UNIVERSITÀ DEGLI STUDI DI PAVIA

DIPARTIMENTI DI GIURISPRUDENZA, INGEGNERIA INDUSTRIALE E DELL'INFORMAZIONE, SCIENZE ECONOMICHE E AZIENDALI, SCIENZE POLITICHE E SOCIALI, STUDI UMANISTICI

CORSO DI LAUREA INTERDIPARTIMENTALE IN

COMUNICAZIONE, INNOVAZIONE, MULTIMEDIALITÀ

LA PIRATERIA ONLINE E IL SUO CONTRASTO

Relatore:

Chiar.mo Prof. FABRIZIO SANNA

Correlatore:

Chiar.mo Prof. EMANUELE TUCCARI

Tesi di laurea di

ALESSIA SINA

ANNO ACCADEMICO 2023/24

Esprimo la mia più profonda gratitudine al Prof. Fabrizio Sanna per il costante supporto e la preziosa guida durante tutto il percorso di stesura di questa tesi. I suoi suggerimenti e il suo incoraggiamento sono stati fondamentali per il raggiungimento di questo traguardo.

Un sentito ringraziamento va anche all'Avv. Stefano Longhini e all' Avv. Vincenzo Colarocco, per aver gentilmente messo a disposizione documenti e risorse essenziali per la mia ricerca. La loro disponibilità e competenza sono state di grande aiuto nella realizzazione di questo lavoro.

Infine, un ringraziamento speciale va anche alla mia famiglia, al mio fidanzato, ai miei colleghi universitari e a tutti i miei amici.

INDICE

LA PIRATERIA ONLINE E IL SUO CONTRASTO

INTRODUZIONE

La pirateria online rappresenta una delle sfide più complesse del mondo digitale contemporaneo. In un'epoca in cui l'accesso ai contenuti digitali è divenuto quasi illimitato, il fenomeno della pirateria si è evoluto, sfruttando le nuove tecnologie per aggirare le leggi sul diritto d'autore e minare le fondamenta dell'industria dei media e dell'intrattenimento. Questa pratica si estende a numerosi settori, dalla musica al cinema, dai libri al software. In questo modo, si genera un impatto molto pregiudizievole sia in termine economici che culturali. Le cause della pirateria online sono molteplici e interconnesse. Trovano le proprie radici nelle dinamiche economiche, sociali e tecnologiche della nostra società. La difficoltà di accesso legale ai contenuti in molte ragioni del mondo, i costi elevati dei prodotti digitali, le discrepanze nella distribuzione dei contenuti e la percezione diffusa che l'accesso alla cultura debba essere un diritto universale sono solo alcuni dei fattori che spingono milioni di persone a rivolgersi a piattaforme illegali. Inoltre, la facilità con cui è possibile scaricare e condividere contenuti piratati ha reso la pirateria un'opzione sempre più attraente per molti utenti, specialmente in un contesto in cui l'anonimato online offre una protezione percepita contro le conseguenze online.

La pirateria non è un fenomeno nuovo; affonda le sue radici nei primi giorni di Interne e dei media digitali. Sin dagli anni '80, con l'emergere dei Bulletin Board Systems (BBS), i primi sistemi di condivisione di software e contenuti digitali protetti da copyright, la pirateria è divenuta un problema crescente. Questo fenomeno ha subito una rapida evoluzione con l'avvento delle reti di condivisione file peer-to-peer (P2P) negli anni 90, che hanno reso possibile la diffusione massiccia di contenuti digitali illeciti, come musica, film e software. Napster, Kazaa, eMule e BitTorrent sono solo alcuni degli strumenti che hanno facilitato questa pratica. Sono stati loro a trasformare il modo in cui i contenuti digitali vengono consumati a livello globale. Oggi, la pirateria online rappresenta una sfida significative per le industrie creative, che devono affrontare perdite economiche ingenti e un'erosione della propria base di consumatori legali. Nonostante gli sforzi per combattere il fenomeno attraverso misure legali, tecnologie di protezione dei contenuti, come i sistemi di Digital Rights Management (DRM) e campagne di sensibilizzazione, la pirateria continua a prosperare, alimentata dalla domanda incessante di contenuti digitali gratuiti e facilmente accessibili. Questa tesi si propone

di esplorare in profondità le dinamiche della pirateria online, analizzando le sue cause, le sue conseguenze e le sue strategie di contrasto dai vari settori colpiti, con l'obiettivo di fornire una panoramica completa e aggiornata su uno dei fenomeni più controversi dell'era digitale.

