendo gli utenti a truffe, frodi di natura economico-finanziaria e contenuti espliciti, rappresentando in tal senso una grave minaccia per la sicurezza online degli utenti, soprattutto più giovani. Un ulteriore studio effettuato sulla popolazione adulta in Australia evidenzia che il rischio di ricevere un virus o un'altra tipologia di malware sul dispositivo utilizzato per la visione di contenuti multimediali in streaming sarebbe circa dieci volte maggiore nei soggetti che fruiscono di prodotti piratati rispetto ai non piratati. Per quanto riguarda l'Italia, un primo studio in merito è quello presentato da FAPAV/Ipsos a dicembre 2025, che ha indagato il target d'età 15-25 anni, mostrando come il 62% dei pirati in questa fascia di età ha subito attacchi informatici nel corso degli anni. Oltre ciò, è opportuno evidenziare che il rapporto tra rischi informatici e pirateria online va ben oltre considerazioni di natura meramente economica, potendo palesarsi altresì conseguenze in ambito legale, reputazionale, nonché in termini di perdita della privacy e del controllo sui propri dati personali.

Ciò premesso, l'ultima sezione di questa seconda parte si focalizza su un'analisi di impatto economico per verificare quanto le minacce cibernetiche correlate al fenomeno della pirateria digitale impattino sulla popolazione italiana, opportunamente differenziata per fasce di età e titolo di studio. Partendo dal risultato finale, si è potuto evidenziare che il danno economico è aumentato nel tempo, passando da €1,24 miliardi del 2022, a €1,32 miliardi del 2023, fino a superare €1,42 miliardi nel 2024. Pertanto, si può affermare che su base triennale è stato registrato un aumento del 14,5% in termini di impatto economico delle minacce cibernetiche sulla popolazione italiana over 16.

Rispetto al titolo di studio, è stata operata una distinzione tra individui non laureati e laureati e ne è risultato che questi ultimi presentano un'incidenza dei danni da pirateria più elevata rispetto alla popolazione generale. In ultimo, è stato osservato un andamento crescente nel tempo in termini di danno economico, dove il range 35-44 anni è quello maggiormente impattato, essendo passato dai €259 milioni del 2022 ai €340 milioni del 2024, seguito dagli individui tra i 45-54 anni (da €227 a €300 milioni) e dalla fascia 25-34 anni (da €216 a €293 milioni). In definitiva, è possibile affermare che, oltre al danno economico per l'industria audiovisiva evidenziato negli altri capitoli, i dati relativi ai cyberattacchi dimostrano come la pirateria comporti gravi conseguenze anche per i consumatori. Contrastare la pirateria è dunque fondamentale non solo per proteggere il settore, ma anche per tutelare gli utenti.

2.1. I rischi per la sicurezza informatica legati alla pirateria digitale

Negli ultimi anni, la diffusione di contenuti digitali ha subito una crescita esponenziale, con un incremento significativo nell'accesso a film, musica, software e trasmissioni in streaming live e on demand attraverso canali non autorizzati. La fruizione di questi contenuti tramite modalità non consentite dalla legge può condurre a un grave rischio per la sicurezza informatica degli utenti. Difatti, le piattaforme che offrono questi servizi in maniera illegale sono pensate e costruite appositamente per generare truffe e furti di identità, per cui costituiscono un ambiente fertile per la diffusione di malware, attacchi di phishing e altre minacce cibernetiche. Ciò vale, come si vedrà meglio in seguito, sia nel caso in cui il servizio sia gratuito ("se il prodotto è gratuito, il prodotto sei tu" per il tramite dei dati e delle informazioni personali cedute), sia nelle ipotesi – sempre più diffuse – di servizi pirata in abbonamento.

Le piattaforme che offrono questi servizi in maniera illegale sono pensate e costruite appositamente per generare truffe e furti di identità, per cui costituiscono un ambiente fertile per la diffusione di malware, attacchi di phishing e altre minacce cibernetiche

Pertanto, va considerato che un simile meccanismo si verifica quotidianamente in uno scenario in base al quale attraverso il web transitano in ogni istante diversi attori che agiscono per innumerevoli scopi e tra questi un ruolo sempre più preoccupante e insidioso è svolto da singoli individui ma – soprattutto – dalle organizzazioni cybercriminali. Queste ultime, dopo aver violato la sicurezza di uno o più sistemi informatici, carpiscono in maniera mirata o a tappeto le informazioni ivi contenute e le utilizzano successivamente per una o più finalità specifiche, tra cui quelle di tipo economico-finanziario, le quali rappresentano il nucleo delle attività condotte dai cybercriminali, garantendo introiti più o meno consistenti nel tempo in considerazione di una serie di fattori, come le misure di sicurezza adottate dall'utente, il livello di consapevolezza digitale, l'intensità delle attività di contrasto e così via.

Ciò premesso, è possibile delineare le principali tipologie di attacco in ambito cybercrime che possono palesarsi quando si effettuano attività di pirateria online. Un'assoluta rilevanza in questo contesto è riconosciuta al *malware*, che si sostanzia nell'esecuzione – spesso inconsapevole – di software malevoli sul dispositivo mobile o fisso dell'utilizzatore di contenuti illegali in rete (es: navigando sui siti e i portali pirata ci si imbatte in molti link, banner e schermate pop-up che possono reindirizzare l'utente verso siti web dannosi). Più nel dettaglio, le principali fonti tramite le quali i *malware* infettano il dispositivo utilizzato per consumare prodotti pirata sono:

- a) siti web verso cui l'utente viene attirato e che contengono software malevolo mascherato da giochi, aggiornamenti di sistema e/o promesse di denaro. Pertanto, queste piattaforme utilizzano spesso la pubblicità come vettore per il download dei *malware*;
- b) "P2P File Sharing", che riguarda il download di contenuti pirata tramite file .torrent, i quali a loro volta nascondono un malware auto-eseguibile sul dispositivo della vittima;

- c) e-mail di phishing¹ contenenti link o allegati con un *malware* incorporato, così come app indicate come necessarie alla fruizione dei contenuti pirata – che all'apparenza possono sembrare lecite, ma sono sostanzialmente malevole – fatte scaricare da siti web anziché da app store ufficiali. Gli allegati possono essere di diverse tipologie, pdf o file video condivisi tramite app di messaggistica, che risultano malevoli una volta aperti dall'utente.

Tra i *malware*, quelli maggiormente diffusi sono i seguenti:

- *virus* = permette di creare una copia dei file infettati;
- *trojan* = ha la particolarità di celarsi dietro a file o software legittimi, ingannando gli utenti e ottenendo così accesso non autorizzato ai loro sistemi e di conseguenza ai dati ivi contenuti, come la posizione tramite la geolocalizzazione, gli sms, il registro chiamate, le conversazioni tramite il microfono, immagini e video tramite la fotocamera e/o screenshot.. In alcuni casi può garantire anche il controllo da remoto dei dispositivi infettati;
- *spyware* = permette di ottenere alcune informazioni, senza consenso, sulla navigazione online dell'utente;
- *keylogger* = consente di acquisire tutto ciò che viene digitato sulla tastiera;
- *browser hijacking* = consiste nel dirottare la navigazione online dell'utente verso determinati siti web al fine di acquisire informazioni sull'identità dello stesso;
- *ransomware* = blocca l'accesso del dispositivo che infetta, cifrando i file ivi contenuti. Per poter riavere i propri dati, nuovamente accessibili e leggibili, viene chiesto un riscatto e l'estorsione può essere forzata dalla minaccia di rendere pubbliche le informazioni più sensibili presenti nei sistemi attaccati (es: documenti di identità, brevetti, informazioni confidenziali o dati personali dei clienti) per amplificare i potenziali danni reputazionali e spingere così la vittima al pagamento illecito.

Gli effetti dannosi per l'utente possono essere molteplici: i) l'intercettazione del traffico di rete e delle credenziali bancarie digitate durante la navigazione per commettere frodi, come nel caso del pagamento di beni e servizi tramite transazioni online; ii) facilitare il furto di identità dell'utente, ottenendo i numerosi dati personali memorizzati sul dispositivo; iii) il movimento laterale (*lateral movement*) all'interno della rete domestica o di altro a cui si connette/connetterà il dispositivo dell'utente per compromettere allo stesso modo altri dispositivi².

A titolo di esempio può essere riportato il caso, ormai particolarmente diffuso, di un utente che sceglie di utilizzare una piattaforma online che include un vasto catalogo di contenuti multimediali piratati, come nel caso di una serie TV appena rilasciata. Pertanto, sarà tenuto a cliccare su "play" per avviare la riproduzione ed è proprio in quella circostanza che si apriranno una o più finestre pop-up che lo inviteranno a scaricare "un video player aggiornato" (o formule analoghe) e/o a registrarsi per accedere al contenuto "gratuitamente". Ebbene, procedendo in questo senso, l'utente del caso di specie avrà avviato l'installazione di un trojan, uno *spyware* o un *keylogger* – così come definiti sopra – che consentono all'attore malevolo (mosso tendenzialmente da motivazioni economiche) di accedere da remoto al dispositivo della vittima. Peraltro, se l'utente in questione avrà fornito i propri dati e le credenziali di autenticazione – che magari utilizza anche

¹ Il phishing si sostanzia nell'utilizzo di mail o altri mezzi di comunicazione allo scopo di ingannare la vittima facendole fare cose o fornire informazioni che normalmente non farebbe o non fornirebbe (es: click su un link che conduce a un sito web dove si richiede di creare un'utenza pirata tramite indicazione – quantomeno – di un indirizzo e-mail e dei dati personali di base).

² Audiovisual Anti-Piracy Alliance (AAPA), Audiovisual piracy cyber risk for European consumers. The rise of malware, settembre 2022.

per altri portali o siti web, tra cui i social network – questi senza ombra di dubbio andranno ad alimentare i database venduti nel dark web, facendo finire l’identità digitale della vittima nelle dinamiche tipiche dell’underground cybercriminale.

Altra casistica, altrettanto diffusa, è quella in cui l’utente utilizza un’applicazione o un sito P2P per scaricare sul dispositivo contenuti .torrent (*P2P File Sharing* sopra menzionato), mostrando chiaramente il proprio indirizzo IP ad altri *peer*³, inclusi eventuali attori malevoli, con la conseguenza di incorrere nel rischio che la rete domestica/aziendale a cui è collegato il dispositivo che si sta utilizzando (e tutti i dispositivi che si collegheranno da quel momento in poi) sia esposto agli attacchi diretti da parte dei cybercriminali.

Inoltre, come accennato sopra, le e-mail di *phishing* sono una delle fonti principali per ricevere attacchi cibernetici di gravità e insidiosità sempre più allarmante e ciò è particolarmente vero nell’ipotesi in cui l’utente opti per registrarsi a una di queste piattaforme pirata, come le IPTV illegali.

Le e-mail di phishing sono una delle fonti principali per ricevere attacchi cibernetici di gravità e insidiosità sempre più allarmante e ciò è particolarmente vero nell’ipotesi in cui l’utente opti per registrarsi a una di queste piattaforme pirata, come le IPTV illegali

Oltre a quanto detto sin qui rispetto al furto dei dati personali (e quindi dell’identità digitale dell’individuo) e alla vendita di questi ultimi sul dark web, le IPTV pirata nascondono ancor più rischi cibernetici rispetto al “mero” utilizzo di siti di streaming illegali. In tema, è opportuno distinguere i rischi che l’utente corre nel fruire contenuti su portali di streaming (che possono essere usati da altri criminali, non necessariamente dal pirata stesso, come esca per le proprie truffe) dai rischi che lo stesso corre nello scaricare software artatamente creato dal pirata sui propri dispositivi, concedendo potenzialmente permessi eccessivi a file, fotocamera, ecc. In questa seconda casistica, l’app IPTV del pirata potrebbe anche infettare la rete internet domestica (modem/router), coinvolgendo altri dispositivi collegati e trasformando alcuni di essi in dispositivi appartenenti a botnet - o reti di dispositivi controllati a distanza - per sferrare attacchi informatici su larga scala.

Ebbene, l’effetto che si scatena è quello di mettere a disposizione dell’attaccante le credenziali personali per accedere ad altri account (e-mail, home banking, social media, ecc.) o – nel caso di siti clone/*scam*⁴ – le coordinate bancari/i dati di pagamento (il classico pop-up che recita “verificare subito i dati di pagamento per non perdere l’accesso al servizio” si fa sempre più convincente ed elaborato). Per di più, sfruttando quei permessi eccessivi ottenuti, il soggetto malevolo può altresì spiare l’utente in tempo reale, accendere la fotocamera e il microfono a proprio piacimento, come pure rimanere nel dispositivo per carpire quanto più materiale possibile

³ Seguendo la definizione della Treccani, un “peer” è un sistema che consente a un utente di scambiare con altri utenti in quel momento collegati, in regime di assoluta autonomia (senza, cioè, passare per un server centrale), programmi, banche dati, materiali audiovisivi, ecc.

