# IL PREZZO DELLA GRATUITÀ

## Pirateria e rischi informatici

#ApparentementeGratis

FAPAV
FEDERAZIONE PER LA TUTELA DEI CONTENUTI AUDIOVISIVI E MULTIMEDIALI

*Chiunque abbia il controllo della tecnologia ha nelle mani il mondo.*

Lex Luthor

# PREFAZIONE

**di Federico Bagnoli Rossi**
*Segretario Generale FAPAV*

Niente è come sembra.

Questo incipit racchiude il senso della guida, di questo approfondimento ad uso e consumo di tutti, non soltanto dei più giovani.

Un argomento delicato quello della pirateria audiovisiva multimediale e digitale, sviscerato nei suoi punti salienti senza pretesa di esaustività, ma con il solo intento di fornire uno strumento di consapevolezza, prima ancora che di studio.

Un ringraziamento speciale va a tutti i Soci Permanenti della Federazione, a tutte le Aziende Associate e ai nostri Consiglieri Delegati che in questi anni hanno supportato con passione e determinazione il lavoro della FAPAV sostenendo la sua crescita e la continua trasformazione nei confronti di un fenomeno, come quello della pirateria audiovisiva, in continuo mutamento. Il 2018, anno in cui si è celebrato il trentannale della Federazione, è stato

un anno determinante per il rafforzamento di tutte quelle attività che sono state implementate attraverso un continuo aggiornamento richiesto dalla costante sfida tecnologica e che il contrasto di questo fenomeno ci impone.

Prendere coscienza del pericolo, dei rischi, è il primo passo per contrastare con maggiore efficacia i suoi effetti lesivi, in quello scacchiere ipotetico dove la sicurezza dei dati, oltre ai danni economici e sociali, la fa da regina e ognuno di noi deve giocare la sua partita, per evitare lo scacco matto.

"Conoscere per deliberare", diceva il Presidente Luigi Einaudi: l'augurio è che le Istituzioni e le Autorità preposte riescano sempre più a giocare d'anticipo, non solo per arginare il problema, ma anche potenziando gli strumenti già a disposizione con norme e sistemi di prevenzione che tutelino gli utenti e i loro dati.

Allo stesso modo gli utenti devono sapersi barcamenare in quel guazzabuglio digitale che è la rete laddove nulla, si ribadisce, è come sembra. Un luogo fatto di maschere, dove chiunque può travestirsi da Robin Hood e strizzare l'occhio a centinaia di inconsapevoli internauti, mentre in realtà li si sta derubando. Un gioco delle parti, quindi, dove la somma delle forze può fare la differenza.

# IL PROBLEMA DELLA PIRATERIA AUDIOVISIVA IN ITALIA

## Lo scenario

In Italia il fenomeno legato alla pirateria audiovisiva, pur segnando una piccola flessione rispetto agli anni precedenti (37% nel 2017 con un calo di due punti percentuali rispetto al 2016), rappresenta ancora una fetta importante di illegalità che contribuisce all'erosione di una parte rilevante dell'economia del settore audiovisivo, con tutto ciò che ne deriva in termini di mancati incassi e, di conseguenza, di perdita di posti di lavoro e riduzione degli investimenti.

Con oltre 617 milioni di euro di fatturato perso annualmente



dall'industria audiovisiva italiana e un danno stimato di oltre un miliardo al sistema economico del nostro Paese, la pirateria continua a rappresentare un forte freno allo sviluppo e alla crescita del mercato.

Oltre al danno economico e culturale, i dati contenuti nel rapporto FAPAV/Ipsos, presentato a luglio 2018, ci rivelano anche altro.

Gli utenti che fruiscono di contenuti pirata, infatti, non hanno piena consapevolezza del rischio di compromettere la propria attrezzatura tecnologica, né delle frodi informatiche cui potrebbero imbattersi accedendo ai siti illegali. Solo il 55% dei pirati è consapevole di questi rischi, mentre tra i più giovani la percentuale è ancora più bassa. La possibilità di imbattersi in *malware*, *phishing* e furto di dati personali è ben più alta di quanto si possa pensare.

## MALWARE E PHISHING

Il *malware* (*malicious software*) è un programma dannoso che, una volta scaricato sul dispositivo da cui si naviga, ne compromette le funzionalità, ruba dati sensibili, accede a sistemi informatici privati.

Il *phishing* è una tipologia di frode messa in pratica attraverso la rete Internet con lo scopo di carpire agli utenti informazioni riservate e sensibili quali, ad esempio, username, password, codici di accesso, numeri del conto corrente o dati della carta di credito.

Uno studio condotto da EUIPO[1] a settembre 2018 (Ufficio dell'Unione Europea per la Proprietà Intellettuale) ha rivelato, su 1.000 siti web sospettati di condividere illegalmente contenuti protetti da copyright, l'esistenza di oltre 4.000 file contenenti malware o programmi potenzialmente indesiderati che erano stati sviluppati per indurre gli utenti a condividere i dati della loro carta di credito, del loro accesso ai "social" e altri dati personali.

La fruizione di contenuti audiovisivi sui siti pirata avviene infatti "apparentemente gratis": seppure nella maggior parte dei casi non venga corrisposto dagli utenti del denaro o il prezzo di un abbonamento per usufruire del singolo contenuto, il "prezzo" di quello che guardiamo viene corrisposto in altri modi.

Nella presente guida illustreremo i vari rischi in cui gli utenti possono imbattersi guardando o scaricando un contenuto audiovisivo presente sulle piattaforme abusive.

[1] EUIPO "Identificazione e analisi di malware su siti web selezionati sospettati di violazione del Diritto d'Autore" (settembre 2018)

# PIRATERIA ONLINE: SAI COSA RISCHI?

## Le diverse modalità di distribuzione illecita online

La pirateria online rappresenta il fulcro della nostra trattazione e presenta molteplici sfaccettature che possiamo riassumere nelle seguenti modalità di illecita distribuzione di contenuti audiovisivi:

- BitTorrent
- Streaming o download da cyberlocker
- IPTV
- App di messaggistica istantanea
  (es. Telegram e WhatsApp, tra le più popolari)

### BitTorrent

La tecnologia BitTorrent sfrutta un protocollo di tipo *peer to peer* (P2P) utilizzato per lo scambio di file in rete (*file sharing*).

Uno dei principali protocolli utilizzati nelle architetture P2P per lo scambio di file è BitTorrent. Questo protocollo, a differenza del protocollo P2P puro usato dal noto software di *file sharing* eMule, prevede la presenza di un server centralizzato, che viene utilizzato per la fase di aggancio alla rete e, quindi, rispetto ai tradizionali sistemi di *file sharing*, l'obiettivo del BitTorrent è quello di realizzare e fornire un sistema efficiente per distribuire lo stesso file verso il maggior numero di utenti disponibili che possono sia prelevarlo scaricandolo sul proprio terminale (meccanismo del *download*) sia inviarlo ad altri (*upload*).