Il primo capitolo offre una panoramica generale sulla pirateria online e ne analizza le cause che hanno portato alla sua diffusione e i primi casi storici. Viene esplorato il contesto socioeconomico e tecnologico che ha favorito la nascita della pirateria digitale. Si esaminano le principali piattaforme e tecnologie che hanno facilitato la pirateria, come Napster e BitTorrent. Si discute, inoltre, di come la mancanza di accesso legale ai contenuti, le discrepanze nei tempi di distribuzione e i costi elevati dei prodotti digitali abbiano contribuito alla diffusione della pirateria.

Il secondo capitolo si concentra sugli strumenti tecnologici sviluppati per contrastare la pirateria online. Tra questi, un'attenzione particolare è dedicata ai sistemi di Digital Rights Management (DRM), che sono stati progettati per proteggere i contenuti digitali dalle copie non autorizzate. Il capitolo analizza le componenti dei sistemi DRM, l'evoluzione di queste tecnologie nel contesto del mercato globale e le implicazioni economiche, politiche e legali che ne derivano. Si esplorano inoltre le sfide legate alla protezione dei consumatori e alla privacy nei sistemi DRM. Vengono considerati anche i possibili scenari futuri e le implicazioni giuridiche legate all'equo compenso per l'uso di queste tecnologie.

Il terzo capitolo affronta gli aspetti legali e procedurali nel contrasto alla pirateria online. Viene analizzata la tutela del diritto d'autore nel contesto digitale, con particolare riferimento alle opere protette, e si discutono le norme e gli strumenti di tutela a disposizione nei vari ambiti: civilistico, penalistico e amministrativo. Viene esaminato il ruolo delle istituzioni e delle leggi, come il regolamento AGCOM e la legge antipirateria, nel proteggere i diritti d'autore e nell'arginare la diffusione dei contenuti piratati. Il capitolo offre una visione dettagliata delle procedure legali utilizzate per perseguire i pirati informatici e le piattaforme che facilitano la pirateria, e ne evidenzia le difficoltà e le complessità di far rispettare queste normative in un contesto globale.

Il quarto, e ultimo, capitolo si concentra su un caso di studio specifico: il fenomeno del *pezzotto,* una delle forme più diffuse e complesse di pirateria nel contesto italiano. Viene analizzato il rilievo e la diffusione di questo fenomeno, che consente l'accesso illegale a canali televisivi a pagamento, e le modalità attraverso cui viene contrastato, sia tramite l'uso di sistemi tecnici avanzati sia attraverso l'applicazione del diritto penale. Il capitolo esplora le implicazioni economiche e legali

del pezzotto, e mette in evidenza come questo caso rappresenti una delle principali sfide nel contrasto alla pirateria in Italia e in Europa.

I. PIRATERIA ONLINE: UNA PANORAMICA GENERALE

1. CAUSE DELLA PIRATERIA ONLINE E PRIMI CASI

La pirateria online è un fenomeno complesso e multifattoriale presente nel mercato dei contenuti digitali sin dagli albori di Internet. La sua diffusione è alimentata da diverse cause interconnesse. In primo luogo, l'assenza di accesso legale ai contenuti digitali, in molte aree del mondo, induce i consumatori a scegliere la pirateria come unica alternativa per ottenerli. Le piattaforme legali spesso non riescono a coprire uniformemente il mercato globale, lasciando un vuoto che viene colmato dai siti pirata. Ad esempio, in alcune aree geografiche non è possibile accedere legalmente a determinati film, serie televisive o album musicali. Questa mancanza costringe i residenti a rivolgersi alla pirateria per ottenere questi contenuti. Le discrepanze nei tempi di distribuzione di film, musica e altri contenuti tra diverse aree geografiche, inoltre, generano una frustrazione che incoraggia ulteriormente il consumo illegale. Quando un contenuto viene rilasciato in un'area geografica molto prima rispetto ad altre, gli utenti delle regioni escluse spesso si sentono svantaggiati e ricorrono alla pirateria per accedere ai contenuti nello stesso momento degli altri. Questa pratica è comune nel settore cinematografico, dove le anteprime e i rilasci scaglionati sono frequenti.