⁴ I siti truffa o scam sono pagine web create appositamente per trarre in inganno gli utenti al fine di carpirne informazioni personali e sensibili o somme di denaro e criptovalute. Essi imitano graficamente i siti legittimi (come quelli utilizzati dai circuiti di pagamento o dell’home banking, come pure di piattaforme di streaming legali e marketplace online falsi) per indurre gli utenti a fornire in dati personali ed estremi del metodo di pagamento.

nel tempo ed eventualmente anche installarvi *malware* di diverso tipo, come il sempre più tristemente noto *ransomware*, esponendo l'utente anche a una richiesta di riscatto per riaccedere ai propri dati e alla piena funzionalità del suo dispositivo.

Se questi sono i principali attacchi utilizzati dai cybercriminali nel contesto delle piattaforme audiovisive pirata, è opportuno esplicitare il nesso tra le attività malevole perpetrate in/attraverso la rete e la fruizione di contenuti pirata online.

A tal proposito, uno studio condotto da Corsearch e The Industry Trust for IP Awareness sulla popolazione del Regno Unito (febbraio 2025)⁵ evidenzia che il 76% dei siti pirata più visitati nel Paese sta attivamente esponendo gli utenti a truffe, frodi di natura economico-finanziaria e contenuti espliciti, rappresentando in questo modo una grave minaccia per la sicurezza online degli utenti, soprattutto più giovani. In particolare, lo studio in questione evidenzia che il 29% di chi fruisce di contenuti illegali online è stato infettato da un virus, un *malware* o un *ransomware*, mostrando un incremento del 14% rispetto a quanto registrato nel 2019.

Per di più, si rileva una situazione ancora più preoccupante per quei soggetti che optano per pagare un abbonamento a una piattaforma di streaming illegale, in quanto per l'accesso al servizio devono comunicare, fra l'altro, i dati del proprio metodo di pagamento. Difatti, rispetto a questi ultimi soggetti – che costituiscono circa un terzo degli attuali fruitori di materiale piratato online – l'incidenza delle frodi è piuttosto importante: circa un quarto ha dichiarato di essere stato spesso vittima di frodi gravi (26%), mentre il 25% ha palesato di aver subito addebiti multipli non autorizzati.

Similmente, uno studio effettuato sulla popolazione adulta in Australia mostra che chi effettua in maniera sporadica o continuativa atti di pirateria digitale legati alla visione di film, programmi televisivi o eventi sportivi in streaming si imbatte maggiormente in problematiche di cybersicurezza rispetto a chi ha utilizzato esclusivamente canali autorizzati.

Chi effettua in maniera sporadica o continuativa atti di pirateria digitale legati alla visione di film, programmi televisivi o eventi sportivi in streaming si imbatte maggiormente in problematiche di cybersicurezza rispetto a chi ha utilizzato esclusivamente canali autorizzati

Più nel dettaglio (Fig.2.1), oltre il 10% dei rispondenti che ricadono nella categoria dei "pirati" ha dichiarato di aver ricevuto un virus/*malware* sul dispositivo utilizzato, mentre il 9,8% ha registrato la perdita o l'esfiltrazione dei propri dati personali e l'8,5% ha riconosciuto di essere stato vittima di una frode o di un attacco *ransomware*. Diversamente, le problematiche di cybersicurezza appena menzionate hanno interessato meno dell'1% dei soggetti "non pirati", il che consente di evidenziare la stretta correlazione tra utilizzo di siti web/piattaforme non autorizzate e minacce

⁵ <https://www.industrytrust.co.uk/press-releases/consumers-experience-sharp-rise-in-incidence-of-risks-associated-with-accessing-entertainment-content-illegally/>

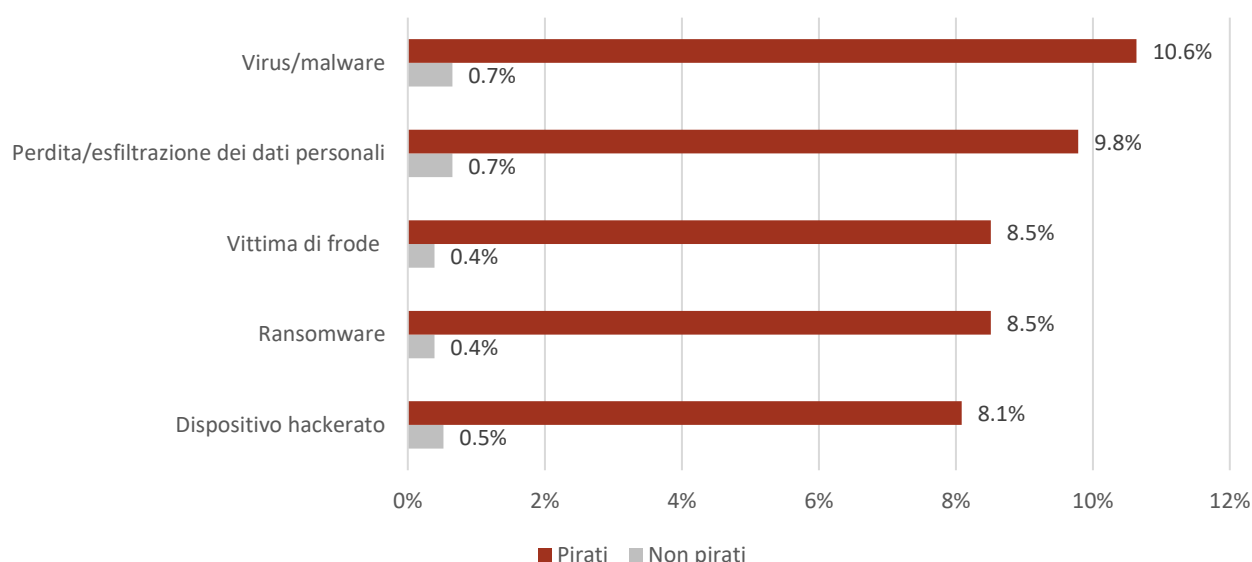
cibernetiche, nella misura in cui la pirateria aumenta di circa 10 volte il rischio di ricevere un virus o altro tipo di *malware* sul proprio dispositivo.

Le problematiche di cybersicurezza appena menzionate hanno interessato meno dell'1% dei soggetti "non pirati", il che consente di evidenziare la stretta correlazione tra utilizzo di siti web/piattaforme non autorizzate e minacce cibernetiche, nella misura in cui la pirateria aumenta di circa 10 volte il rischio di ricevere un virus o altro tipo di malware sul proprio dispositivo

Fig.2.1: Problematiche di cybersicurezza riscontrate dagli utenti durante/a seguito della visione di film, programmi televisivi o eventi sportivi in streaming (2023)

Note: La fonte indica tra i "Pirati" (*Active pirates*) coloro che hanno effettuato una o più attività legate alla pirateria sporadicamente (una volta al mese o meno spesso) e continuativamente (almeno una volta a settimana); viceversa, tra i "Non pirati" (*Non pirates*) rientrano coloro che non hanno mai effettuato attività di questo tipo.

Fonte: Creative Content Australia, Australian piracy behaviours and attitudes, 2023



Per quanto riguarda l'Italia, un primo studio in merito è quello presentato da Fapav/Ipsos nel dicembre 2025⁶ che, tramite un modello di ricerca integrato quali-quantitativo, ha indagato il target d'età 15-25 anni, mostrando che il 62% dei pirati in questa fascia d'età ha subito attacchi informatici nel corso degli anni.

Quanto detto sin qui mostra chiaramente che il rapporto tra rischi informatici e pirateria online va ben oltre mere considerazioni di natura economica – certamente rilevanti, come si vedrà più nel dettaglio in seguito⁷ – potendo palesarsi altresì conseguenze in ambito legale e reputazionale, oltre che in termini di perdita della privacy e del controllo sui propri dati personali. In questo scenario, le autorità – con particolare riferimento alle forze di polizia – a livello regionale e

⁶ Ricerca FAPAV/Ipsos su stili di vita dei giovani italiani e pirateria audiovisiva, dicembre 2025.

⁷ Si v. *infra*, par.3 ss..

internazionale si stanno impegnando per favorire una maggiore consapevolezza del fenomeno tra la popolazione.

Quanto detto sin qui mostra chiaramente che il rapporto tra rischi informatici e pirateria online va ben oltre mere considerazioni di natura economica – certamente rilevanti, come si vedrà più nel dettaglio in seguito – potendo palesarsi altresì conseguenze in ambito legale, reputazionale e di privacy

Ad esempio, l'Interpol (l'Organizzazione internazionale della polizia criminale) ha avviato una serie di iniziative volte a sensibilizzare gli utenti, a partire dalla diffusione delle modalità con cui i servizi pirata in rete si garantiscono un guadagno, tra cui rilevano: a) la pubblicità, in quanto queste piattaforme ricevono denaro dagli inserzionisti in base al numero di click degli utenti su un banner o simili; b) le donazioni o la quota di abbonamento, poiché è – purtroppo – prassi diffusa richiedere un pagamento per accedere alle funzionalità premium della piattaforma; c) la vendita dei dati personali degli utenti a terze parti, le quali possono essere mosse da intenti a loro volta criminali o comunque porsi in maniera aggressiva nei confronti delle vittime. In questo senso, l'utente può, per un verso, essere esposto alle dinamiche tipiche dell'underground (cyber)criminale e, dall'altro, foraggiare indirettamente e – spesso – inconsapevolmente quest'ultimo con le proprie informazioni personali.

L'utente può, per un verso, essere esposto alle dinamiche tipiche dell'underground (cyber)criminale e, dall'altro, foraggiare indirettamente e – spesso – inconsapevolmente quest'ultimo con le proprie informazioni personali

Come già accennato, una delle conseguenze potenzialmente più spiacevoli riguarda il furto dell'identità digitale, in particolar modo nei casi in cui – tramite l'utilizzo di un *infostealer malware* (software malevolo finalizzato al furto di informazioni) – vengano carpite le credenziali e i dati personali salvati quotidianamente dagli utenti nei propri browser e quindi facilmente accessibili ed esfiltrabili dai cybercriminali i quali, una volta acquisite tali informazioni, le vendono a prezzi modici su forum nel dark web oppure sfruttano appositi gruppi o canali presenti su alcune app di messaggistica, ove altri criminali potranno acquistarle e sfruttarle in attacchi finalizzati al profitto.

Questo meccanismo – sempre più diffuso – ha contribuito alla creazione di un vero e proprio mercato parallelo delle identità digitali, che vede un account LinkedIn costare mediamente intorno ai 45 dollari, seguito – con notevole distacco – da Facebook (\$14), Discord e Instagram (\$11)⁸. Si tratta evidentemente di cifre irrisorie per un'organizzazione cybercriminale, che può arrivare a "fatturare" anche come una media-grande impresa italiana, il che rende particolarmente appetibile basare il business illecito su questa tipologia di attività.

⁸ <https://www.stationx.net/social-media-hacking-statistics/>

E, infatti, l'attaccante mantiene l'accesso all'account della vittima potendo agire a proprio piacimento, ad esempio inviando link contenenti virus e *malware* ai contatti, pubblicando immagini e video conservati in archivio o in chat private, come pure commenti pubblici che possono minarne la reputazione sia online che offline, oppure utilizzare i metodi di pagamento eventualmente registrati su queste piattaforme per effettuare acquisti sui *marketplace* interni.

Ad ogni modo, tra le conseguenze più diffuse oggi, si rilevano: a) l'accesso illecito ai propri account social, al fine di raccogliere maggiori informazioni relative alla propria identità digitale da vendere o sfruttare in successive truffe; b) il furto di informazioni sensibili presenti nelle proprie caselle email (documenti di identità e di varia natura amministrativa e sanitaria, conferme di registrazione a siti ed iniziative, ecc.); c) l'accesso a tutti quei portali online dove si svolge ormai parte della nostra vita, come i siti di e-commerce e gli account di pagamento digitale, guidati sempre e comunque dal facile profitto e dall'effetto "sorpresa" dell'ignara vittima.