Per potere sfruttare la tecnologia in questione è necessario prelevare un file con estensione specifica (torrent) che rappresenterà il file sorgente nel quale sono contenute tutte le indicazioni dei pacchetti in cui lo stesso è stato suddiviso, unitamente alle chiavi codificate in *codice hash* che garantiscono l'integrità e la genuinità dei pacchetti stessi.

> Una cosa è conoscere la strada giusta, altra cosa è imboccarla.
>
> *The Matrix* (A. e L. Wachowski, 1999)

Trattasi dunque di un file statico in cui sono contenute le informazioni, opportunamente codificate, relative a pacchetti di contenuti che il client che si connette al sito

potrà scaricare/trasferire. Utilizzando la tecnologia relativa ai servizi torrent per scaricare contenuti audiovisivi protetti da copyright è molto alto il rischio di imbattersi in *malware*. Infatti, per poter utilizzare questi servizi, spesso si rende necessaria la disabilitazione dei sistemi di protezione del PC, rendendolo vulnerabile a qualsiasi tipo di infezione da virus o da *malware*.

Recentemente i ricercatori di Kasperky Lab hanno rilevato un nuovo e pericoloso *malware*, denominato "PirateMatryoshka", diffuso tramite il popolare *tracker torrent* "The Pirate Bay". Si tratta di una tipologia di *malware* "a catena" che si attiva non appena il malcapitato utente avvia il programma di installazione. Inizialmente sul dispositivo della vittima compare una copia della pagina web di "The Pirate Bay" che, in realtà, è una pagina di *phishing*. A questo punto viene chiesto all'utente di inserire le

## IL CODICE HASH

Il *Codice Hash* è una funzione che, a partire da un qualsiasi stringa in input A, produce una stringa B (impronta) che ha una lunghezza costante, a prescindere dalle dimensioni di A.

L'Hash è una funzione irreversibile ovvero non si può ricondurre al testo iniziale, partendo dalla stringa generata con la funzione medesima. Tale funzione è utilizzata nella crittografia dei dati per verificarne integrità e autenticità.

## ADWARE

Con *adware* (abbreviazione di *Advertising-Supported Software*) si intende un programma installato in maniera inconsapevole durante la navigazione e usato per raccogliere informazioni sull'utente e per proporre all'occorrenza messaggi e spot pubblicitari non richiesti.

proprie credenziali per procedere con l'installazione. Dopo di che il *malware* utilizza queste medesime credenziali per creare dei nuovi *seeder* (fonti da cui il file viene scaricato in parte o integralmente), diffondendo ulteriormente "PirateMatryoshka" verso altri PC collegati al primo. Il *malware* si diffonde a macchia d'olio su tutta la rete con conseguenze devastanti per la sicurezza dei nostri dati.

I ricercatori hanno stimato che finora il link al sito di *phishing* è stato consultato circa 10.000 volte. Il processo di infezione, in realtà, è in grado di continuare anche se l'utente non ha inserito le sue credenziali, installando ulteriori moduli dannosi tra cui un "*clicker*" che è in grado di "*flaggare*" automaticamente la casella "Accetto" per attivare l'*installer* di *adware*, invadendo il dispositivo

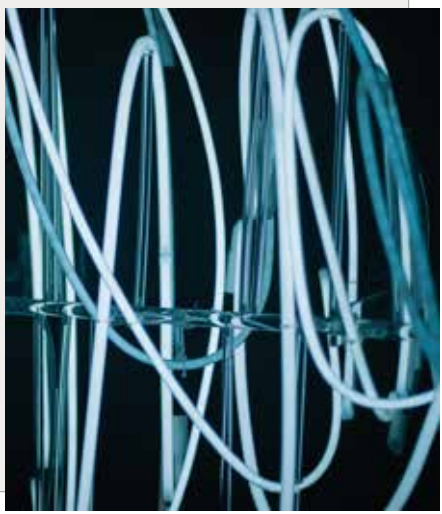
dell'utente con numerosi software indesiderati.

### Cyberlocker

Tra le varie tipologie di pirateria online, molto diffusi sono lo *streaming* e il *download* dai *cyberlocker*, servizi di archiviazione progettati per ospitare i file degli utenti, permettendogli di caricare file che possono poi essere scaricati da altri utenti tramite la condivisione di un link. I siti che condividono questi link ad opere archiviate su domini esterni, indicizzandole e favorendone la fruizione, vengono definiti "aggregatori". Molto spesso questi siti manipolano la navigazione degli utenti andando a inserire dei link nascosti nella pagina o sovrapposti ad altri elementi che potrebbero essere di interesse per l'utente.

## COS'È UN AGGREGATORE?

Con il termine aggregatore si indica un software o un'applicazione web che ricerca contenuti, in questo caso file multimediali, per poi riproporli in forma aggregata per consentirne una migliore fruizione a chiunque ne faccia richiesta.



Di conseguenza, colui che naviga su questi siti, ignaro della situazione, interagisce con elementi malevoli che lo inducono a scaricare a sua insaputa software infetti o a navigare verso siti terzi non sicuri, o ancora ad accettare inconsapevolmente termini e condizioni di servizio relativi a determinati contratti (si pensi alla facilità con la quale si possono attivare servizi in abbonamento non desiderati navigando in Internet da *smartphone* come ad esempio meteo, news, oroscopo, calcio...). Pertanto, i contenuti e le informazioni di altri siti web, che non rappresentano l'oggetto della ricerca dell'utente, vengono visualizzati sul proprio browser.

### Streaming

Lo *streaming* è una delle pratiche più diffuse di pirateria online. Essa presuppone un flusso di dati audio/video messi a disposizione da una sorgente (rete telematica) e che viene riprodotto in via temporanea man mano che giungono a destinazione necessitando di una connessione ad Internet per la fruizione del contenuto.

Lo *streaming* si differenzia dal *download* in quanto quest'ultimo prevede che il file venga scaricato in copia e salvato sull'hard disk o su una periferica esterna restando a disposizione dell'utente a prescindere da una connessione Internet attiva.

Lo *streaming* può essere di due tipologie: *live* oppure *on demand*.

### Streaming Live

Nel caso dello *streaming live* i dati vengono trasmessi utilizzando una o più appropriate tecniche di compressione in maniera tale da alleggerire il più possibile il flusso di traffico sulla rete utilizzata per la trasmissione delle informazioni necessarie.

Un esempio di *streaming live* illegale è rappresentato dalle partite in diretta tv su piattaforme che non detengono i diritti televisivi degli eventi medesimi.