Il costo elevato dei contenuti digitali legali rappresenta un'altra barriera economica significativa per molti consumatori. Ed è così che la pirateria diventa un'alternativa più accessibile. I prezzi elevati di film, musica, software e libri digitali possono essere proibitivi per una parte consistente della popolazione, specialmente in periodi di crisi economica. La pirateria offre un modo per accedere a questi contenuti senza sostenere il costo elevato e incentiva il comportamento illegale[1].La facilità con cui è possibile scaricare e condividere contenuti piratati su Internet contribuisce ulteriormente alla diffusione del fenomeno. Piattaforme peer-to-peer, siti di torrent e servizi di streaming illegali offrono un accesso rapido e spesso gratuito a una vasta gamma di materiali digitali[2]. La tecnologia ha reso estremamente semplice per gli utenti trovare e scaricare file illegali,

[1] **SMITH M. D. e JONSSON J. E.**, *What the Online Piracy Data Tells Us About Copyright Policymaking,* Hudson Institute, 2023 https://www.hudson.org/intellectual-property/what-online-piracy-data-tells-us-about-copyright-policymaking

[2] **JENNINGS K. e BOSSLER A.M**, In: Holt, T., Bossler, A. (eds) *The Palgrave Handbook of International Cybercrime and Cyberdeviance.* Palgrave Macmillan, Cham, 2020. https://doi.org/10.1007/978-3-319-78440-3_44

spesso con pochi clic. Questo accesso semplificato riduce la barriera tecnica e rende la pirateria un'opzione attraente per molti. La percezione di anonimato online riduce il timore di conseguenze legali, mentre la cultura digitale, prevalente in alcune comunità, considera la pirateria come un comportamento socialmente accettabile, se non addirittura normale. L'anonimato offerto da Internet fa sì che molti utenti si sentano protetti dalle conseguenze legali delle loro azioni, e anzi sono incoraggiati a infrangere le leggi sulla proprietà intellettuale. Inoltre, in alcune subculture online, la pirateria è vista come un atto di ribellione contro le grandi aziende o come un modo legittimo di condividere la cultura[3]. La qualità dei servizi legali spesso non riesce a competere con quella dei servizi pirata, i quali offrono interfacce user-friendly e l'assenza di pubblicità invasive. Gli utenti che scelgono i servizi pirata spesso trovano un'esperienza d'uso superiore rispetto a quella offerta dai servizi legali, con meno restrizioni e interruzioni. Questo può includere la disponibilità di contenuti ad alta definizione, download veloci e un'ampia selezione di materiali senza le limitazioni imposte dai diritti digitali di gestione (DRM). Infine, la mancanza di consapevolezza sulle leggi sulla proprietà intellettuale e sulle conseguenze della pirateria, unita alla percezione che l'accesso alla cultura e all'informazione debba essere un diritto universale, contribuisce a perpetuare il fenomeno. Alcuni utenti non sono pienamente consapevoli delle leggi che proteggono i diritti d'autore e delle potenziali sanzioni legali che potrebbero affrontare. Inoltre, esiste una convinzione diffusa che l'accesso alla cultura debba essere gratuito e disponibile per tutti, indipendentemente dalla capacità di pagare[4]. Questi fattori combinati creano un ambiente favorevole alla pirateria online, nonostante gli sforzi legali e tecnologici per contrastarla. La complessità del fenomeno impone un approccio multidisciplinare per capire a fondo le sue cause e trovare strategie efficaci per affrontarlo.

Come abbiamo già detto in precedenza, la storia della pirateria online risale ai primi giorni di internet e dei media digitali. Uno dei primi casi significativi è rappresentato dallo sviluppo e dall'uso dei **Bulletin Board Systems (BBS)** negli anni '80. I BBS consentivano agli utenti di condividere software, compresi quelli protetti dal diritto d'autore. Nascono così le prime forme di

[3] **GUBITOSA C.,** *Elogio della pirateria. Dal Corsaro Nero agli hacker, dieci storie di ribellioni creative,* Terre di mezzo, 2000

[4] **EUIPO**, *I cittadini europei e la proprietà intellettuale: percezione, consapevolezza e comportamento,* 2023 https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2023_IP_Perception_Study/2023_IP_Perception_Study_ExSum_it.pdf

pirateria digitale: gli utenti cominciano a caricare e scaricare software, spesso eludendo l'acquisto legale[5].

Prima dell'avvento del World Wide Web e dei social network, le Bulletin Board System (BBS) rappresentavano un'importante forma di comunicazione e scambio di informazioni su Internet. Il primo BBS fu lanciato il 16 febbraio 1978, in un periodo in cui aziende come Apple e Microsoft erano ancora startup emergenti guidate da giovani imprenditori. Questi sistemi erano accessibili tramite collegamenti telefonici, i quali comportavano tempi di attesa lunghi e una connettività limitata[6]. Durante il grande blizzard del Midwest statunitense alla fine del gennaio 1978, noto come "The Great Blizzard", due ragazzi trentenni appassionati di computer, Ward Christensen e Randy Suess, membri del club Cache (Chicago Area Computer Hobbyists Exchange), concepirono l'idea di portare online le bacheche elettroniche già presenti negli ambienti lavorativi e accademici. Queste bacheche, denominate Bulletin Board, divennero i precursori delle BBS. Nonostante il primo BBS fosse attivo già nel febbraio del 1978, la notizia del loro sviluppo fu divulgata solo nell'edizione di novembre della rivista specializzata Byte, suscitando un grande interesse nella comunità tecnologica dell'epoca. Negli anni '80, il numero di BBS crebbe rapidamente, ciascuna con una specializzazione tematica unica, nonostante le sfide tecnologiche e le limitazioni delle connessioni dell'epoca[7].Questo ambiente rappresentava un microcosmo di appassionati disposti a superare le difficoltà tecniche e le limitazioni della tecnologia emergente, contribuendo così allo sviluppo e alla diffusione delle prime forme di socialità online.