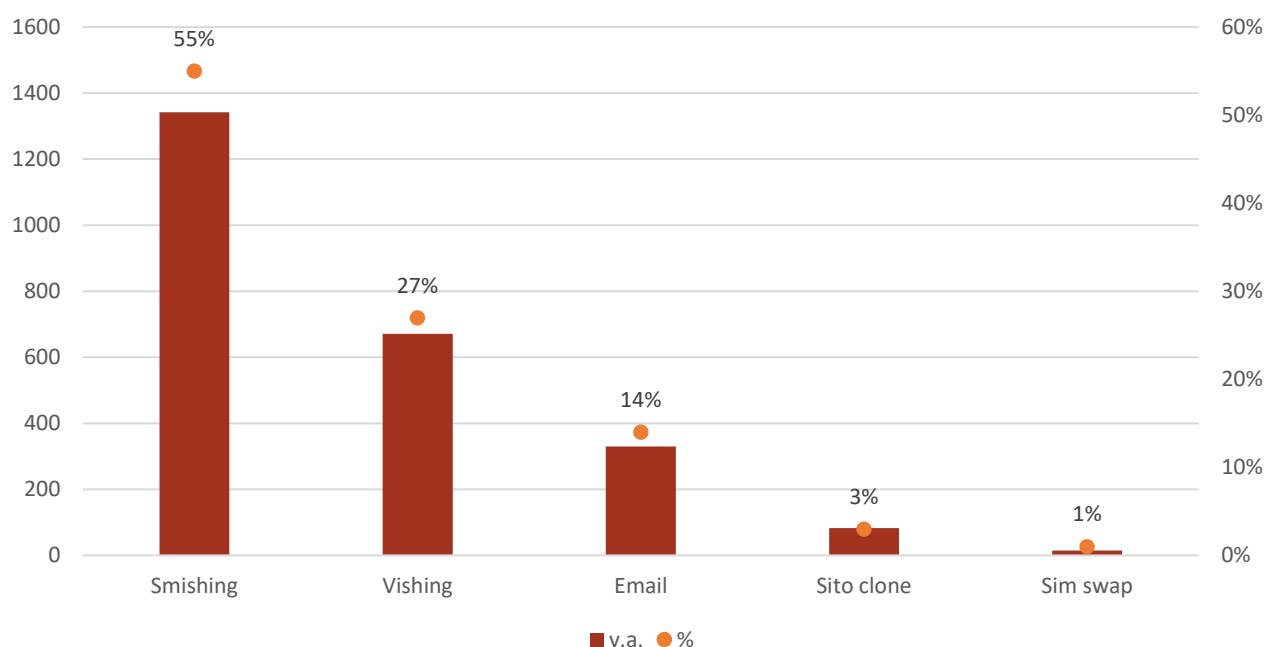
Volgendo uno sguardo al contesto nazionale, i dati forniti dalla Polizia Postale confermano la tendenza appena descritta a livello generale anche per l'Italia, dove il furto di identità digitale perpetrato sfruttando l'ingegneria sociale continua a costituire una delle minacce più insidiose nell'ambito dei reati economico-finanziari perpetrati tramite i sistemi informatici. In particolare, l'ingegneria sociale (*social engineering*) è una metodologia di truffa che permette ai criminali informatici di raccogliere informazioni personali della vittima tramite l'inganno, facendo leva sulle emozioni umane quali la curiosità, l'ansia, la paura o l'impazienza. Tra i principali metodi utilizzati ci sono il phishing via messaggio (SMS o messaggistica istantanea – "smishing"), quello via voce (o telefonico) detto "vishing" e il phishing tradizionale (via e-mail).

Volgendo uno sguardo al contesto nazionale, i dati forniti dalla Polizia Postale confermano la tendenza appena descritta a livello generale anche per l'Italia, dove il furto di identità digitale continua a costituire una delle minacce più insidiose nell'ambito dei reati economico-finanziari perpetrati tramite i sistemi informatici

In base a un'analisi degli eventi gestiti nel 2024 (Fig. 2.2), limitatamente a quei casi in cui è stato possibile rilevare la metodologia con cui è avvenuto il furto di identità digitale, i dati forniti dalla Polizia Postale evidenziano che lo *smishing* (55%) è il metodo più ricorrente in questo ambito, soprattutto in combinazione con il *phishing* telefonico (o *vishing*) per rafforzare il sentimento di ansia e preoccupazione nella vittima, che costituisce la seconda categoria più diffusa (27%), seguita dall'email *phishing* (14%), dove i malintenzionati inviano mail – sempre più sofisticate anche grazie all'ausilio dei sistemi di IA generativa – per convincere il target a seguire istruzioni specifiche, le quali portano quest'ultimo a cliccare su un collegamento ipertestuale o a fornire dati e informazioni riservate/personali.

Fig.2.2: Distribuzione dei metodi di furto di identità nei reati economico-finanziari, 2024 (in valori assoluti e percentuale)

Note: I dati riportati in figura costituiscono una porzione limitata degli eventi gestiti dalla Polizia Postale nel 2024, ossia solo in quei casi in cui è stato possibile rilevare la metodologia con cui è avvenuto il furto di identità digitale
Fonte: Mattinale Polizia Postale e per sicurezza cibernetica, 2025

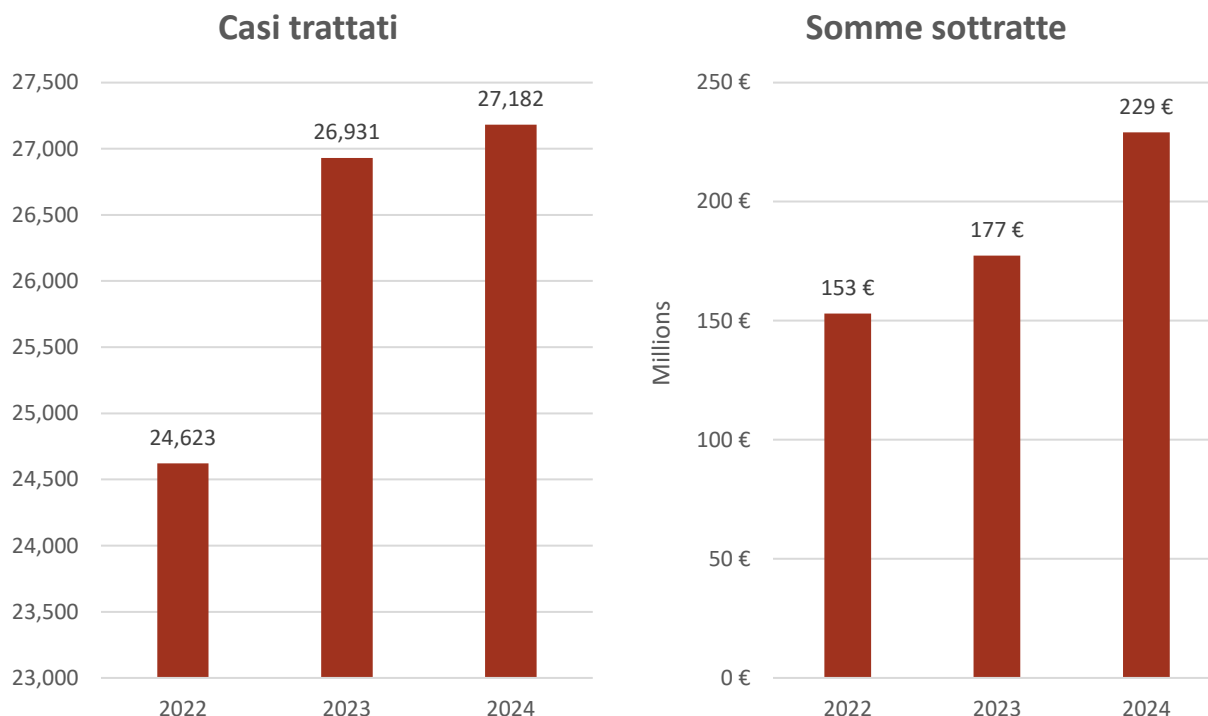


Scarse competenze si traducono inevitabilmente in una maggior vulnerabilità alle minacce informatiche. A tal proposito, i dati derivanti dai resoconti sulle attività effettuate dalla Polizia Postale, con particolare riferimento alle truffe online e alle frodi informatiche, forniscono ulteriore concretezza a quest'ipotesi (Fig.2.3). Nel 2024 è stato registrato un aumento delle attività fraudolente perpetrate in rete. Ciò è vero sia con riferimento al numero di casi trattati (+251 rispetto al 2023 e +2.559 sul 2022), sia in relazione all'ammontare delle somme sottratte, che è passato da circa 153 milioni di euro nel 2022 a 177 nel 2023, fino a giungere a oltre 229 milioni di euro nell'anno successivo. Pertanto, tali dati sottolineano l'urgenza di un deciso cambio di rotta in merito al binomio competenze e consapevolezza dei cittadini italiani in campo digitale, con particolare attenzione alla fruizione di contenuti illegali in rete, i quali possono rappresentare un importante vettore per la compromissione dei dispositivi digitali da parte degli attaccanti e - di conseguenza - l'accesso alla vita stessa degli utenti.

Nel 2024 è stato registrato un aumento delle attività fraudolente perpetrate in rete. Ciò è vero sia con riferimento al numero di casi trattati (+251 rispetto al 2023 e +2.559 sul 2022), sia in relazione all'ammontare delle somme sottratte, che è passato da circa 153 milioni di euro nel 2022 a 177 nel 2023, fino a giungere a oltre 229 milioni di euro nell'anno successivo

Fig.2.3: Numero di casi trattati e somme sottratte (in milioni di euro) in relazione alle truffe online e alle frodi informatiche in Italia (2022-2024)

Fonte: Elaborazioni I-Com su Resoconti attività 2023 e 2024 della Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica



In tema, a giugno 2025 è stata resa nota una nuova metodologia di attacco in base alla quale gli utenti ricevono una e-mail (di phishing) che richiede il pagamento di una sanzione, che sarebbe stata irrogata da un fantomatico Servizio clienti - Piracy Shield di AgCom⁹. Nello stesso periodo, la Polizia Postale ha reso nota una campagna di phishing avente ad oggetto una presunta attività di sorveglianza tecnica legata all'accesso a "contenuti informatici vietati dalla legislazione italiana"¹⁰ (Fig.2.4). Pertanto, è possibile ipotizzare che questi attacchi prendano di mira gli utilizzatori del cosiddetto "pezzotto" e di altri servizi pirata, ricorrendo all'escamotage di "finte" multe o avvisi, in quanto i dati personali delle vittime possono essere stati compromessi proprio utilizzando i servizi illeciti gestiti, spesso, da organizzazioni criminali.

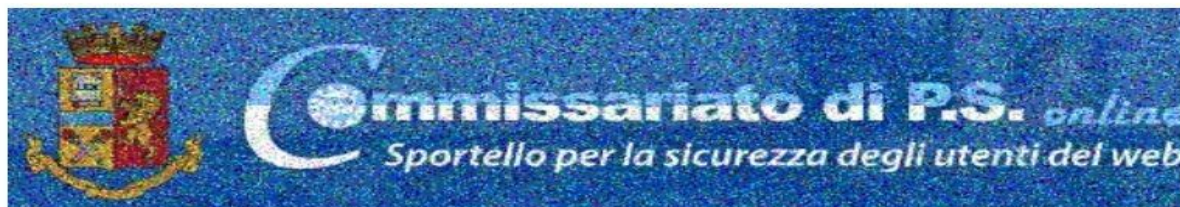
È possibile ipotizzare che questi attacchi prendano di mira gli utilizzatori del cosiddetto "pezzotto" e di altri servizi pirata, ricorrendo all'escamotage di "finte" multe o avvisi, in quanto i dati personali delle vittime possono essere stati compromessi proprio utilizzando i servizi illeciti gestiti, spesso, da organizzazioni criminali

⁹ <https://www.agcom.it/comunicazione/avvisi/comunicazioni-fraudolente-di-sedicente-servizio-clienti-agcom-piracy-shield>

¹⁰ <https://www.commissariatodips.it/notizie/articolo/hai-ricevuto-una-notifica-giudiziaria-urgente-non-cadere-nella-truffa/index.html>

Fig.2.4: Esempio di finta notifica attribuita alla Polizia Postale contenente un allegato infetto

Fonte: Polizia Postale, giugno 2025



Buongiorno,

Vi informiamo che, nell'ambito di un'attività di sorveglianza tecnica legata al vostro indirizzo IP e a diversi dispositivi, sono stati rilevati elementi preoccupanti relativi all'accesso a contenuti informatici vietati dalla legislazione italiana.

Vi chiediamo espressamente di prendere visione del documento allegato al presente messaggio e di inviarci, nel più breve tempo possibile, una spiegazione formale.

Cordiali saluti,

Rivedi il tuo documento

Considerata l'urgenza di questo documento, saremmo grati se volesse risponderci al più presto via email.

Nuova
procedura (...)



PDF

Un ulteriore caso pratico che può essere preso come riferimento sul tema è il malware Kolpatra, individuato dagli specialisti di Cleafy a ottobre 2025. Questa minaccia cibernetica si nasconde proprio dietro app di streaming illegale, le quali millantano l'accesso gratuito a contenuti live a pagamento. L'obiettivo di questo malware è svuotare i conti correnti degli utenti pirata nel momento in cui il dispositivo utilizzato per consumare contenuti illegali è inattivo¹¹. Più recentemente, a novembre, uno studio effettuato nel Regno Unito da BeStreamWise ha evidenziato che il 40% degli utenti pirata intervistati (ossia che hanno attivato un abbonamento a piattaforme di streaming illecito) ha subito una perdita economica media pari a 1.680 sterline, con picchi – registrati per 1 utente su 10 – fino a 7.500 sterline¹².

In base alle evidenze riportate in questa prima sezione è possibile affermare che la pirateria digitale non espone gli utenti solo a rischi legali (si veda il caso italiano, dove nei mesi scorsi la Guardia di Finanza ha emesso le prime multe per i fruitori di IPTV illegali), ma anche a rischi potenzialmente rilevanti in merito alla propria sicurezza finanziaria e digitale, sia con riferimenti al singolo utente, sia al nucleo domestico-familiare a cui appartiene, proprio per l'effetto – sempre più dirompente, ma allo stesso tempo silenzioso – delle minacce cibernetiche. Ne costituiscono conseguenze immediate la perdita del controllo del proprio conto bancario, così come l'impossibilità di accedere agli account sui social media, oltre a ritrovarsi con dispositivi infetti e, pertanto, inutilizzabili.