### Streaming On Demand

Lo *streaming on demand* prevede invece che i contenuti audiovisivi si trovino già disponibili per l'uso, trattandosi di file compressi su un particolare computer predisposto a soddisfare le richieste che, ogni volta, vengono effettuate dagli utenti. In questo caso, quando un utente richiede un determinato file audio e/o video, quest'ultimo, appena giunge a destinazione, viene immediatamente decompresso da un apposito

programma o dispositivo che provvede a riprodurre le informazioni contenute nel file richiesto.

Una recente ricerca[2] condotta dall'Università di KU Leuven, in Belgio, ha analizzato circa 20.000 siti online che trasmettono in *streaming* eventi sportivi di ogni genere. Il dato che ne è emerso è davvero sconfortante. Risulta infatti che la maggior parte degli annunci pubblicitari che compaiono durante la navigazione su questi siti propongono l'installazione di programmi, reclamizzati come necessari per poter fruire del contenuto desiderato, che in realtà installano *malware* dannosi, sia per la sicurezza dei dati presenti nel PC, sia per la funzionalità stessa del dispositivo infettato.

Lo *streaming on demand* di contenuti audiovisivi e multimediali è tra le forme di pirateria online più conosciute e diffuse, soprattutto tra i giovani, ma è anche quella a più alto tasso di infezione da virus e di rischio *malware*.

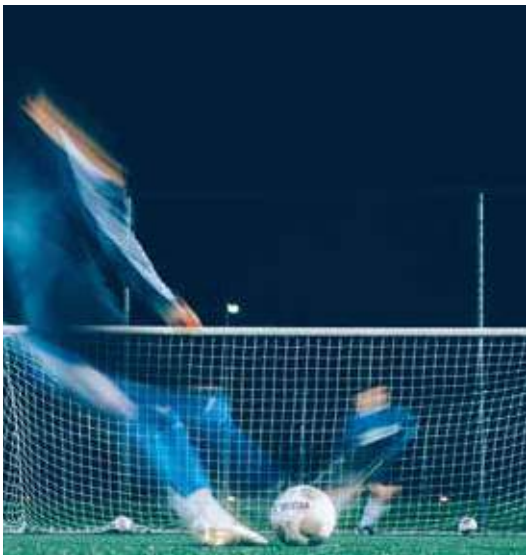
C'è sempre un prezzo da pagare e, come spesso accade in questo ambito, il conto è salatissimo.

[2] Per la ricerca consultare il link https://www.studioconsulentionline.it/siti-streaming-illegali-la-meta-contengono-malware

Come abbiamo visto, inconsapevolmente, navigando su questi siti, apriamo il nostro computer a *malware*, e ad altri programmi indesiderati o virus. Può capitare dunque che vengano sottratti dati sensibili, come le password o, peggio ancora, dati bancari.

Ma non solo. Il computer può anche essere utilizzato, sempre all'insaputa dell'utente, per attacchi hacker contro obiettivi sensibili. Ad alcuni siti web pirata basta un attimo per infettare un computer.

Altri siti della stessa tipologia, invece, utilizzano dei veri e propri "trucchi" come, ad esempio, la promessa di riprodurre in *streaming* un film famoso se si scarica un determinato codec video, il quale invece contiene un virus "trojan" che infetta irrimediabilmente il PC.



Un discorso a parte lo merita il fenomeno dell'IPTV.

## IPTV

L'IPTV (*Internet Protocol Television*) è un sistema che consente a un utente di fruire di contenuti televisivi in formato digitale (*live* e *on demand*) per il tramite di una connessione a banda larga come l'ADSL o la Fibra Ottica. Anche coloro che utilizzano questo sistema di fruizione dei contenuti multimediali spesso fanno leva su strumenti che ne garantiscono l'anonimato, come ad esempio la connessione in VPN (*Virtual Private Network*). Tale modalità di connessione consente il transito dei pacchetti da una parte all'altra dei punti di connessione senza che sia possibile captarne il contenuto in quanto la comunicazione dei dati avviene in maniera criptata.

Il fenomeno delle IPTV illegali è in forte crescita anche nel nostro Paese e si sviluppa su molteplici livelli.

> "Io posso condurti fino alla soglia, ma la porta devi varcarla da solo.
>
> *The Matrix* (A. e L. Wachowski, 1999)

Inoltre, data la sua semplicità, esso consente al cliente di divenire a sua volta "rivenditore" (in gergo "*reseller*") dei pacchetti in abbonamento. Sono ormai molteplici le piattaforme che, previo pagamento di una quota, consentono di "costruire" un pannello (interfaccia grafica ove è

possibile configurare a proprio piacimento la composizione dei vari pacchetti di abbonamento o bouquet di canali) su misura per le esigenze dei *reseller*. Questi pannelli, una volta pronti, vengono immessi nel florido mercato dell'IPTV dove i clienti si trovano a potere scegliere, come se si trovassero in un grande supermercato, l'offerta migliore, ovvero quella che consente loro di ottenere il pacchetto completo, per il periodo di tempo maggiore, al minor costo.

Il successo delle IPTV illegali è dovuto certamente alla facilità di fruizione e alla notevole disponibilità di canali, sia in rete che tramite passaparola, ma soprattutto a un deficit di consapevolezza degli utenti circa i rischi in cui essi possono incorrere in termini di sicurezza dei propri dati sensibili (anagrafici, bancari, geolocalizzazione...). C'è quindi il rischio di assistere a una sorta di tsunami digitale con il fondato pericolo, ove non si corra al più presto ai ripari, di cedere il passo alla criminalità informatica che ha fiutato da tempo le potenzialità di un settore con molte lacune e poche regole, bramosa di allungare le mani sui nostri dati che, a ben vedere, costituiscono una nuova fonte di ricchezza.

La fruizione illegale avviene letteralmente "sniffando" i flussi dati criptati per convertirli in segnali decodificati da indirizzare, tramite apposite strutture server costruite

*ad hoc*, ai decoder dei clienti. Un sistema assai ingegnoso e dispendioso, che necessita di un'infrastruttura tale che non può essere gestita da un novello Robin Hood, da un pensionato che vuole sbarcare il lunario o dal ragazzo di periferia che sogna di comprarsi il cellulare nuovo con i soldi ricavati.

Dietro questo sistema spesso ci sono gruppi organizzati di criminali che investono migliaia di euro in un settore redditizio e a basso rischio se paragonato a quello dello sfruttamento della prostituzione o allo spaccio di sostanze stupefacenti.

Diviene quindi spontaneo porsi la seguente domanda: "come mai questi gruppi di criminali investono molte risorse a fronte di prezzi irrisori per il servizio distribuito?"