Un altro evento importante è stato l'introduzione delle **reti di condivisione file peer-to-peer (P2P)** alla fine degli anni '90. Uno dei casi più celebri è **Napster**. Lanciato nel 1999, da Shawn Fanning e Sean Parker, è diventato uno dei primi, e più famosi, software di pirateria online. Questa piattaforma permetteva di cercare e scaricare qualsiasi canzone desiderata, purché disponibile su uno dei computer utilizzanti il programma, permettendo agli utenti di scaricarla gratuitamente e successivamente condividerla con gli altri. La crescita di Napster è stata esponenziale: già nell'ottobre del 1999 contava 4 milioni di canzoni disponibili, e entro marzo 2000, meno di un anno dopo il lancio, gli utenti del software superavano i 20 milioni. Durante l'estate dello stesso anno, venivano scaricate

[5] **SHINDER LITTLEJOHN D. E CROSS M.** *Scene of the Cybercrime*, 2 ed., 2008 https://www.sciencedirect.com/science/article/abs/pii/B9781597492768000029

[6] **LUNA R.,** *Va online la prima Bbs: era come stare sui social network prima del Web*, La Repubblica, 2022 https://www.repubblica.it/tecnologia/2022/02/16/news/va_online_la_prima_bbs_un_po_come_stare_sui_social_network_prima_del_web-337936092/

[7] **CROSS M.,** *Social Media Security. Leveraging Social Networking While Mitigating Risk,* 2013

circa 14.000 canzoni al minuto. Questa proliferazione ha scosso profondamente l'industria musicale, soprattutto quando la **Recording Industry Association of America (RIAA)**, riunitasi a Washington, scoprì che praticamente tutte le sue canzoni erano presenti su Napster. La creazione di Fanning e Parker, inizialmente, sembrava innocua: Napster consentiva agli utenti di condividere file indipendentemente dal loro status di copyright, senza archiviarli su server centralizzati. Tuttavia, scaricare tali file violava le leggi sul copyright, e nel 2001 le prime denunce colpirono rapidamente 18.000 utenti. Poco dopo, la RIAA e grandi nomi come Metallica e Dr. Dre intentarono una causa diretta contro i creatori del software. I tribunali decisero rapidamente che Napster violava il **Digital Millennium Copyright Act**[8] ed emisero un ultimatum: rimuovere tutti i contenuti protetti da copyright o chiudere il programma. I fondatori non riuscirono a rispettare le disposizioni del tribunale, e così, nel luglio 2001, solo due anni dopo la sua nascita, Napster chiuse. Tuttavia, questo non fermò l'esplosione dell'uso di cloni di Napster su internet, che resero il download illegale di musica, e successivamente di film e serie TV, una pratica quotidiana per un numero crescente di utenti della rete. Kazaa, Gnutella, eMule, DC++, Audio Galaxy e Soul Seek, tra gli altri (alcuni dei quali ancora attivi oggi), sono solo alcuni dei software più noti che hanno adottato e migliorato il concetto di peer-to-peer introdotto da Napster. Inoltre, il 2 luglio 2001, proprio mentre Napster stava chiudendo, il ventiseienne Bram Cohen lanciò su internet BitTorrent, che rimane oggi lo strumento più importante per la condivisione di file peer-to-peer[9].

I primi anni 2000 hanno visto la proliferazione di siti torrent come **The Pirate Bay**, che facilitavano la condivisione di file più grandi tra cui film, software e giochi. Queste piattaforme utilizzavano il protocollo BitTorrent, che semplificava la condivisione di grandi file suddividendoli in pezzi più piccoli e distribuendoli su molti computer degli utenti. In questo modo la rete divenne più resiliente e difficile da chiudere completamente. Fondato nel 2003 in Svezia da un gruppo di attivisti anti-copyright, questo tracker torrent ha rapidamente ottenuto una vasta popolarità grazie alla sua ricca selezione di contenuti, che include film, serie TV, musica, software, videogiochi e altro ancora. The Pirate Bay si distingue per la sua interfaccia user-friendly, la semplicità d'uso e la capacità

[8] Il Digital Millennium Copyright Act (DMCA) è una legge statunitense sul diritto d'autore che implementa i due trattati del 1996 dell'Organizzazione Mondiale per la Proprietà Intellettuale. Questa normativa rende illegale la produzione e la distribuzione di tecnologie, strumenti o servizi che possono essere utilizzati per aggirare le misure di protezione degli accessi a opere coperte dal copyright, noti anche come DRM (Digital Rights Management).