2.2. Analisi I-Com sui rischi della fruizione di contenuti illegali online

In questa seconda parte si procederà a mostrare le principali evidenze di un'analisi di impatto economico effettuata dall'Istituto per la Competitività (I-Com) a partire dai dati contenuti nei resoconti annuali della Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica, integrati con ulteriori fonti pubbliche di riferimento, tra cui Istat ed Eurostat. L'obiettivo prefissato consta nel verificare quanto le minacce cibernetiche correlate al fenomeno della pirateria digitale impattino sulla popolazione italiana, opportunamente differenziata per fasce di età e titolo di studio.

In particolare, è stato possibile ottenere l'impatto delle minacce cibernetiche – espresso in miliardi di euro – per il triennio 2022-24 (Fig.2.5). Il danno economico è aumentato nel tempo, passando da €1,24 miliardi nel 2022 a €1,32 miliardi nel 2023, fino a superare €1,42 miliardi nel 2024. Pertanto, si può affermare che su base triennale è stato registrato un aumento del 14,5% in termini di impatto economico delle minacce cibernetiche legate alla fruizione di contenuti illegali in rete sulla popolazione italiana over 16¹³.

¹¹ Per un approfondimento, si v. <https://www.key4biz.it/streaming-pirata-e-la-minaccia-del-trojan-che-svuota-i-conti-bancari/549440/>

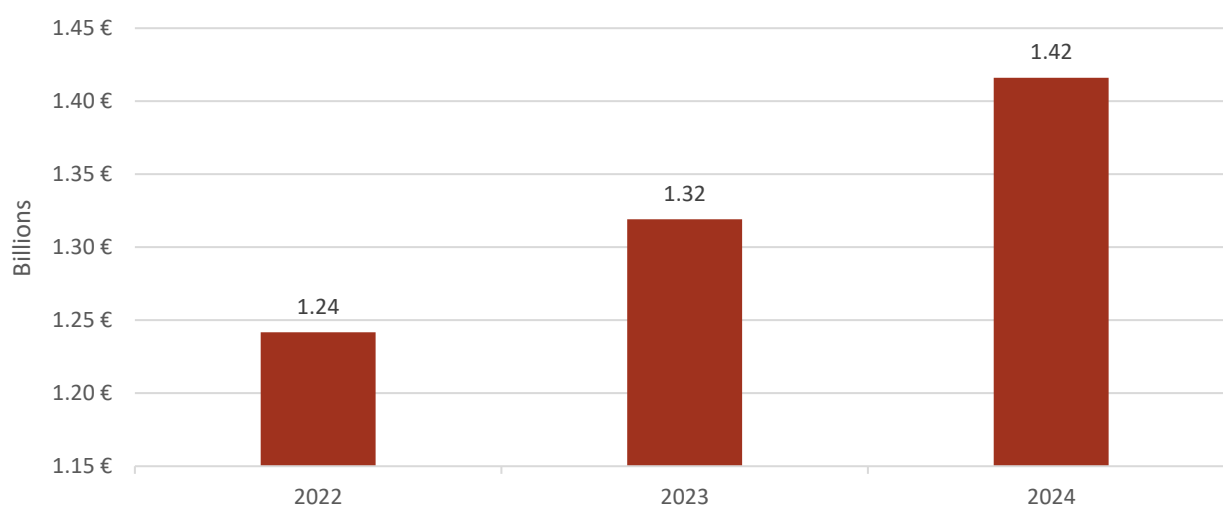
¹² Per un approfondimento, si v. <https://www.key4biz.it/streaming-illegale-in-gran-bretagna-truffe-fino-a-1-700-sterline-e-attacchi-malware/555921/>

¹³ Come si specificherà meglio nella parte finale del paragrafo, l'impatto delle minacce cibernetiche legate alla fruizione di contenuti illegali in rete è stato ottenuto a partire dal valore medio delle somme sottratte in relazione alle truffe online e alle frodi informatiche (Polizia Postale). In seguito, la popolazione italiana è stata suddivisa per fasce di età (Istat) al fine di parametrarla con la quota di over 16 che conducono attività associabili alla pirateria digitale (FAPAV/Ipsos). Successivamente, questo risultato intermedio è stato dapprima rapportato al valore medio ottenuto nella prima elaborazione e poi con la percentuale di italiani che hanno subito una perdita economica da furti di identità, messaggi fraudolenti o siti clone (Eurostat). In questo modo, si è ristretto il campo esclusivamente a chi ha subito un danno economico correlabile all'effetto delle minacce cibernetiche derivanti da attività di pirateria digitale. Infine, sommando i singoli risultati per fasce di età e applicando il medesimo procedimento ai tre anni considerati è stato possibile ottenere la Fig.2.5.

Si può affermare che su base triennale è stato registrato un aumento del 14,5% in termini di impatto economico delle minacce cibernetiche legate alla fruizione di contenuti illegali in rete sulla popolazione italiana over 16

Fig.2.5: Impatto delle minacce cibernetiche legate alla fruizione di contenuti illegali in rete sulla popolazione italiana over 16 (in miliardi di euro), per anno

Fonte: Elaborazioni I-Com su dati Resoconti attività 2023 e 2024 della Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica; Eurostat; Istat



Per di più, è stato possibile valutare tale impatto in maniera differenziata per titolo di studio, operando una distinzione tra individui laureati e non laureati, utilizzando i dati forniti da Eurostat, i quali restituiscono la quota di perdita economica relativamente alle attività malevole in considerazione di tre livelli di istruzione: nessun titolo o livello base (fino alla scuola secondaria di primo grado); livello medio (fino alla scuola secondaria di secondo grado e ai percorsi non terziari, come gli Istituti Tecnici Superiori – ITS); livello alto (che va dalla laurea triennale sino al dottorato di ricerca)¹⁴. In seguito, sono stati aggregati i primi due livelli al fine di ottenere la quota di non laureati (Fig.2.6).

Sebbene i non laureati presentino una quota di danno derivante dalle minacce cibernetiche legate alla pirateria digitale più elevata rispetto a coloro che possiedono almeno un titolo di laurea triennale, questi ultimi presentano un'incidenza del danno più elevata rispetto alla quota di popolazione che rappresentano (Fig.2.6). Ne consegue che, in coerenza con quanto emerge dalle analisi svolte da FAPAV, l'incidenza dei danni da pirateria tra i laureati sia più elevata rispetto al resto della popolazione¹⁵.

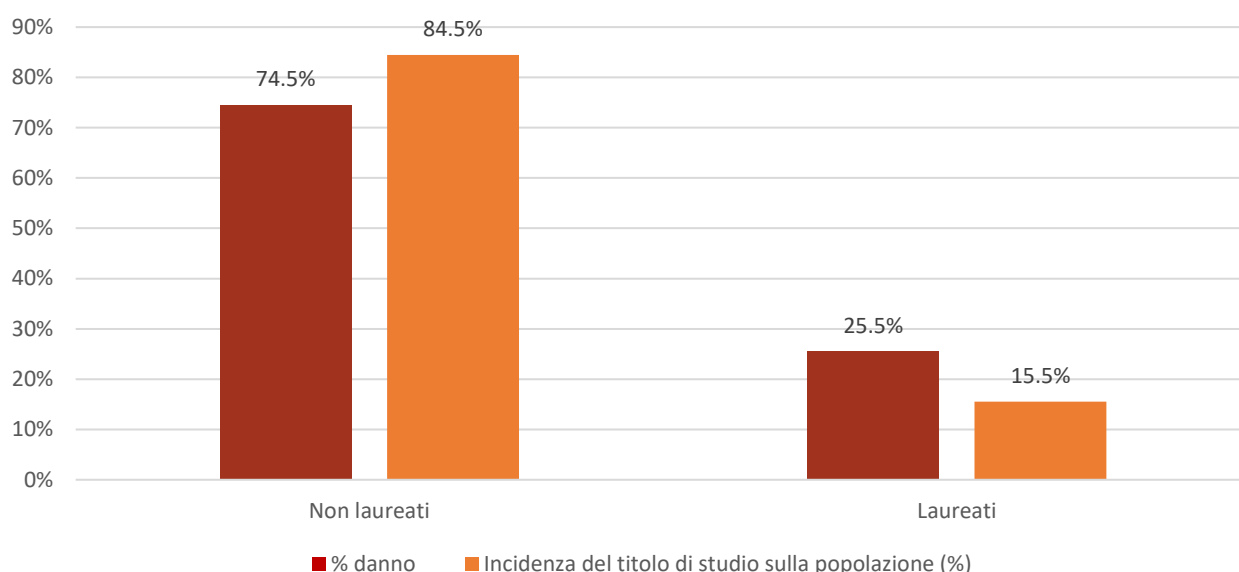
¹⁴ La distinzione operata da Eurostat segue la classificazione di riferimento a livello internazionale ISCED-UNESCO/2011.

¹⁵ È opportuno specificare che per "incidenza del danno" si fa riferimento alla quota di popolazione considerata (laureati e non laureati) sul totale degli over 16. Considerando che i laureati in Italia sono decisamente meno numerosi dei non laureati, si spiega perché per i primi si osserva un'incidenza maggiore.

I laureati presentano un'incidenza del danno più elevata rispetto alla quota di popolazione che rappresentano. Ne consegue che l'incidenza dei danni da pirateria tra i laureati sia più elevata rispetto al resto della popolazione

Fig.2.6: Distribuzione dell'impatto economico derivante dalle minacce cibernetiche correlate alla pirateria digitale tra laureati e non laureati

Fonte: Elaborazioni I-Com su dati Resoconti attività 2023 e 2024 della Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica; Eurostat; Istat



L'analisi si è focalizzata altresì sull'impatto delle minacce cibernetiche correlate alla pirateria digitale integrando gli anni considerati (2022-2024) con le fasce di età, a partire dagli individui con almeno 16 anni (Fig.2.7). Innanzitutto, i risultati mostrano un andamento crescente nel tempo in termini di danno economico, con la classe di età compresa tra 35 e 44 anni che è quella maggiormente impattata, essendo passato da €259 milioni nel 2022 a €340 milioni nel 2024, seguito dagli individui tra i 45 e i 54 anni (da €227 a €300 milioni) e dalla fascia 25-34 anni (da €216 a €293 milioni).

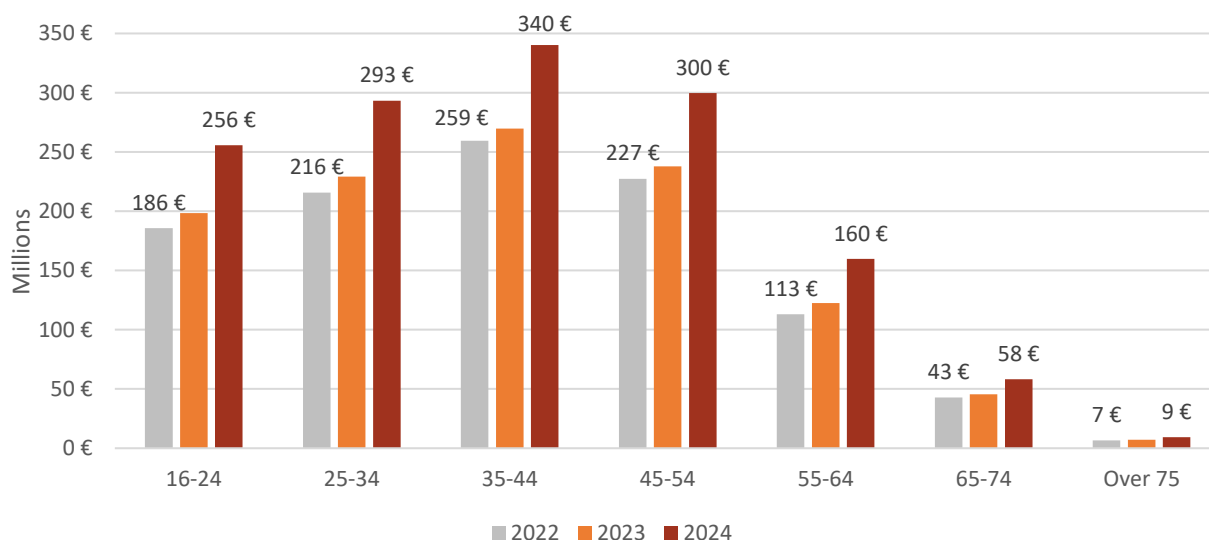
I risultati mostrano un andamento crescente nel tempo in termini di danno economico, con la classe di età compresa tra 35 e 44 anni che è quella maggiormente impattata, essendo passata da €259 milioni nel 2022 a €340 milioni nel 2024, seguita dagli individui tra i 45 e i 54 anni (da €227 a €300 milioni) e dalla fascia 25-34 anni (da €216 a €293 milioni)

In aggiunta, è opportuno sottolineare che nel periodo di riferimento le classi di età in cui l'incremento è stato più consistente sono quelle 55-64 anni e over 75 (+41% dal 2022 al 2024).