Perché il loro guadagno non è solo l'abbonamento mensile percepito. Il guadagno è anche il cliente, o meglio i suoi dati sensibili. Quegli stessi dati che senza battere ciglio vengono forniti in sede di registrazione al servizio e consegnati, come spesso e volentieri accade, a perfetti sconosciuti. D'altronde - si dirà da parte di qualcuno - qualcosa bisognerà pur concedere ai profittatori per poter assistere all'ultima stagione di una serie tv o ad un film campione d'incassi, bypassando il circuito legale. Ma vediamo quali sono queste preziose informazioni che stiamo gentilmente consegnando infiocchettate e con un biglietto di sola andata verso mete sconosciute.

Di certo viene condiviso l'indirizzo IP del PC che dà indicazioni sull'operatore con cui è stato stipulato il contratto linea Internet/voce dell'utenza domestica. Anche l'indirizzo MAC (*Media Access Control*) viene fornito a questi sconosciuti per permettere alle applicazioni che gestiscono l'IPTV di ricevere ed abilitare la visualizzazione del flusso video su un determinato dispositivo. Poi vengono certamente fornite importanti informazioni come numero di telefono ed email o dati sulla geolocalizzazione degli utenti, i quali comunicano la propria posizione, che è spesso associata alla propria abitazione, calibrata a poca distanza da quella reale. Si elargiscono poi i dati sulla nostra navigazione, i siti visitati, la cronologia delle

ricerche effettuate, le preferenze in rete e la natura del dispositivo utilizzato (il modello del PC o dello *smartphone*) e del sistema operativo di cui è dotato.

Tutti questi dati, combinati tra loro, costituiscono una vera e propria miniera, un database illimitato a cui attingere per poter effettuare attacchi informatici mirati.

Se, ad esempio, si scopre che quel PC è dotato di un determinato sistema operativo di cui sono state appena riscontrate delle vulnerabilità, è possibile sferrare un attacco in grado di far leva su quelle disfunzioni riscontrate e che, certamente, nella maggior parte dei casi, andrà a buon fine. Se un PC non ha aggiornato le *patch* di sicurezza, sicuramente risulterà vulnerabile a determinati attacchi che ne minano la sicurezza. L'ipotesi di scuola è quella del classico sconosciuto che, essendo venuto in possesso della combinazione, può aprire con estrema facilità la cassaforte.

### INDIRIZZO IP

Per indirizzo IP si intende una serie di numeri che identificano il dispositivo da cui ci si collega alla rete.

### PATCH

Una *patch* di sicurezza è un aggiornamento del sistema di un software, finalizzato alla correzione di vulnerabilità.

Ecco, nel nostro caso, il sistema antivirus è la combinazione, mentre il PC è la cassaforte. Eludendo il primo si accede al secondo. Non vanno inoltre trascurati gli attacchi che sfruttano l'ingegneria sociale (*Social Engineering*): disponendo ad esempio dei dati sull'operatore telefonico è facile allestire false telefonate promozionali, finalizzate ad acquisire nuove informazioni sull'utente.
Di questo guazzabuglio criminale si è allo stesso tempo vittime e complici, poiché si tende a favorire questa criminalità sottoscrivendo gli abbonamenti ai servizi abusivi che ci vengono proposti.

### App di messaggistica istantanea

Le App di messaggistica istantanea, infine, consentono di condividere con gruppi di utenti materiale audiovisivo e multimediale e/o i relativi collegamenti ipertestuali alle opere.

Il rischio per l'utente che apre questi link è insito nella probabilità, assai elevata, di scaricare materiale di vario genere in cui è presente un virus o un *malware* oppure di essere reindirizzato su pagine che attivano automaticamente abbonamenti su dispositivi mobili, oltre ovviamente al rischio sempre presente di fornire dati personali anche solo per mezzo della semplice navigazione sul link (*url shortner link*).

# APPARENTEMENTE GRATIS: IL VALORE DEI DATI PERSONALI

## I dati personali come merce per il profitto

Come abbiamo visto, dietro la pirateria online si nascondono numerose insidie, rischi e pericoli per l'utente finale che è bene non sottovalutare. Nella maggior parte dei casi, infatti, gli utenti sono pronti a scaricare o vedere illegalmente un contenuto audiovisivo non prestando attenzione al fatto che il beneficio che traggono da questa semplice operazione è assai minore rispetto alle conseguenze cui possono incorrere, non solo dal punto di vista amministrativo e penale, ma anche e soprattutto dal punto di vista della sicurezza della loro privacy. Questo perché il business dei dati è tra i crimini informatici più redditizzi.

I dati ci dicono non solo chi siamo, ma anche quali sono i nostri film e i programmi preferiti e, cosa ben più importante, i nostri orientamenti politici, le nostre inclinazioni sessuali, chi siamo, in quale città viviamo e cosa cerchiamo sul web. Tutto ciò viene rubato dagli hacker e

rivenduto successivamente ad aziende terze che pagano cifre ingenti per avere a disposizione questa ricchezza, ossia le nostre informazioni personali. Questo avviene perché conoscendo il profilo degli utenti, è possibile veicolare messaggi mirati, in grado di influenzare le masse, incidendo sulle loro intenzioni di acquisto con specifici messaggi di marketing o, nei casi più gravi, dirottando le intenzioni di voto durante una campagna elettorale.

Ma questa è ovviamente solo la punta dell'iceberg, in quanto la componente più pericolosa di questo avventurarsi sulla rete è dato da pericoli assai più gravi. Basti pensare al sempre più frequente furto di dati o alla clonazione delle carte di credito, alla duplicazione di documenti d'identità con i dati rubati e la commissione di reati di vario genere (ad esempio le truffe online) le cui conseguenze ricadono sulle malcapitate vittime del furto subito.

Ebbene, il gioco vale la candela? Sembra proprio di no, dato che in ballo ci sono interessi ben più importanti che quelli di guardare un film o una serie tv o un evento sportivo a costi notevolmente ridotti. Questi contenuti audiovisivi sono il veicolo preferito dagli hacker per immettere i cosiddetti *trojan*, virus che, come veri e propri "cavalli di Troia", una volta entrati nel PC della vittima ed eluso le relative difese, consentirebbero all'attaccante di

prenderne il controllo. In tal modo l'hacker ha a disposizione il computer dell'ignaro utente per i suoi scopi poco leciti: oltre a poter rubare ovviamente tutti i dati a partire dalle carte di credito e ai dati dell'identità dello stesso egli ha accesso a qualunque dato contenuto nel computer dell'utente. Ma non solo. In una visione più ampia e complessa del problema, il computer della vittima potrebbe fungere da "zombie" ovvero assumere il ruolo di dispositivo ai comandi di un altro PC il quale, in base a particolari comandi può essere utilizzato per veicolare diversi attacchi hacker, denominati DDOS (*Distributed Denial of Service*), verso siti web di vario tipo, anche istituzionali o governativi.

## HACKER

Per *hacker* si intende una persona esperta di sistemi informatici, in grado di violare la rete ed introdursi illegalmente all'interno di reti di computer private, violando i protocolli di sicurezza.