[9] **SIGNORELLI A. D.,** *Cosa resta di Napster, 20 anni dopo. Wired Italia*, 2019 https://www.wired.it/attualita/tech/2019/06/01/napster-20-anni-dopo-storia-sean-parker/

di fornire accesso a contenuti altrimenti difficili da ottenere o costosi da acquistare, diventando un punto di riferimento per milioni di utenti in tutto il mondo[10].

Un ultimo caso emblematico nella storia della pirateria online è **eMule**. Creato il 13 maggio 2002 dal programmatore tedesco Hendrik Breitkreuz, noto anche come Merkur, questo software ha rapidamente attirato un gruppo di sviluppatori devoti, trasformandolo in uno strumento imprescindibile per gli utenti dell'epoca. La prima versione ufficiale è stata rilasciata il 9 agosto, supportando inizialmente i sistemi Windows 2000 e Windows XP. In quanto basato su licenza libera, il programma è stato sempre distribuito gratuitamente. Questo sistema prevede due reti peer-to-peer: eDonkey e Kad. Nonostante il suo successo abbia visto il software scaricato oltre 700 milioni di volte in tutto il mondo, nel corso degli anni ha perso parte della sua popolarità originaria. Nonostante ciò, ha mantenuto un'aura di rilevanza con una comunità di utenti e sviluppatori che, nonostante le difficoltà e la riduzione della base di utenti, hanno continuato a supportarne lo sviluppo[11].

Nel corso degli anni, la crescente popolarità di eMule ha portato a una serie di complicazioni legali a causa della presenza diffusa di contenuti protetti da copyright. Questo ha attirato l'attenzione indesiderata da parte di istituzioni, forze dell'ordine e importanti aziende cinematografiche. Nel 2006, la polizia belga ha agito per chiudere due dei server più noti del programma; nel 2007, Francia, Paesi Bassi e Germania hanno fatto altrettanto con altri tre server. Nonostante le azioni legali e la graduale perdita di popolarità nel tempo, eMule è riuscito a resistere: sorprendentemente, ha evitato il destino di molti dei suoi concorrenti dell'epoca. Mantenendo salda la sua filosofia originaria, eMule ha continuato per la sua strada senza essere completamente messo a tacere[12].

Questo periodo ha segnato un'escalation significativa nella scala e nell'impatto della pirateria online, passando dai forum di nicchia e dai BBS all'uso mainstream di internet. La crescita della pirateria digitale è stata alimentata da diversi fattori, tra cui la crescente disponibilità di internet ad alta velocità, la mancanza di alternative legali accessibili e la facilità di accesso ai contenuti piratati. La lenta risposta iniziale dell'industria al passaggio al digitale e il fallimento nel fornire tempestivamente accesso conveniente ai contenuti digitali hanno ulteriormente alimentato la crescita della pirateria. Nel tempo, le misure per combattere la pirateria si sono evolute, con un aumento delle

[10] **PIROSA G.**, *Piratebay: storia e sviluppi del sito di Torrent più famoso,* digital-pr.it., 2024 https://www.digital-pr.it/piratebay-storia-e-sviluppi-del-sito-di-torrent-piu-famoso/

[11] **LAI M.,** *eMule: origini e ritorno alla ribalta dello storico software p2p*., Everyeye Tech, 2020 https://tech.everyeye.it/articoli/speciale-emule-origini-ritorno-ribalta-storico-software-p2p-50124.html

[12] Ibidem

azioni legali e lo sviluppo delle tecnologie di gestione dei diritti digitali (DRM), sebbene con successi alterni.