Viceversa, l'aumento è stato più contenuto per coloro che sono compresi tra i 35 e i 44 anni (+31%) e tra i 45 e i 54 anni (+32%).

Fig.2.7: Impatto delle minacce cibernetiche (in milioni di euro), per anno e fasce di età

Fonte: Elaborazioni I-Com su dati Resoconti attività 2023 e 2024 della Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica; Eurostat; Istat



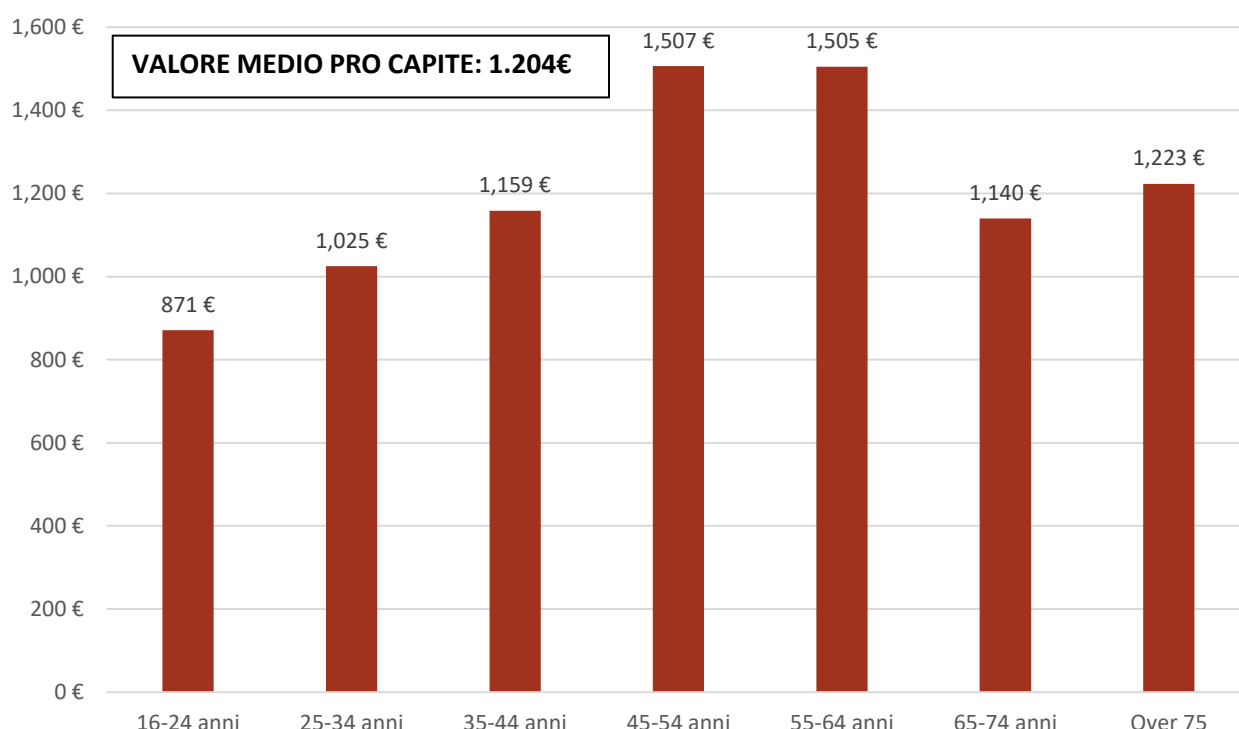
Con l'obiettivo di approfondire ulteriormente le evidenze fin qui emerse, è stato calcolato, per il 2024, il valore medio pro capite relativo all'impatto delle minacce cibernetiche legate alla pirateria digitale (Fig. 2.8). I risultati mostrano che il danno economico pro capite è più elevato nella fascia 45-54 anni (1.507 €), seguita a breve distanza dagli individui tra i 55 e i 64 anni (1.505 €) e si mantiene per quasi tutte le altre classi di età al di sopra dei 1.000€. Infatti, il valore medio pro capite si attesta a €1.204 nel periodo considerato¹⁶. Simili evidenze mostrano la significatività del danno a fronte di una probabilità non trascurabile e di un risparmio economico derivante dalla pirateria decisamente più limitato.

Il danno economico pro capite è più elevato nella fascia 45-54 anni (1.507€), seguita a breve distanza dagli individui tra i 55-64 anni (1.505€) e si mantiene per quasi tutte le altre classi di età al di sopra dei 1.000€. Infatti, il valore medio pro capite si attesta a €1.204 nel periodo considerato. Simili evidenze mostrano la significatività del danno a fronte di una probabilità non trascurabile e di un risparmio economico derivante dalla pirateria decisamente più limitato

¹⁶ Come si specificherà meglio nella parte finale del paragrafo, per calcolare danno economico pro capite è stata innanzitutto moltiplicata la quota di over 16 che conducono attività associabili alla pirateria digitale (FAPAV/Ipsos) per la percentuale di italiani che hanno subito una perdita economica da furti di identità, messaggi fraudolenti o siti clone (Eurostat). È stata così determinata la frazione di popolazione per fascia di età che ha effettuato pirateria e, allo stesso tempo, ha subito perdite economiche da cyber attacchi. Infine, è stato ottenuto il valore medio pro capite dividendo il totale dell'impatto economico per fascia d'età per le quote di popolazione poco fa menzionate, come mostrato nella Fig. 2.8.

Fig.2.8: Impatto delle minacce cibernetiche pro capite, per fasce di età (2024)

Fonte: Elaborazioni I-Com su dati Resoconti attività 2023 e 2024 della Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica; Eurostat; Istat



I risultati mostrati sin qui si sono ottenuti utilizzando i dati Eurostat sulla quota di italiani, distinta per fasce di età, che hanno subito una perdita economica da furti di identità, messaggi fraudolenti o siti clone (Fig.2.9)¹⁷, integrati, per un verso, con i risultati forniti annualmente dalla Polizia Postale rispetto alle somme sottratte tramite truffe online e frodi informatiche¹⁸, dall'altro, con la popolazione italiana (ISTAT) e la quota – pari al 37% – di individui over 16 che conducono attività associabili alla pirateria digitale (FAPAV/Ipsos)¹⁹ e ipotizzando, sulla base di uno studio condotto sulla popolazione adulta in Australia (citato nel paragrafo precedente – Fig. 2.1), che la pirateria digitale aumenti di circa dieci volte il rischio di contrarre un virus o altro tipo di *malware* sul proprio dispositivo.

Come si può notare, la probabilità di subire un danno economico derivante da cyberattacchi segue un andamento decrescente con l'avanzare degli anni, in quanto si passa dal 1,55% tra i più giovani allo 0,04% negli over 75. Pertanto, si può affermare che i rischi siano più elevati per la popolazione più giovane, anche a causa di un maggior uso dei dispositivi elettronici ma anche di una minore consapevolezza.

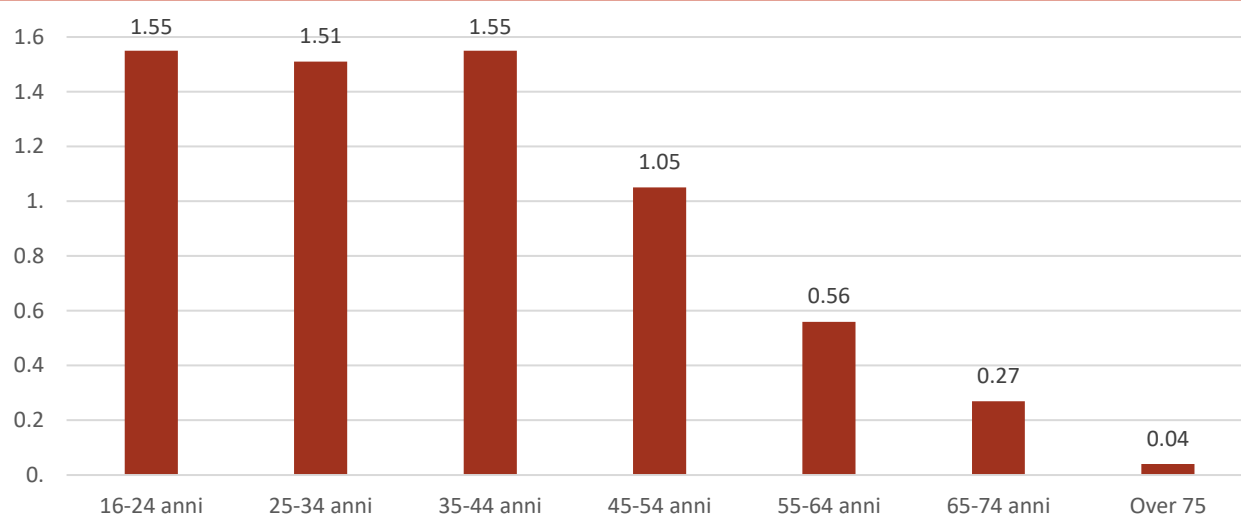
¹⁷ I valori presi in considerazione fanno riferimento al 2019, anno dell'ultima rilevazione di Eurostat in questo ambito.

¹⁸ Si v. supra, par.2.1.

¹⁹ Ricerca Fapav/Ipsos sulla pirateria audiovisiva in Italia, giugno 2024.

Fig.2.9: Quota di italiani che hanno subito una perdita economica da furti di identità, messaggi fraudolenti o siti clone, per fascia di età (%)

Fonte: Eurostat



La probabilità di subire un danno economico derivante da cyberattacchi segue un andamento decrescente con l'avanzare degli anni, in quanto si passa dal 1,55% tra i più giovani allo 0,04% negli over 75. Pertanto, si può affermare che i rischi siano più elevati per la popolazione più giovane, anche a causa di un maggior uso dei dispositivi elettronici ma anche di una minore consapevolezza

In definitiva, è possibile affermare che, oltre al danno economico per l'industria audiovisiva evidenziato negli altri capitoli, i dati relativi ai cyberattacchi dimostrano come la pirateria comporti gravi conseguenze per i cittadini-consumatori. Contrastare la pirateria è dunque fondamentale per tutelare gli utenti e per proteggere il settore.

È possibile affermare che, oltre al danno economico per l'industria audiovisiva evidenziato negli altri capitoli, i dati relativi ai cyberattacchi dimostrano come la pirateria comporti gravi conseguenze per i cittadini-consumatori. Contrastare la pirateria è dunque fondamentale per tutelare gli utenti e per proteggere il settore

3. L'IMPATTO SOCIO-ECONOMICO DELLA PIRATERIA

La pirateria audiovisiva sta avendo un impatto devastante sull'occupazione dell'intera filiera produttiva, colpendo non solo i broadcaster. Solo nel 2025 I-Com stima una mancata crescita di 3.399 posti di lavoro. L'aumento in termini di posti di lavoro, osservabile in alcuni settori, non deve trarre in inganno. L'impatto della pirateria si è, infatti, manifestato prima sui broadcaster (B2C), immediatamente penalizzati dalla fuga di consumatori verso soluzioni illegali. Tuttavia, anche i produttori (B2B) subiranno le conseguenze nei prossimi anni, a causa del calo degli investimenti e dalla riduzione del valore del prodotto derivante dal periodo in cui il fenomeno non era ancora stato efficacemente contrastato. Questa tendenza sarà accentuata dal fatto che al danno immediato (ad esempio l'impatto della pirateria sui contenuti live) è destinato a sommarsi il danno differito (come la perdita di valore dei contenuti non live nell'arco di tutto il periodo di sfruttamento). Il risultato sarà una crescita più contenuta rispetto alle potenzialità del settore.

Questo dimostra come il danno vada oltre chi trasmette i contenuti, influenzando negativamente l'intero ecosistema creativo e produttivo. Dopo un periodo di espansione, sostenuto anche dalla spinta post pandemia e da politiche di sostegno al settore (in particolare, il *tax credit*), anche il comparto della produzione sta frenando la sua crescita occupazionale. Sebbene non si parli di una perdita netta di posti di lavoro, il settore registra un rallentamento significativo nell'incremento dell'occupazione, con potenziali ripercussioni su investimenti e sviluppo futuro.

Se il fenomeno della pirateria non verrà contrastato con misure efficaci, le proiezioni I-Com realizzate per questo studio, in base all'analisi che andremo a esporre nei prossimi paragrafi, indicano una perdita complessiva di 34.012 posti di lavoro nel periodo 2025-2030. Le stime sono state elaborate sulla base di dati che si riferiscono al periodo precedente all'introduzione di Piracy Shield. Grazie a questa iniziativa, gli effetti negativi potrebbero essere attenuati nei prossimi anni, con un impatto meno forte rispetto a quanto inizialmente previsto. Tuttavia, Piracy Shield, pur essendo una misura essenziale, da solo non basta. Inoltre, alcune conseguenze della pirateria, in particolare quelle sulla produzione, continueranno a farsi sentire nel tempo. Questo perché il settore produttivo subisce un impatto più graduale rispetto ai broadcaster, con ripercussioni che emergono nel medio-lungo periodo a causa della riduzione degli investimenti e della minore crescita occupazionale.