## TROJAN

Il *trojan* è un file malevolo (es. *malware*) che può infettare il pc della vittima e prenderne possesso. Sono una tipologia di *malware* che i criminali possono usare per prendere il controllo del dispositivo, mobile o fisso, e svolgere qualsiasi tipo di operazione compromettendo il sistema informatico e cancellando i dati in esso presenti.

## COS'È IL DDOS?

L'attacco informatico DDOS (*Distrubuted Denial of Service*) è una tipologia di attacco che prevede la contemporanea utilizzazione di più PC infetti che vengono trasformati in dispositivi "zombie" in quanto del tutto asserventi agli ordini impartiti da un PC principale.

Il meccanismo è quello di dirottare le richieste di connessione dei PC infetti verso un particolare sito internet, con lo scopo di saturarne la banda di traffico e mandarlo offline, creando disagi per gli utenti che realmente hanno bisogno dei servizi elargiti da quel sito. Quindi l'intensità di questo vero e proprio "fuoco incrociato" rende il servizio instabile o, peggio, indisponibile.

Il tutto senza che il legittimo proprietario, nonché utilizzatore del PC, ne sia a conoscenza. Così un bel giorno potremmo avere l'amara sorpresa di una chiamata dall'istituto bancario che ci comunica che il nostro conto è stato bloccato o, peggio, prosciugato, o che è stato acceso un mutuo o richiesto un prestito a nostro nome o che non vi sono le condizioni per poter ottenere un mutuo, anche a distanza di molti anni perché, a nostra insaputa, siamo "schedati" nell'elenco dei cattivi pagatori.

In particolare, va rimarcato che il furto di dati spesso viene perpetuato per commettere reati quali truffe a nostro nome. Pertanto, potremmo trovarci a dover rispondere

alle richieste di danni da parte di soggetti truffati da persone che si sono sostituite a noi nell'ambito di accordi di compravendita che, non essendo stati rispettati, hanno portato ad una denuncia a nostro carico presso le Autorità competenti.

In altri termini, potremmo essere letteralmente fagocitati in un vortice che, partendo dalla denuncia, ci vedrebbe obbligati a rivolgerci agli avvocati per difendere i nostri diritti, con un notevole dispendio di tempo e di risorse economiche. E tutto ciò avviene in quel limbo che molti di noi continuano a sottovalutare.

Dobbiamo quindi essere consapevoli che nel momento in cui accendiamo il PC con l'intento di gustarci un film o un evento qualsiasi in maniera illecita, ci assumiamo un rischio di cui non siamo consapevoli, che non riusciamo il più delle volte a percepire come tale. Questo perché riteniamo, in maniera infondata ed erronea, che chi mette a disposizione del pubblico tutta quella "babele" di contenuti audiovisivi, non pretenda da noi nulla in cambio, secondo quel sentito comune, molto diffuso, per cui esisterebbero persone che impiegano molto del loro tempo libero per consentire a noi di trascorrerlo come più ci aggrada.

# BITCOIN E CRIPTOVALUTA

## Una miniera d'oro

Quando cerchiamo o guardiamo un contenuto pirata non vi sono avvisaglie dei pericoli cui andiamo incontro in quanto si tratta di minacce silenti che in maniera subdola si insinuano nei nostri sistemi installando applicazioni che rendono il PC lento, o peggio, uno strumento passivo azionabile da remoto, da qualunque parte del mondo.

L'esempio, nell'era dei Bitcoin, è dato dal sempre più comune furto di risorse provenienti dal dispositivo dell'utente, le quali vengono utilizzate per "minare" criptovaluta a spese degli utenti (consumo di CPU e RAM che rendono inutilizzabile il PC per le proprie necessità). Infatti, data l'elevata potenza di calcolo richiesta per poter generare criptovalute, alcuni siti sfruttano le risorse del PC degli utenti che si intrattengono sui siti pirata. In questo modo, la potenza computazionale e la spesa energetica

## BITCOIN

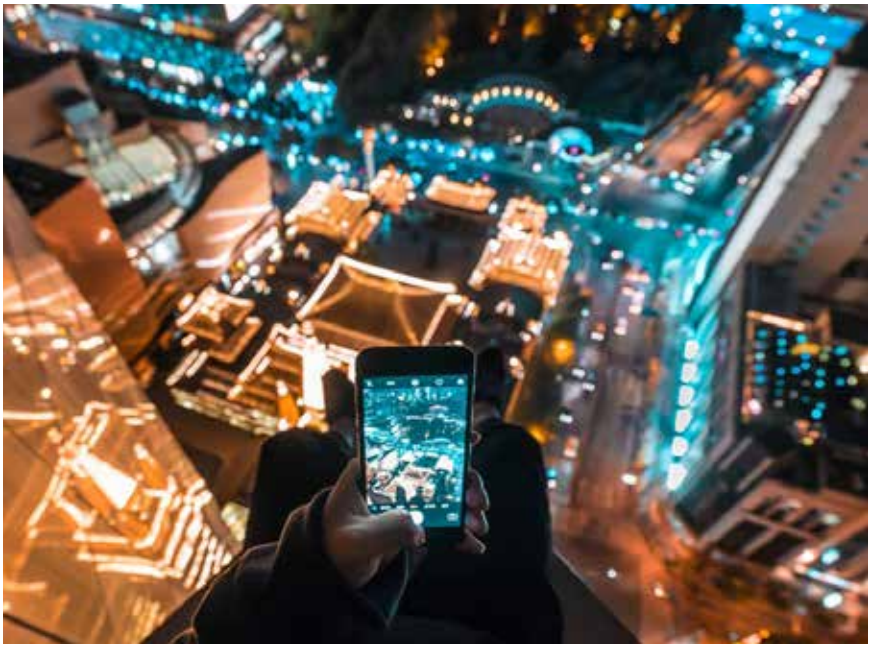
Il Bitcoin è una criptovaluta, una tipologia di denaro virtuale che basa il proprio funzionamento sui principi della crittografia.
Quest'ultima viene utilizzata per verificare le transazioni e controllare l'entrata della valuta nel sistema attraverso l'attività di mining.

## MINARE CRIPTOVALUTA

Con il termine "mining" si fa riferimento all'attività di "estrazione di valuta digitale" mediante la risoluzione di complessi problemi matematici che, in cambio, generano appunto monete digitali. Il procedimento rende il sistema stesso più robusto, ma allo stesso tempo più sicuro.

viene distribuita fra gli utenti visitatori della pagina web ed è possibile generare molta potenza di calcolo e più unità di criptovaluta. Se il sito web creato è abbastanza frequentato dagli utenti potrebbe generare criptovaluta dal valore di migliaia di euro in un solo giorno.