2. DIMENSIONE FATTUALE DEL FENOMENO (SETTORI PIÙ COLPITI)

La pirateria online incide gravemente su vari settori economici e determina ingenti perdite finanziarie e danni all'integrità del mercato legale. Uno dei settori a risentire maggiormente dei danni causati dalla pirateria informatica è l'industria musicale: vi sono state, in questi ultimi anni, ingenti perdite economiche e gravi danni alla creatività artistica. I download e lo streaming non autorizzati riducono drasticamente le entrate per artisti e case discografiche, e limitano la capacità di investire in nuovi talenti e progetti. Questo calo delle entrate implica una diminuzione delle royalties e dei compensi che dovrebbero sostenere la carriera degli artisti, in particolare quelli emergenti. Inoltre, la pirateria mina l'intera catena del valore della musica, dagli autori ai produttori, danneggiando l'ecosistema musicale nel suo complesso. Nel settore musicale si parla molto di produzione non autorizzata. Questo termine si riferisce alla duplicazione o distribuzione di opere musicali senza il permesso del titolare dei diritti d'autore. Questo tipo di violazione può assumere diverse forme, tra cui, ad esempio, la masterizzazione di CD, la distribuzione digitale e la riproduzione fisica[13].

La masterizzazione di CD è un processo tecnico che consente di copiare dati su un disco compatto (CD) utilizzando un masterizzatore, un dispositivo hardware collegato a un computer[14]. Sebbene il processo di masterizzazione sia legale quando viene effettuato per uso personale o con autorizzazione, diventa illegale quando si tratta di duplicare contenuti protetti da copyright senza il permesso del titolare dei diritti, con l'intento di distribuirli o venderli. La riproduzione non autorizzata di CD avviene proprio in questa maniera: quando una persona copia contenuti musicali protetti da diritto d'autore senza il consenso del titolare dei diritti, con l'obiettivo di distribuirli o venderli. Questo comportamento è considerato pirateria e comporta gravi conseguenze legali. La diffusione della masterizzazione illegale è favorita principalmente dalla sua economicità e dalla facilità di accesso agli strumenti necessari. La pratica consente la duplicazione su larga scala a costi contenuti, rendendola attraente per chi desidera produrre molte copie senza investimenti significativi. Inoltre,

[13] **BENEGGI M.,** *Legalpop, cos'è la pirateria informatica, quali sanzioni ha,* 2021

[14] **BARILLARO A.,** *Cosa significa masterizzare e come si fa,* 2023 articolo disponibile su www.informaticapertutti.com

l'ampia disponibilità sul mercato dei masterizzatori e dei software necessari, unita alla loro semplicità d'uso, facilita l'adozione di questa pratica anche da parte di individui con limitate competenze tecniche.

La pratica della masterizzazione illegale di CD comporta diversi impatti negativi, tra cui significative perdite economiche per gli artisti e le case discografiche[15]. Queste perdite derivano dal fatto che ogni copia pirata rappresenta una potenziale vendita persa del prodotto originale. Le conseguenze sono disastrose e comprendono la riduzione dei profitti e la limitazione delle risorse disponibili per le nuove produzioni e per lo sviluppo artistico. Inoltre, i CD masterizzati illegalmente tendono a presentare una qualità inferiore rispetto agli originali, sia in termini di qualità audio che di durabilità del supporto stesso. Ciò può influenzare negativamente l'esperienza del consumatore, e può compromettere la reputazione degli artisti e delle etichette discografiche. I consumatori potrebbero associare la bassa qualità del prodotto alla sua fonte originale. Si potrebbe creare così un danno reputazionale. Dal punto di vista legale, la masterizzazione illegale è soggetta a severe sanzioni. Coloro che sono coinvolti in questa pratica possono affrontare sanzioni significative e, in casi gravi, anche pene detentive, in linea con le rigide leggi sul diritto d'autore volte a proteggere i diritti dei detentori dei contenuti[16].

Un'altra forma sofisticata di pirateria online dell'industria musicale è la contraffazione, la quale non solo viola i diritti d'autore, ma inganna anche il consumatore finale. Questa pratica comporta la produzione e distribuzione di copie identiche all'originale, complete di logo, ologrammi di autenticità ed imballaggi. La contraffazione nell'ambito della pirateria online dei prodotti dell'industria musicale rappresenta una grave minaccia economica e culturale per gli artisti, le etichette discografiche e l'intero settore musicale. Questo fenomeno si manifesta attraverso la diffusione non autorizzata di opere musicali tramite la condivisione e il download di file audio, senza il consenso dei titolari dei diritti d'autore[17].