3.1. Introduzione metodologica

Obiettivo della presente sezione è quello di valutare l'impatto esercitato dalla pirateria di contenuti audiovisivi sull'occupazione in varie attività economiche. In tal modo si riuscirà a comprendere quanto è alto il livello di rischio in termini occupazionali, oltre a valutare quali tra le attività economiche considerate siano le più esposte.

Per far ciò, si farà leva su due fonti principali, cioè ISTAT e i già menzionati rapporti FAPAV/IPSOS sulla pirateria audiovisiva in Italia. In particolare, dalla prima sono tratte le evidenze riguardanti l'occupazione nella categoria ATECO J "Servizi di informazione e comunicazione", all'interno della quale sono selezionate sei attività economiche che verranno delineate con maggior dettaglio successivamente; dalla seconda è stato preso il dato sulla stima del danno in termini di fatturato perso direttamente a causa della mancata fruizione legale di film e serie tv/fiction e sport live. Inoltre, dal momento che quest'ultima misura è stata introdotta solamente nel rapporto

pubblicato nel 2022, la copertura temporale del dataset costruito riguarda il periodo tra il 2021 ed il 2024.

Obiettivo della presente sezione sarà quella di valutare l'impatto esercitato dalla pirateria di contenuti audiovisivi sull'occupazione in varie attività economiche

Da un punto di vista più strettamente metodologico, la relazione tra occupazione e pirateria è indagata mediante una specificazione log-log, in cui sia la variabile Y che X sono trasformate in logaritmi. I coefficienti ottenuti dal modello, stimato con il metodo OLS, potranno essere interpretati come elasticità, ovvero come impatto percentuale sulla variabile dipendente (occupazione in varie attività economiche) a seguito di una variazione percentuale della variabile indipendente (danno derivante da pirateria). Successivamente, i risultati ottenuti relativamente agli anni 2021-2024 saranno utilizzati per effettuare una previsione sul numero di posti di lavoro persi per il medio lungo periodo, ovvero per il periodo relativo al 2025-2030.

Tuttavia, dato che per alcune attività economiche si è assistito negli ultimi anni a sostanziali aumenti occupazionali, la metodologia appena esposta non risulta valida per queste ultime. Le elasticità associate risulterebbero infatti di segno positivo, segnalando una relazione controintuitiva nonché errata tra dinamiche occupazionali e danni causati dalla pirateria. Per questa ragione si utilizzerà un metodo alternativo, consistente nel calcolo della c.d. "occupazione controfattuale", a partire dal fatturato teorico in assenza di fruizione illegale di film/serie tv e sport live. In tal modo si riuscirà sia a visualizzare sullo stesso grafico l'andamento dell'occupazione reale e quella controfattuale, sia a calcolare il divario che restituirà il dato complessivo sulla mancata creazione di posti di lavoro per il periodo 2025-2030. Il paragrafo seguente sarà interamente dedicato alla presentazione delle risultanze derivanti dall'applicazione della metodologia appena esposta ai dati ISTAT e FAPAV/IPSOS selezionati.

3.2. Stima dell'impatto della pirateria audiovisiva sulle prospettive occupazionali

Effettuando una fotografia iniziale nonché complessiva dei risultati ottenuti, essi hanno messo in luce un impatto della pirateria in termini occupazionali di 3.399 unità guardando solamente al 2025, di cui 2.677 imputabili alla "Attività di produzione cinematografica, di video e di programmi televisivi", 200 alla "Edizioni di software", 260 alle "Trasmissioni radiofoniche", 213 alle "Attività di registrazione sonora e di editoria musicale", 200 alle "Edizioni di software", e solamente 25 e 24 rispettivamente alla "Attività di programmazione e trasmissioni televisive" ed alla "Edizione di libri, periodici ed altre attività editoriali" (Fig. 3.1). Rispetto al 2024, quando si registravano 2.316 posti di lavoro persi, nel 2025 si osserva un aumento di 1.083 posti di lavoro persi, pari a un incremento del 47%. In termini relativi, la perdita occupazionale passa dal 2,93% degli occupati nel 2024 al 4,31% nel 2025.

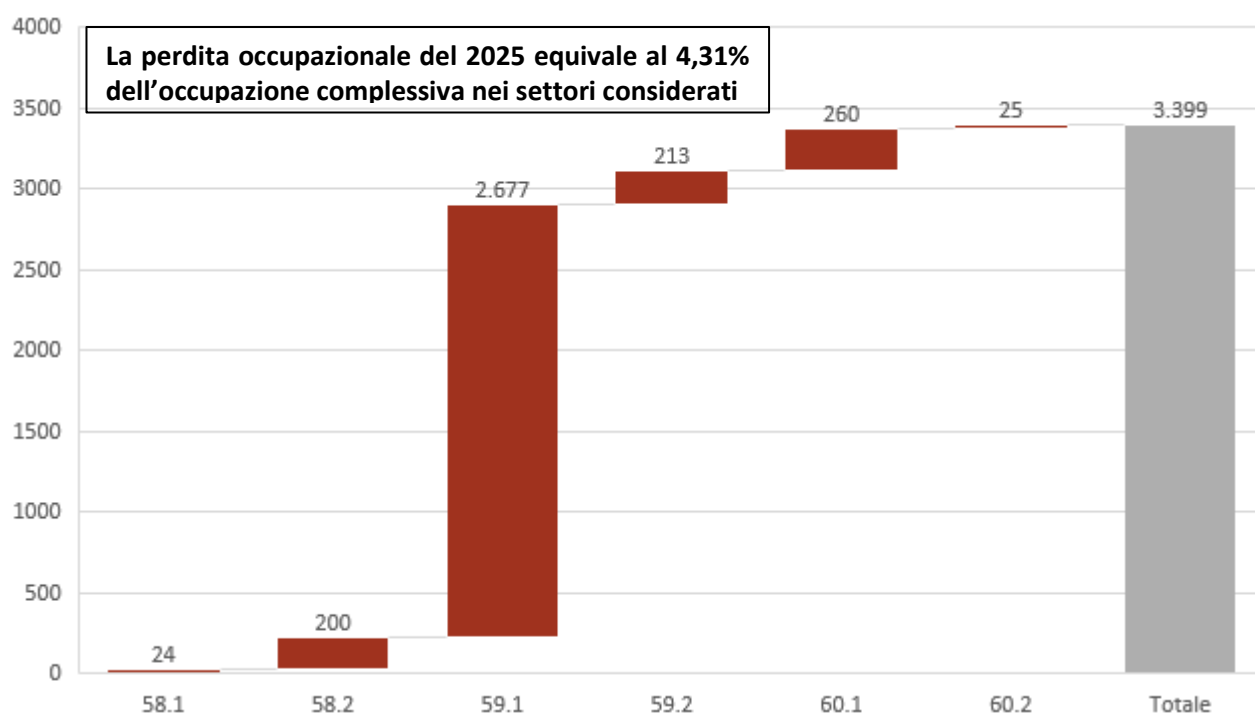
Ampliando invece lo sguardo all'intero arco temporale 2025-2030, l'impatto stimato complessivo è di 34.012 unità, di cui ben 26.786 nella "Attività di produzione cinematografica, di video e di programmi televisivi", 2.916 nella "Trasmissioni radiofoniche", 2.148 nella "Attività di registrazione

sonora e di editoria musicale”, 1.880 nella “Edizione di software”, 142 nelle “Attività di programmazione e trasmissioni televisive” e 140 nella “Edizione di libri, periodici ed altre attività editoriali” (Fig. 3.2). In termini relativi, la perdita di occupazione complessiva rappresenta il 7,2% dell’occupazione nei settori considerati, con un incremento di oltre 3 punti percentuali rispetto al solo 2025.

Rispetto al 2024, quando si registravano 2.316 posti di lavoro persi, nel 2025 si osserva un aumento di 1.083 posti di lavoro persi, pari a un incremento del 47%. In termini relativi, la perdita occupazionale passa dal 2,93% degli occupati nel 2024 al 4,31% nel 2025

Fig. 3.1: Perdita di occupazione per attività economica nel 2025

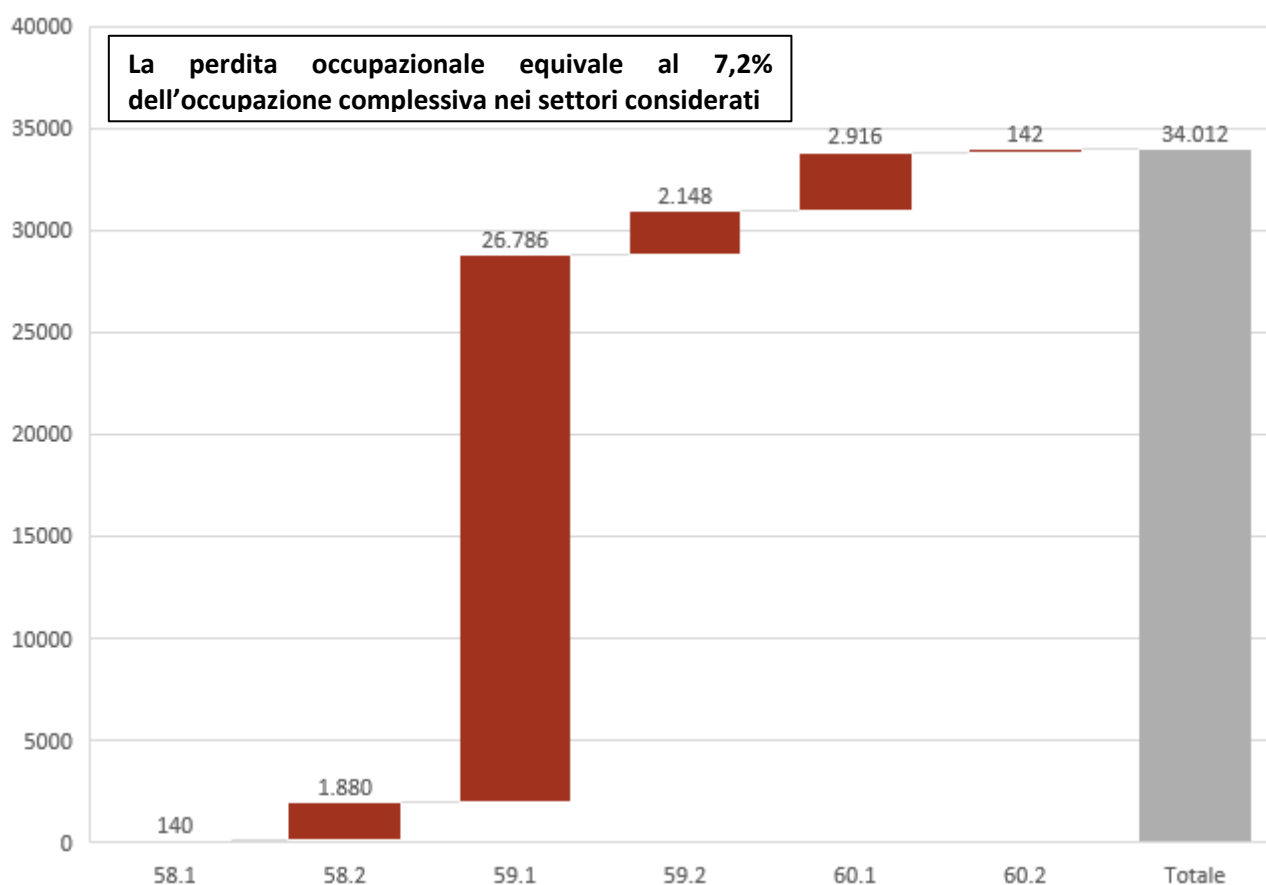
Fonte: Elaborazioni I-Com su dati Istat e FAPAV-IPSOS



Ampliando invece lo sguardo all’intero arco temporale 2025-2030, l’impatto stimato complessivo è di 34.012 unità, di cui ben 26.786 nella “Attività di produzione cinematografica, di video e di programmi televisivi”, 2.916 nella “Trasmissioni radiofoniche”, 2.148 nella “Attività di registrazione sonora e di editoria musicale”, 1.880 nella “Edizione di software”, 142 nelle “Attività di programmazione e trasmissioni televisive” e 140 nella “Edizione di libri, periodici ed altre attività editoriali”