Questo sistema è spesso implementato nei motori di ricerca torrent che ricevono moltissime visualizzazioni al giorno. Gli utenti possono accorgersi di questa minaccia quando, navigando in rete, alcuni processi del browser



rimangono bloccati anche dopo aver chiuso la sessione oppure quando il PC rallenta o si surriscalda richiedendo un maggior carico di lavoro al sistema di raffreddamento senza un reale motivo.

# COOKIES E DATI DI NAVIGAZIONE

## Sappiamo chi sei

Vediamo più da vicino qualche esempio pratico in grado di chiarire ulteriormente la dinamica appena esposta.

Immaginiamo la classica serata da passare a casa. La prima immagine che ci viene in mente è quella di un ragazzo, seduto o disteso sul proprio divano, intento a ricercare un film o una serie tv sul proprio PC. Basta un click su un motore di ricerca et voilà, il gioco è fatto. Si entra in un mondo onirico fatto di colori, immagini pompose che attirano l'attenzione e slogan invi-tanti a caratteri cubi-tali che recitano più o meno così:

- "MIGLIAIA DI FILM IN STREAMING GRATIS!"
- "FILM E SERIE TV TUTTO GRATIS QUANDO VUOI"
- "TUTTI I FILM LE SERIE A PORTATA DI CLICK"

Il tutto corredato da homepage con immagini dei nostri attori preferiti e scritte accattivanti che quasi ci invitano, ci supplicano di aprire quella pagina, di cliccare su quel link, attraverso il quale potremo trovare tutto quello che desideriamo vedere. Chi non si lascerebbe sedurre da una pubblicità così accattivante?

Basta un altro click per scavalcare il recinto oltre il quale non avremo che l'imbarazzo della scelta. L'unica cosa che quel ragazzo deve fare in questa tranquilla serata domestica, seduto comodamente sul proprio divano, è quello di cliccare su quella piccola, innocente e minuscola finestra per accedere ai contenuti desiderati. L'obiettivo, quel film da poco uscito nelle sale o quella serie in prima visione, è a portata di mano, anzi di click, e questa volta è l'ultimo passaggio da effettuare, o almeno questo è quanto recita la didascalia che annuncia il contenuto desiderato. Un unico click separa l'annoiato giovane internauta dalla meta.

Ma già qui siamo entrati in un terreno minato, più o meno inconsapevolmente. Un territorio fatto di pubblicità, fastidiosi e incessanti avvisi, pop-up , finestre che si aprono anche a nostra insaputa, che restano in disparte senza quasi farsi notare. A ben vedere però i problemi sono iniziati dal momento in cui è stato aperto quel sito perché è

in quel momento che sono stati memorizzati i dati relativi alla navigazione in rete. Ma come vengono memorizzati questi dati?

In questo caso occorre parlare dei famigerati cookie. No, purtroppo non sono i classici biscotti della nonna, ma degli strumenti che il server utilizza per migliorare la nostra sessione di navigazione, quando ci si collega ad un sito ospitato dal server stesso. Esistono tre tipologie di cookie:

- tecnici
- di profilazione
- di terze parti

## POP-UP

I pop-up sono finestre che si aprono da sole durante la navigazione su internet. Possono pertanto aprirsi indipendentemente da quello che facciamo. Oltre ai pop-up ci sono anche i pop-under. I pop-under, pur essendo a loro volta molto insistenti, si posizionano sotto la pagina caricata dal browser ed appaiono soltanto quando questa viene chiusa o ridimensionata. In questo modo la navigazione dell'utente non viene interrotta o intralciata in partenza, come invece accade con altre forme di web advertising.

I cookie tecnici consentono la normale navigazione di un sito e la rendono ottimale per ogni singolo utente poiché salvano le preferenze e i criteri di navigazione di ognuno. Per questa tipologia di cookie non è necessario il consenso degli utenti.

I cookie di profilazione creano profili personalizzati relativi all'utente per finalità pubblicitarie e vengono utilizzati poi per intraprendere attività di marketing sui social network. Poiché questa tipologia di dati viene elaborata ed utilizzata per attività diverse dalla navigazione, è necessario il consenso dell'utente per l'acquisizione.

I cookie di terze parti sono una categoria che fa riferimento al differente soggetto che installa i cookie medesimi sul terminale dell'utente, a seconda che si tratti dello stesso gestore del sito che l'utente sta visitando e che di norma viene indicato come "editore" o di un sito diverso che li installa per il tramite del primo c.d. "terze parti". La terza categoria di cookie è quella che maggiormente è stata posta sotto la lente d'ingrandimento, visti i problemi che può arrecare in termini di omesso controllo. I social network sono quelli che ricorrono a questa tipologia di cookie dato che gli stessi vengono implementati e

offerti da società terze con tutti i rischi che ne derivano in termini di sicurezza dei dati sensibili. A ciò si aggiunga che la scoperta di casi attinenti l'uso distorto dei dati, o addirittura il furto degli stessi, avviene sempre in ritardo rispetto al verificarsi del problema.

Pertanto, una consapevolezza sulle conseguenze e i rischi delle proprie abitudini sul web deve iniziare a farsi strada tra gli utenti: ogni volta che si naviga all'interno di un sito non sicuro, come lo è un sito pirata di *streaming* o *download*, si va incontro ad una serie di rischi di cui non è possibile percepirne la reale portata.

Meno il sito è sicuro e più va da sé che i rischi aumentano esponenzialmente e in maniera direttamente proporzionale rispetto alla frenesia con cui si aprono e chiudono le pagine pubblicitarie al suo interno, pagine che memorizzano dati ed innescano a loro volta altre attività tra cui l'installazione sottotraccia di file eseguibili che girano silenti nel nostro pc, il tutto ad insaputa dell'utente. File che aprono porte per l'ingresso di virus (*malware*) e che per l'appunto vengono definiti *backdoor*. Ma questa è solo la parte più innocua dell'intero processo. Da qui in poi iniziano i primi disagi. Più passano i giorni e più ci si accorge

che il proprio PC è lento anche nell'eseguire i processi più basilari (accensione/spegnimento) oppure chiude le pagine automaticamente e con la stessa disinvoltura ne apre altre senza alcun input. Sono i primi sintomi di qualcosa di ben più grave, come il motore di una macchina che inizia a dare segni di cedimento finché non decide di lasciare a piedi il conducente.

La differenza è che il PC, per il quale si ritiene che i problemi siano dovuti all'usura dei componenti dato l'utilizzo protratto nel tempo, in realtà è una macchina infetta, utilizzata da qualcun altro anche distante centinaia di migliaia di chilometri per i suoi loschi affari. E come una macchina infetta reagisce in maniera anomala, diventa vulnerabile e, il più delle volte, una fonte da cui attingere informazioni sensibili per i criminali informatici.