La pirateria online ha un impatto significativo sulle entrate economiche dell'industria musicale. L'accesso gratuito o a basso costo alla musica riduce drasticamente le vendite legali di album e singoli, oltre a compromettere la sostenibilità finanziaria degli artisti e delle etichette

[15] **JINDAL M.,** *How Much Does Piracy Cost the Music Industry? – 8 Effects*, Bytescare blogs, 2024, https://bytescare.com/blog/how-much-does-piracy-cost-the-music-industry

[16] Ibidem

[17] **FIMI**, *FPM – Contro la pirateria musicale e multimediale,* 2024 https://www.fimi.it/chi-siamo/tutela-dei-contenuti/fpm.kl

discografiche. Le perdite economiche limitano le risorse disponibili per nuove produzioni musicali e per il supporto agli artisti emergenti, e influenzano negativamente la diversità e l'innovazione all'interno del panorama musicale. Inoltre, la pirateria online spesso porta a una degradazione della qualità dell'esperienza d'ascolto. I file musicali piratati sono frequentemente di qualità inferiore rispetto alle versioni ufficiali. Viene compromessa così la fedeltà e la chiarezza dell'audio. Questo fenomeno può danneggiare la reputazione degli artisti, poiché i consumatori potrebbero erroneamente associare la scarsa qualità del materiale piratato alla sua origine legittima. La percezione di una qualità inferiore può influenzare negativamente l'immagine dell'artista e la fiducia del pubblico nelle produzioni musicali originali. Dal punto di vista normativo e legale, la pirateria online solleva complesse questioni di enforcement. Le violazioni del copyright derivanti dalla pirateria online possono portare a azioni legali, multe e sanzioni per gli individui coinvolti nella distribuzione illegale di contenuti musicali. Tuttavia, la natura globale e decentralizzata di Internet rende difficile l'identificazione e il perseguimento degli autori di tali violazioni, spesso operanti attraverso canali e piattaforme digitali che sfuggono alle giurisdizioni nazionali[18].

Per contrastare efficacemente la pirateria online, l'industria musicale adotta una serie di strategie integrate. Queste includono l'implementazione di tecnologie avanzate di protezione dei contenuti, la collaborazione con piattaforme digitali per identificare e rimuovere contenuti piratati, e sforzi educativi per sensibilizzare il pubblico sugli impatti negativi della pirateria sulla creatività artistica e sulla sostenibilità economica dell'industria musicale[19].La contraffazione nell'ambito della pirateria online dell'industria musicale rappresenta una sfida critica che richiede una risposta globale e coordinata. È essenziale promuovere un ambiente digitale sicuro e sostenibile che protegga i diritti dei creatori musicali e sostenga la diversità culturale attraverso iniziative legislative, tecnologiche e educative mirate.

Come abbiamo già detto, la pirateria online nel settore musicale può assumere diverse forme, tra cui anche la distribuzione digitale e la riproduzione fisica del prodotto. In un mondo in cui la distribuzione digitale si sta espandendo velocemente, la distribuzione fisica della musica, attraverso formati come CD e vinili, potrebbe sembrare un anacronismo. Nonostante tutto però continua a rivestire un ruolo significativo nel panorama musicale contemporaneo. Esistono diverse ragioni che

[18] **RIAA**, *About Piracy,* 2022, https://www.riaa.com/resources-learning/about-piracy/

[19]**BACCI M.,** *Plagio Musicale e Contraffazione di Opera Musicale,* IPRights, 2020 https://www.iprights.it/plagio-musicale/

ne attestano la validità come opzione ancora rilevante. In primo luogo, il possesso di una copia fisica di un album musicale rappresenta molto più che un semplice mezzo per ascoltare musica. Esso permette di possedere un oggetto artistico tangibile, conferendo una sensazione unica di proprietà che la musica digitale non può replicare. Tenere in mano un CD o un vinile offre un'esperienza estetica e sensoriale che va oltre la mera fruizione sonora. Dal punto di vista della qualità del suono, i supporti fisici, in particolare i dischi in vinile, sono rinomati per la loro capacità di riprodurre un suono caldo e ricco, altamente apprezzato dagli audiofili. Questo tipo di qualità sonora è spesso sacrificata nei formati digitali compressi, rendendo la distribuzione fisica preferibile per chi dà priorità alla fedeltà acustica.[20]