Fig. 3.2: Perdita di occupazione per attività economica tra il 2025 ed il 2030

Fonte: Elaborazioni I-Com su dati Istat e FAPAV-IPSOS

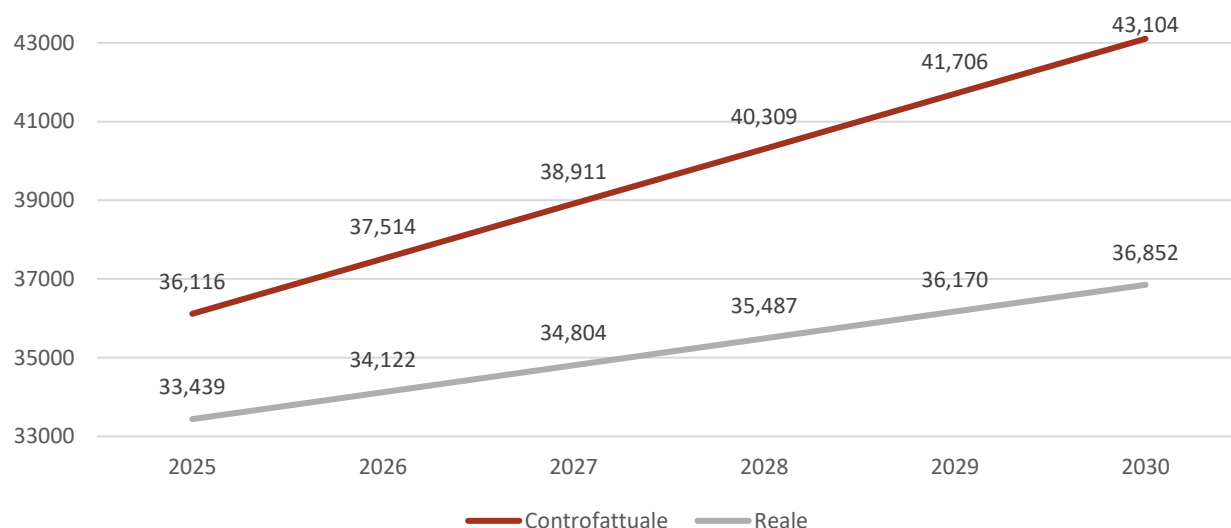


Andando più nel dettaglio, tra le attività economiche considerate nel presente studio quella che risulta maggiormente colpita dalla pirateria risulta essere la 59.1 “Attività di produzione cinematografica, di video e di programmi televisivi”. Il calcolo del fatturato teorico fa emergere importanti gap occupazionali nel settore da dover registrare nei prossimi anni, per un dato totale pari a 26.786 posti di lavoro (Fig. 3.3). In maniera interessante, sembrerebbe che la pirateria eserciterà un impatto sempre più marcato sull'occupazione nei prossimi cinque anni, passando da un dato di 2.676 ad uno di 6.251 nel 2030.

Andando più nel dettaglio, tra le attività economiche considerate nel presente studio quella che risulta maggiormente colpita dalla pirateria risulta essere la 59.1 “Attività di produzione cinematografica, di video e di programmi televisivi”

Fig. 3.3: Previsione dell'occupazione reale vs controfattuale nell'attività economica 59.1 "Attività di produzione cinematografica, di video e di programmi televisivi"

Fonte: Analisi I-Com su dati Istat e FAPAV-IPSOS

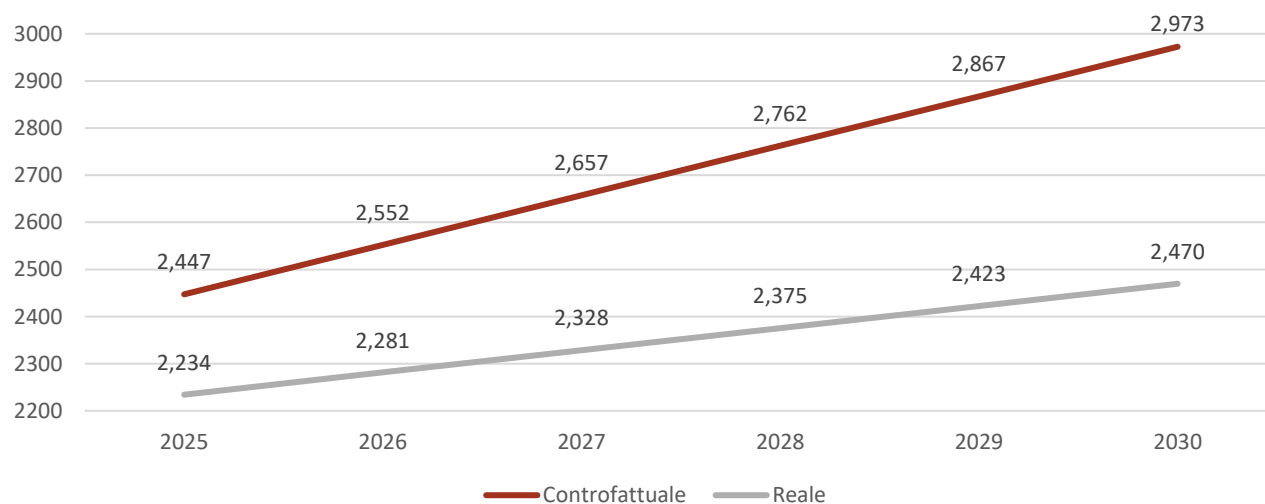


Parallelamente, seppur inferiore in intensità, anche la dinamica del divario occupazionale per l'attività 59.2 "Attività di registrazione sonora e di editoria musicale" presenta un andamento simile. Infatti, partendo da un delta di 212 posti di lavoro nel 2025, si prevede un dato in salita a 503 nel 2030, per un impatto complessivo di 2.148 lavoratori nei cinque anni osservati (Fig. 3.4).

Parallelamente, seppur inferiore in intensità, anche la dinamica del gap occupazionale per l'attività 59.2 "Attività di registrazione sonora e di editoria musicale" presenta un andamento simile

Fig. 3.4: Previsione dell'occupazione reale vs controfattuale nell'attività economica 59.2 "Attività di registrazione sonora e di editoria musicale"

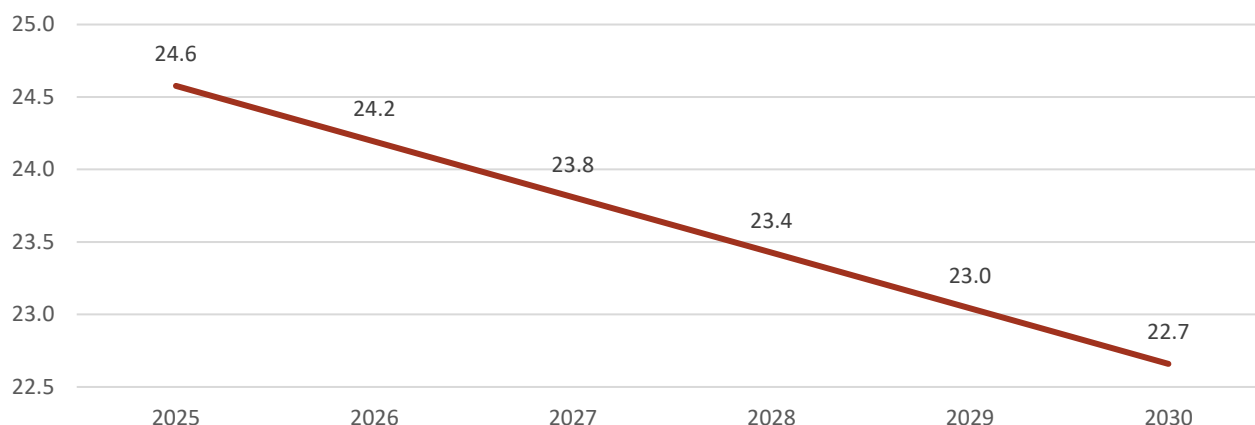
Fonte: Analisi I-Com su dati Istat e FAPAV-IPSOS



Ulteriori interessanti evidenze si estrapolano se guardiamo all'attività economica 60.2, denominata "Attività di programmazione e trasmissioni televisive". In quest'ultimo caso, il coefficiente di elasticità stimato è pari al -0,25%, mostrando una correlazione significativa di segno negativo. In tal senso, secondo le elaborazioni effettuate, si verificherebbe tra il 2025 ed il 2030 una perdita complessiva di posti di lavoro pari a 141, presentando un andamento decrescente nel tempo (Fig. 3.5).

Fig. 3.5: Previsione della perdita occupazionale potenziale tra il 2025 ed il 2030 nell'attività economica 60.2 "Attività di programmazione e trasmissioni televisive"

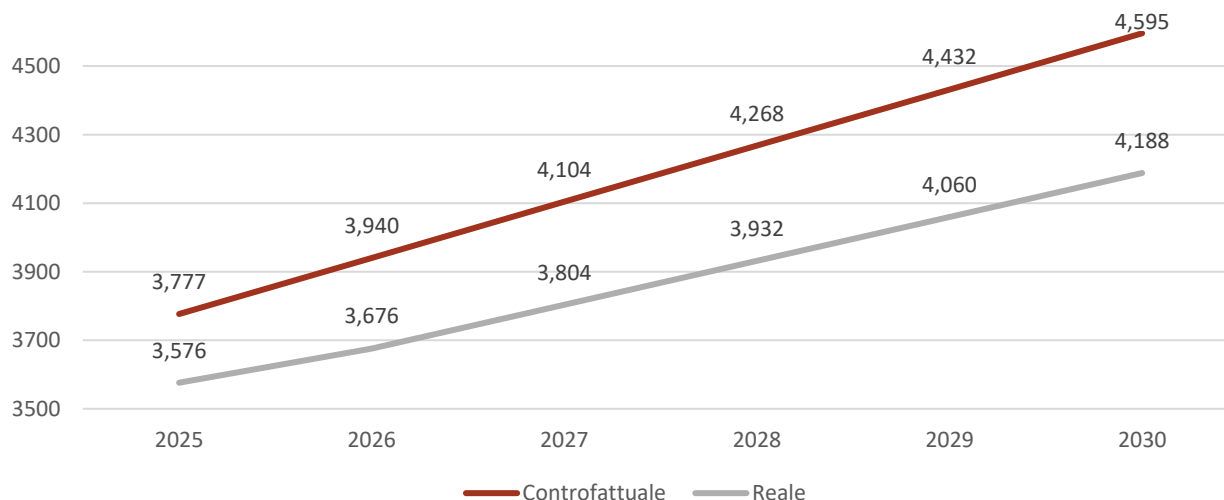
Fonte: Analisi I-Com su dati Istat e FAPAV-IPSOS



Invece, per quanto concerne l'attività economica 59.2 "Attività di registrazione sonora e di editoria musicale" la stima è una mancata creazione complessiva di 1.880 posti di lavoro, con un delta al 2025 di 200 ed al 2030 di 407 (Fig. 3.6).

Fig. 3.6: Previsione dell'occupazione reale vs controfattuale nell'attività economica 58.2 "Edizione di software"

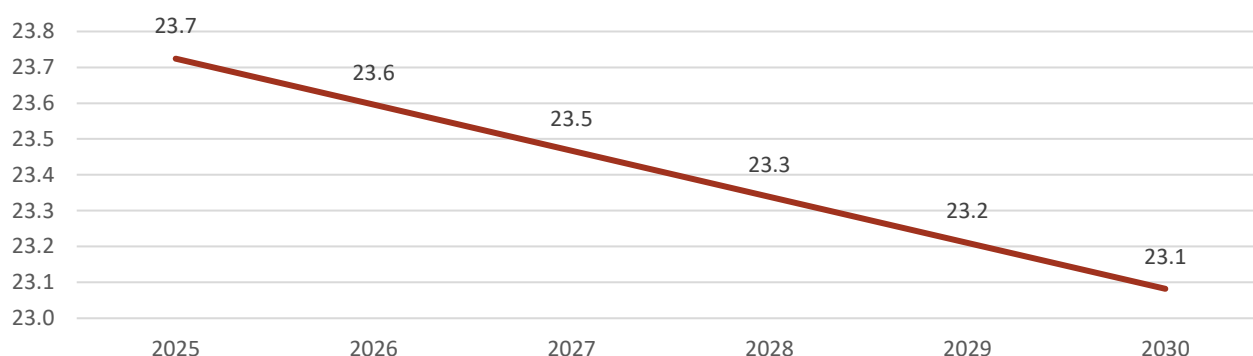
Fonte: Analisi I-Com su dati Istat e FAPAV-IPSOS



Considerando l'attività economica 58.1 "Edizione di libri, periodici e altre attività editoriali", il coefficiente di elasticità stimato è pari a -0,08%, un valore che indica un impatto contenuto della pirateria su questo comparto rispetto alle altre attività. In particolare, si prevede per i prossimi cinque anni una perdita complessiva di circa 140 posti di lavoro. Nel 2025 la riduzione stimata è di 23,7 unità, un valore che tende a diminuire lievemente di anno in anno, fino a raggiungere le 23,1 unità nel 2030 (Fig. 3.7).