Furti d'identità, clonazione di carte di credito o bancomat, oltre che i contatti dei nostri familiari e amici con relativi indirizzi, tutto viaggia su questi PC e tutto costituisce un obiettivo da aggredire in qualunque modo.

# HACKER, TRUFFE ONLINE E ATTACCHI INFORMATICI

## Alcuni dati

Secondo i dati rilasciati da Norton Symantec[3], che ha coinvolto 22.000 consumatori e 20 mercati diversi, nel mondo le vittime di hackers nel 2017 sono state quasi un miliardo, nello stesso periodo i cyber criminali si sono impossessati indebitamente di 146,3 miliardi di Euro.

Ammontano a 16 milioni i connazionali italiani colpiti dalla criminalità organizzata che opera online, circa il 37 % della popolazione adulta, con un danno che si aggira intono a 3 miliardi e mezzo di euro.

Il 69% degli italiani ha avuto a che fare con il crimine informatico lo scorso anno, il 55% ha avuto un dispositivo infettato da un virus o altre minacce alla sicurezza,

[3] Norton Cyber Security Insights Report: https://us.norton.com/cyber-security-insights-2017

al 41% è stato notificato che le proprie informazioni sensibili sono state compromesse a seguito di una violazione di dati.

Sempre dalla stessa indagine emerge come le vittime di crimini informatici condividano un profilo molto simile: utilizzano la rete con regolarità, sono sicuri di sé e utilizzano più dispositivi per connettersi sia da casa sia in mobilità; all'incirca una vittima su tre di crimini informatici utilizza un dispositivo *smart* per lo streaming (31%) rispetto al 20% di coloro che non sono state vittime.
Inoltre, chi ha subìto un crimine informatico generalmente possiede un dispositivo connesso in rete, ed effettua regolarmente acquisti online via mobile quando non è in casa rispetto alla controparte mai colpita da crimine informatico.

> *Un'idea. Resistente, altamente contagiosa. Una volta che un'idea si è impossessata del cervello è quasi impossibile sradicarla. Un'idea pienamente formata, pienamente compresa si avvinghia, qui da qualche parte.*
>
> *Inception* (C. Nolan, 2010)

I dati confermano che la criminalità informatica è

un fenomeno in continua espansione ed avvalora l'analisi effettuata dal Politecnico di Milano che, in un report dell'Osservatorio Security & Privacy[4], rileva una crescita del 12% degli attacchi informatici, sia in termini di numero che di frequenza.

Troppo spesso i siti di *streaming* nascondono, dietro un'apparente gratuità del servizio, un conto salato per quegli utenti che hanno una conoscenza superficiale dell'informatica e delle tecniche di monetizzazione della navigazione e dei dati personali.

Spesso gli attacchi protratti a danno degli internauti non sempre hanno un impatto immediato ed evidente ma tendono a produrre effetti devastanti a medio-lungo termine. Si pensi, a titolo esemplificativo, alle seguenti criticità[5] in cui è possibile incorrere:

- *Hacking* della mail o dei social (danni stimati 509 €)
- Furto d'identità (danni stimati 192 €)
- Frode con carta di credito (danni stimati 183 €)

[4] Osservatorio Security & Privacy del Politecnico di Milano: https://www.corrierecomunicazioni.it/pa-digitale/consip-acquisti-pubblici-per-125-miliardi-di-euro-risparmi-per-oltre-3-miliardi/
[5] https://nova.ilsole24ore.com/infodata/italia-16-milioni-di-cittadini-colpiti-dal-cybercrime-linsicurezza-in-10-grafici/

- Virus su PC/tablet/cellulare (danni stimati 156 €)
- Furto di dati di pagamento mobile (danni stimati 141 €)
- Danni lavorativi causa di post sui social caricato da altri (danni stimati 134 €)
- Acquisti online truffa (danni stimati 131 €)
- Attacco di tipo *ransomware* (danni stimati 77 €)
- Truffa da finto supporto tecnico (danni stimati 71 €)

Grattando la superficie, si entra in un mondo oscuro, fatto di intrusioni non autorizzate in sistemi informatici e macchine infettate, in pieno controllo di soggetti terzi.

Il quadro che ne emerge è terrificante. In tutto ciò, a fare gli onori di casa vi sono i pluricitati siti di streaming illegali, che rappresentano dei veri e propri avamposti dell'illegalità, fungendo da esca per i malcapitati.

L'utente che viene attratto dai loro contenuti ha una probabilità nettamente superiore rispetto agli altri di scaricare inavvertitamente virus e *malware*.

# I RISCHI PER GLI UTENTI DAL PUNTO DI VISTA LEGALE

Alcune note

Dal punto di vista legale, occorre fare chiarezza su alcuni casi specifici.

Il primo è quello relativo al *download* di un file (come ad esempio un film), per uso strettamente personale, tutelato dalle norme sul copyright. In tal caso, pur non essendo prevista una tipica fattispecie delittuosa, residuerà una condotta illecita per la quale è prevista una sanzione pecuniaria amministrativa ai sensi dell'art. 174-ter della L.D.A.

Un'altra ipotesi che presenta maggiori criticità è costituita dal soggetto che, dopo aver scaricato un file tutelato da copyright, decida di condividerlo (ad esempio mediante un software di *file sharing* come eMule), riprodurlo online o venderlo.

Le maggiori criticità di tale comportamento vengono

appunto in rilievo nel momento in cui l'utente mette a disposizione di altri questi file, i quali possono a loro volta condividerli, fino a rendere minime o annullare del tutto le possibilità di guadagno derivanti dalla commercializzazione legale del prodotto da parte del titolare dei diritti.

In questo caso, se l'azione è avvenuta con scopo di lucro, la sanzione sarà di carattere penale e molto più severa visto che l'art. 171- ter n. 2 lett. a-bis L.D.A. prevede, in questi casi, la reclusione da un mese a quattro anni e una multa da 2.582 € a 15.493 €; quando invece l'azione avviene in assenza dello scopo di lucro si applicherà la generale disciplina ex art. 171 lett. a-bis) che prevede la sanzione della multa da 51,65 € a 2.065,83 €.

Da quanto detto, si evince che il limite di demarcazione fra la sanzione penale della reclusione e quella della multa soggetta a oblazione è rappresentato dallo scopo di lucro,

che la giurisprudenza maggioritaria identifica come un fine di guadagno economicamente apprezzabile o un incremento patrimoniale dell'autore dell'illecito (ad esempio il corrispettivo ricevuto per la vendita del file o l'aver risparmiato una somma di denaro necessaria per acquistare un software).

La Legge n. 633/1941 sul Diritto d'Autore disciplina anche il fenomeno dello *streaming online* seppur con opportune diversificazioni. Bisogna infatti sottolineare una fondamentale distinzione tra il soggetto titolare del sito web che rende disponibili i file da visionare e l'utente fruitore del servizio.