Fig. 3.7: Previsione della perdita occupazionale potenziale tra il 2025 ed il 2030 nell'attività economica 58.1 "Edizione di libri, periodici ed altre attività editoriali"

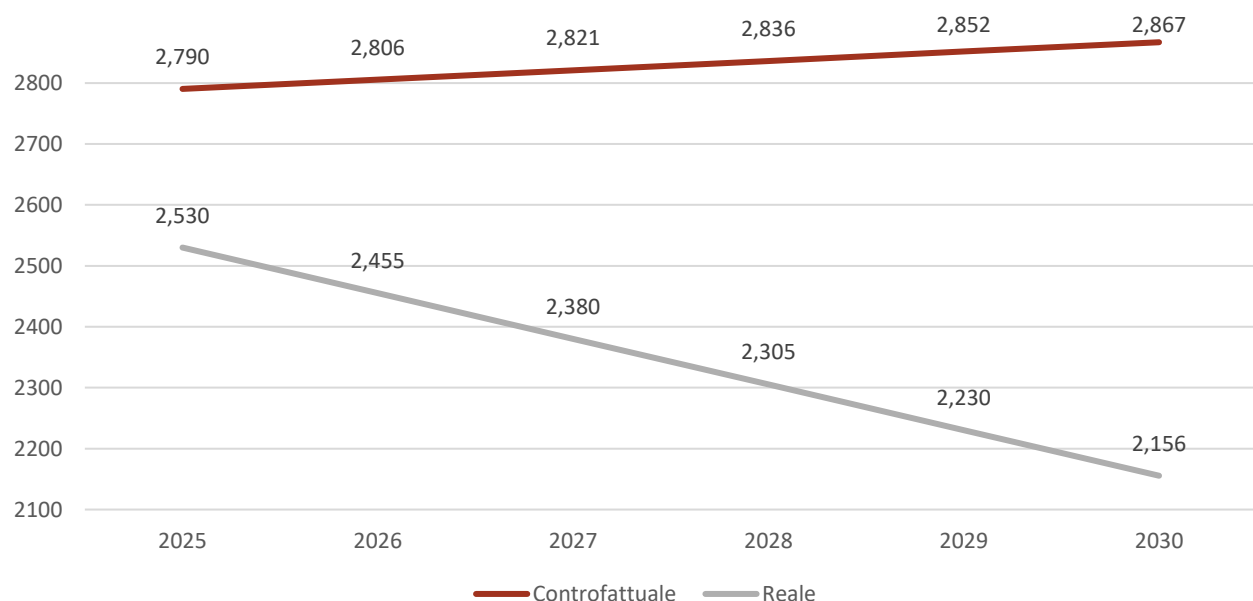
Fonte: Analisi I-Com su dati Istat e FAPAV-IPSOS



Per quanto riguarda l'attività 60.1 "Trasmissioni televisive", si osserva un andamento dell'occupazione particolare. In assenza di pirateria, l'occupazione crescerebbe da 2.790 unità nel 2025 a 2.867 nel 2030, con un aumento del 2,7%. Lo scenario reale, invece, evidenzia una contrazione del 14,8%, passando da 2.530 a 2.156 unità nello stesso periodo. Nel complesso, il settore perderebbe circa 2.916 posti di lavoro tra il 2025 e il 2030 (Fig. 3.8).

Fig. 3.8: Previsione dell'occupazione reale vs controfattuale nell'attività economica 60.1 "Trasmissioni televisive"

Fonte: Analisi I-Com su dati Istat e FAPAV-IPSOS



CONCLUSIONI E SPUNTI DI POLICY

La pirateria audiovisiva continua a rappresentare un fenomeno complesso e dinamico, con implicazioni che superano ampiamente la mera, seppur già di per sé rilevante, violazione del diritto d'autore. Infatti, essa mette in luce come essa si collochi oggi al crocevia tra tre dimensioni cruciali: sicurezza digitale, tutela economica degli utenti e sostenibilità dell'ecosistema produttivo. Se da un lato l'offerta legale continua ad ampliarsi e innovare, dall'altro persistono modelli illeciti sempre più sofisticati, capaci di generare rischi diretti per gli utenti pirata e costi crescenti per l'intero sistema Paese.

La pirateria audiovisiva comporta implicazioni che superano ampiamente la mera, seppur già di per sé rilevante, violazione del diritto d'autore. Il fenomeno si colloca al crocevia tra tre dimensioni cruciali: sicurezza digitale, tutela economica degli utenti e sostenibilità dell'ecosistema produttivo

Rispetto al profilo legato alla cybersicurezza (o, per meglio dire, alla sicurezza digitale), chi accede a contenuti pirata, oltre a commettere un illecito, si espone direttamente a numerose minacce, attraverso malware, phishing, ecc. di cui le piattaforme illegali sono tra i veicoli principali. Dallo studio emerge anche come il danno economico imputabile agli utenti pirata sia rilevante: nel 2024 si registra infatti un valore medio pro capite di circa 1.200 euro, con un aumento preoccupante nell'arco degli ultimi tre anni. È inoltre emerso che l'incidenza dei danni da pirateria tra i laureati risulta più elevata rispetto al resto della popolazione, anche in virtù del fatto che questa categoria è numericamente molto più limitata nel nostro Paese.

Per quanto riguarda l'impatto pro capite, sebbene i picchi maggiori si concentrino nelle fasce 45-54 e 55-64 anni, non va sottovalutato che anche tra i più giovani il danno medio sia tutt'altro che trascurabile. Si tratta, peraltro, di una fascia di popolazione che già affronta difficoltà significative legate al sostentamento durante gli studi, come pure nei primi anni dall'ingresso nel mondo del lavoro.

Accanto a quanto detto, la pirateria ha un impatto profondo sulla filiera audiovisiva e, più in generale, sulla capacità del Paese di attrarre investimenti, generare occupazione qualificata e valorizzare il talento delle nuove generazioni. I risultati evidenziano come la diffusione di contenuti illegali riduca in modo significativo le risorse disponibili per la produzione, in particolare nel settore audiovisivo, con ricadute negative sulle opportunità professionali e sulla dinamica occupazionale. La perdita di posti di lavoro, già oggi rilevante, è destinata a crescere progressivamente proprio a causa della persistenza del fenomeno: entro il 2030 la pirateria potrebbe costare all'Italia oltre 34 mila occupati nell'industria creativa.

Questo scenario si riflette direttamente sul futuro dei giovani che investono tempo e risorse nella propria formazione: un sistema produttivo impoverito offre meno spazio all'inserimento di nuovi talenti, limitando la crescita del capitale creativo nazionale. La conseguenza è un contraccolpo

sull'intero comparto audiovisivo, che rischia di ridurre il proprio peso nell'economia del Paese e di compromettere la sua capacità di competere a livello internazionale.

Alla luce di quanto mostrato nel presente studio, emerge con chiarezza che la risposta al fenomeno della pirateria deve fondarsi sul rafforzamento di un ecosistema di norme e azioni integrate, che combinano monitoraggio continuo, innovazione tecnologica e diffusione di una più matura cultura digitale, insieme a strumenti legislativi adeguati, anche a livello internazionale.

Emerge con chiarezza che la risposta al fenomeno della pirateria deve fondarsi sul rafforzamento di un ecosistema di norme e azioni integrate, che combinano monitoraggio continuo, innovazione tecnologica e diffusione di una più matura cultura digitale, insieme a strumenti legislativi adeguati, anche a livello internazionale

In questo quadro, la tecnologia svolge un ruolo essenziale sia come strumento di contrasto, sia per il monitoraggio intelligente. Il potenziamento di soluzioni avanzate, dalle analisi predittive dei flussi illeciti agli algoritmi di intelligenza artificiale in grado di individuare rapidamente le violazioni, rappresenta un passaggio decisivo per anticipare l'evoluzione dei modelli di pirateria, intervenendo con tempestività.

A ciò si può affiancare un uso etico e trasparente dell'IA anche sul fronte della comunicazione personalizzata, per informare i cittadini, soprattutto i più giovani, sui rischi concreti e quotidiani. Questo significa utilizzare strumenti di IA per proporre contenuti informativi più pertinenti e comprensibili, calibrati sui diversi modi in cui gli utenti si informano e consumano contenuti online. Un uso proattivo dell'IA può consentire, ad esempio, l'analisi in forma aggregata dei trend di ricerca o dei contenuti maggiormente visualizzati, al fine di identificare le situazioni che espongono più frequentemente gli utenti a rischi cyber, tra cui offerte di abbonamenti illegali che imitano servizi ufficiali.

Un uso proattivo dell'IA può consentire, ad esempio, l'analisi in forma aggregata dei trend di ricerca o dei contenuti maggiormente visualizzati, al fine di identificare le situazioni che espongono più frequentemente gli utenti a rischi cyber, tra cui offerte di abbonamenti illegali che imitano servizi ufficiali

Sulla base di queste evidenze è possibile attivare brevi avvisi contestuali o campagne mirate sui canali più utilizzati dagli utenti, sensibilizzando anche sulle possibili conseguenze legali della pirateria digitale. Si tratta di strumenti che non sostituiscono la comunicazione tradizionale, ma la rendono più tempestiva, mirata e capace di intercettare sensibilità diverse, sempre garantendo trasparenza e rispetto della normativa in materia di protezione dei dati personali.

Allo stesso tempo, affinché le potenzialità dell'intelligenza artificiale e delle tecnologie di monitoraggio rafforzino il loro impatto concreto, è necessario che i diversi attori interessati dal

fenomeno potenzino le competenze e le capacità organizzative per rendere ancora più efficace l'uso di queste tecnologie.

Centrale, dunque, deve essere la dimensione educativa, da intendersi non soltanto come sviluppo delle competenze interne alla filiera audiovisiva – certamente centrale, affinché gli operatori siano in grado di adottare con efficacia le tecnologie più avanzate – ma anche come crescita della consapevolezza digitale dei cittadini. Basti pensare che in Italia, secondo gli ultimi dati Eurostat (2023), solo il 45,8% dei cittadini possiede competenze digitali di base, a fronte dell'obiettivo europeo dell'80% entro il 2030.

Centrale, dunque, deve essere la dimensione educativa, da intendersi non soltanto come sviluppo delle competenze interne alla filiera audiovisiva, ma anche come crescita della consapevolezza digitale dei cittadini

Sebbene i giovani presentano livelli di competenze digitali più elevati rispetto alla media nazionale, presentando un dato pari al 58,6%, questo non elude la necessità di rafforzare gli strumenti educativi e informativi. Difatti, competenze più avanzate non si traducono necessariamente e in maniera automatica in una maggiore consapevolezza dei rischi connessi alla pirateria digitale. Diventa quindi prioritario introdurre nei percorsi scolastici componenti strutturate di educazione all'uso consapevole del digitale e alla legalità online, al valore economico della creatività, alla protezione dei dati personali e al funzionamento delle piattaforme, affinché la scelta dell'illegale non sia più percepita come un gesto privo di conseguenze.

Diventa quindi prioritario introdurre nei percorsi scolastici componenti strutturate di educazione all'uso consapevole del digitale e alla legalità online, al valore economico della creatività, alla protezione dei dati personali e al funzionamento delle piattaforme, affinché la scelta dell'illegale non sia più percepita come un gesto privo di conseguenze

Per contrastare efficacemente la pirateria, non è infatti sufficiente evidenziarne i rischi e i danni individuali e sociali, ma occorre anche comunicare in modo chiaro l'intensificazione dei controlli e delle sanzioni. Nell'indagine condotta da FAPAV/Ipsos nel 2024 risulta che, sebbene la maggior parte dei pirati riconosca che si tratti di un reato (il 75% dei pirati adolescenti e il 78% di quelli adulti), solo poco più della metà ritiene probabile essere scoperto e punito (61% dei pirati adolescenti e 56% degli adulti). A ciò si aggiunge una scarsa percezione delle conseguenze del fenomeno: il 49% dei pirati ritiene di non creare danni rilevanti piratando e il 58% non è pienamente consapevole che, a causa della pirateria, i lavoratori dell'industria rischiano di perdere il posto di lavoro²⁰.

²⁰ Ricerca Fapav/Ipsos sulla pirateria audiovisiva in Italia, giugno 2025.

Secondo l'indagine condotta da FAPAV/Ipsos nel 2024, si registra una scarsa percezione delle conseguenze del fenomeno: il 49% dei pirati ritiene di non creare danni rilevanti piratando e il 58% non è pienamente consapevole che, a causa della pirateria, i lavoratori dell'industria rischiano di perdere il posto di lavoro

Occorre dunque rafforzare la comunicazione istituzionale in modo credibile, continuativo e capace di raggiungere i diversi segmenti della popolazione, valorizzando linguaggi contemporanei e canali realmente frequentati dai giovani. Un percorso educativo mirato può contribuire a sviluppare una cultura della responsabilità digitale che non si fondi sulla paura, ma sulla consapevolezza informata e partecipata.

In questo senso è importante rafforzare la collaborazione a livello europeo: la pirateria audiovisiva, infatti, è un fenomeno che colpisce più Paesi e sarebbe utile promuovere politiche e alleanze europee per un contrasto coordinato. Ciò potrebbe includere l'armonizzazione delle normative legate alla protezione dei contenuti e l'intensificazione della cooperazione tra le autorità di diversi Paesi, nonché il rafforzamento degli accordi di assistenza giuridica reciproca.

In definitiva, come sottolineato sin qui, la difesa dei contenuti è al contempo una questione di tutela degli utenti online e un elemento essenziale per la competitività del Paese. Un approccio realmente cooperativo, basato altresì sulla realizzazione di campagne informative credibili e coordinate, può costituire un percorso efficace per contrastare con forza il fenomeno, a beneficio di tutti gli attori (economici e non) in campo.

Un approccio realmente cooperativo, basato altresì sulla realizzazione di campagne informative credibili e coordinate, può costituire un percorso efficace per contrastare con forza il fenomeno, a beneficio di tutti gli attori (economici e non) in campo