Per i soggetti della prima categoria, valgono le disposizioni precedentemente esposte in riferimento all'upload e le rispettive sanzioni indicate agli articoli 171 e 171- ter L.D.A.

Per gli utenti che fruiscono un servizio di fornitura di contenuti protetti dal D.A. messo a disposizione da terzi, la sanzione sarà quella dell'art. 174-ter L.D.A.

# CONCLUSIONI

## Il punto della situazione

Eccoci giunti alla fine di questo approfondimento la cui intenzione è offrire una serie di consigli ed illustrare i rischi cui l'utente di Internet può imbattersi in quanto riteniamo importante sensibilizzare ogni persona sui possibili rischi insiti in una strada che si sceglie di percorrere e che, per quanto possa sembrare semplice e sgombra di ostacoli, in realtà cela tranelli in ogni dove.

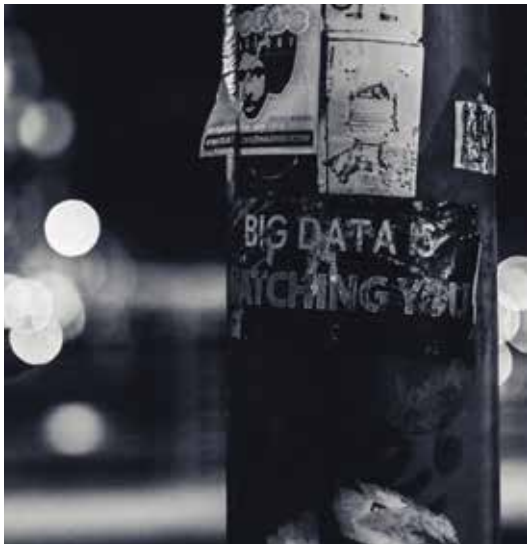
Sapere utilizzare uno smartphone o un PC non ci mette al riparo dai rischi che ne conseguono.

Questa guida si propone l'intento di mettere in guardia e di salvaguardare coloro che potrebbero pensare che di questi consigli, in realtà, non abbiano assolutamente bisogno.

Internet è un luogo talmente vasto che trovare una stella polare risulta fondamentale per evitare di inciampare. Per questo occorre un'adeguata educazione digitale che

consenta di percepire i pericoli insiti nella navigazione su quei siti che barattano le nostre passioni in cambio della nostra privacy, o peggio, dell'integrità delle nostre finanze. Questo perché i dati che noi cediamo sono "denaro".

I dati che noi cerchiamo di salvaguardare strenuamente vengono così ceduti col sorriso inconsapevole di chi è in attesa di una puntata della propria serie tv preferita, tra un pop-up e un click di troppo. Quel PC che tanto gelosamente proteggiamo dietro l'apparente sicurezza di una password di login, è il primo mattoncino del nostro castello che inizia a cadere, e che porta con sé tutto il resto. La criminalità su più livelli lo ha capito e, fiutando il business, ha saputo estendere i propri tentacoli anche su questo settore, certamente meno rischioso rispetto a quelli che fanno parte del proprio background storico. La favola dei cosiddetti "nerd" che sfruttano le proprie conoscenze



per dare al popolo gratuitamente ciò che i "cattivi" vorrebbero far pagare è quella menzogna addolcita che raccontiamo a noi stessi per tirarci fuori dalla sabbia mobile dell'illegalità, in cui scegliamo noi stessi di sguazzare, ogni volta che cediamo alle lusinghe di questo sistema.

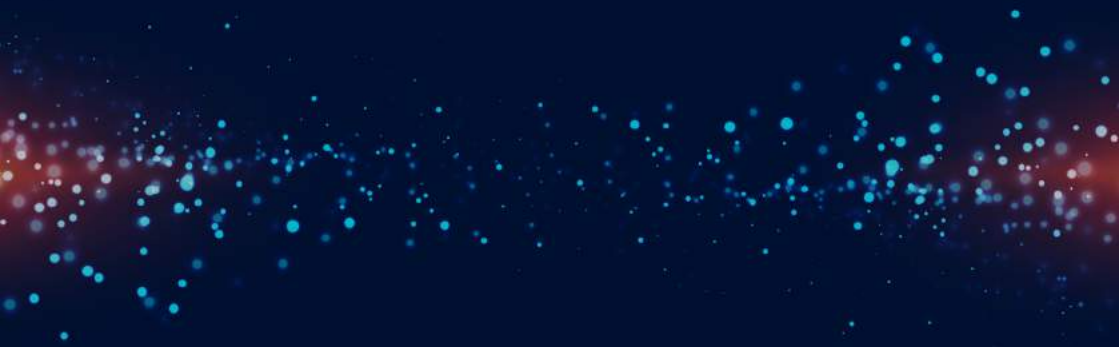
Qui si parla di posti di lavoro che vanno letteralmente in fumo perché si decide di non produrre più un film o una serie televisiva in quanto consapevoli che dopo pochi giorni, quell'opera verrà distribuita gratuitamente e abusivamente, bypassando il giusto riconoscimento agli autori, ai produttori e a tutte le maestranze che hanno lavorato per realizzare quel prodotto. Quel riconoscimento che dovrebbe essere sembre tutelato e garantito ad una così nobile arte che dall'ingegno vede il suo inizio, divenendo trama, storia da raccontare, animata da persone che con impegno, dedizione e professionalità rendono quella scintilla di creatività un pezzo di cultura del nostro Paese.

Dobbiamo dunque sapere che quando accendiamo un PC e cerchiamo un sito web per vedere qualcosa che in rete non dovrebbe esservi, non solo stiamo violando precise regole normative, non solo mettiamo a repentaglio la nostra sicurezza e i nostri dati, contribuendo all'erosione di un settore come quello audiovisivo, che solo in Italia

impiega oltre 180.000 persone, ma agiamo a favore invece dell'industria dell'illegalità, fiorente e incontrollata, che nulla apporta al Sistema Paese in termini di occupazione e ricchezza.

Bisogna capire da che parte stare e fare la scelta giusta, in questi casi, vuol dire muovere il primo passo verso una consapevolezza maggiore verso questo crimine, contrastandolo e facendo in modo di sostenere il settore audiovisivo, garantendo allo stesso tempo un livello di sicurezza adeguato alle nostre risorse (dati bancari, privacy, dati anagrafici, ecc.), che rappresentano quelle stesse risorse che ci ostiniamo con tanta veemenza a difendere e che con altrettanta ingiustificata, quanto smodata, incoscienza, sacrifichiamo sull'altare della pirateria on line.

E tu, da che parte stai?



FAPAV

Federazione per la Tutela dei Contenuti Audiovisivi e Multimediali

Viale Regina Margherita 286 | 00198 Roma

www.fapav.it | info@fapav.it