Un altro aspetto rilevante è il valore di rivendita che caratterizza la musica fisica. A differenza dei file digitali, le copie fisiche, specialmente quelle rare o in edizioni limitate, possono aumentare di valore nel tempo, offrendo non solo un piacere estetico e acustico, ma anche un potenziale investimento economico. Le vendite fisiche continuano inoltre a giocare un ruolo cruciale nel determinare le posizioni in classifica. Nonostante la predominanza dei servizi di streaming, le vendite di supporti fisici contribuiscono significativamente alle metriche di successo commerciale, soprattutto in determinati generi musicali e tra specifici segmenti di pubblico. Pertanto, per gli artisti che aspirano a scalare le classifiche, la distribuzione fisica rimane una strategia da non sottovalutare. Tuttavia, è fondamentale considerare anche gli svantaggi associati alla distribuzione fisica della musica. Uno dei principali ostacoli è rappresentato dai costi. La produzione, lo stoccaggio e la spedizione di supporti fisici comportano spese notevoli, un fattore che può gravare in modo significativo sugli artisti indipendenti con risorse limitate. Inoltre, i supporti fisici richiedono spazio per essere conservati. Gli appassionati di musica con collezioni estese possono trovare problematico gestire lo spazio necessario per archiviare CD, vinili e cassette, un problema inesistente con la musica digitale. La disponibilità rappresenta un'altra limitazione. Non tutta la musica è pubblicata in formato fisico, con alcuni artisti che optano per il rilascio esclusivo sulle piattaforme digitali, limitando così le opzioni per chi preferisce il supporto fisico. I supporti fisici sono inoltre soggetti a danni e degrado nel tempo. Graffi su un CD o un vinile possono compromettere la qualità del suono o renderli del tutto inascoltabili, una preoccupazione che non si pone con i file digitali.

[20]**TEAM D.**, *Pros & Cons of Physical vs Digital Music Distribution*. Daisie Blog, 2024 https://blog.daisie.com/pros-cons-of-physical-vs-digital-music-distribution/

Passando alla distribuzione digitale della musica, emergono numerosi vantaggi. La comodità è senza dubbio uno degli aspetti più attraenti. La musica digitale può essere ascoltata ovunque e in qualsiasi momento, senza la necessità di trasportare supporti fisici. Questo formato elimina anche il problema dello spazio, consentendo di archiviare migliaia di brani su un singolo dispositivo senza alcun ingombro[21]. Dal punto di vista economico, la musica digitale è generalmente più conveniente. L'assenza di costi di produzione e spedizione rende l'acquisto di musica digitale più accessibile. Inoltre, la distribuzione digitale offre un accesso immediato ai nuovi rilasci, permettendo agli ascoltatori di fruire della musica istantaneamente, senza attese per la consegna. Nonostante questi vantaggi, la distribuzione digitale presenta alcune criticità. La mancanza di un prodotto fisico può risultare deludente per coloro che apprezzano l'esperienza tattile e visiva associata ai supporti fisici. I file digitali sono inoltre vulnerabili a corruzione, perdita o furto, con il rischio di perdere intere collezioni musicali in caso di problemi tecnici. La compressione dei file digitali può anche comportare una perdita di qualità audio, un fattore non trascurabile per gli audiofili. La dipendenza dalla tecnologia è un aspetto cruciale. Per ascoltare la musica digitale, è necessario disporre di dispositivi funzionanti e di una connessione internet stabile. Qualsiasi problema tecnico può rendere inaccessibile l'intera libreria musicale, una vulnerabilità assente nei supporti fisici. In conclusione, sia la distribuzione fisica che quella digitale della musica presentano vantaggi e svantaggi distinti. La scelta tra i due formati dipende dalle preferenze individuali e dalle esigenze specifiche di ogni ascoltatore. Il tema della distribuzione digitale e della pirateria online è di crescente importanza nell'industria dell'intrattenimento. Diversi studiosi hanno esplorato l'impatto della distribuzione digitale sulle vendite fisiche e sulla pirateria online attraverso un'analisi empirica basata sulle dinamiche di mercato associate ai contenuti di NBC su iTunes. Viene utilizzato come caso di studio la rimozione e la successiva reintegrazione dei contenuti di NBC dallo store di iTunes tra il 2007 e il 2008. Questi studiosi applicano un modello di differenza-in-differenze per valutare gli effetti sulla domanda di contenuti piratati e sulle vendite di DVD su Amazon.com[22].

La loro ricerca mostra un aumento dell'11,2% nella domanda di contenuti piratati in seguito alla rimozione dei contenuti da iTunes, corrispondente a circa 49.000 download giornalieri, indicando una risposta significativa del mercato illegale a variazioni nella disponibilità di contenuti legittimi. Tuttavia, la reintegrazione dei contenuti su iTunes non ha mostrato una riduzione altrettanto

[21] **TEAM D.**, *Pros & Cons of Physical vs Digital Music Distribution*. Daisie Blog, 2024 https://blog.daisie.com/pros-cons-of-physical-vs-digital-music-distribution/

[22] **DANAHER B, DHANASOBHON S., SMITH D. M. e TELANG R.**, *Converting Pirates Without Cannibalizing Purchasers: The Impact of Digital Distribution on Physical Sales and Internet Piracy,* 2010.

significativa nella pirateria e, anzi, suggerisce che la pirateria online possa essere influenzata più dalla disponibilità immediata di contenuti legittimi che dalla loro reintroduzione. Inoltre, non è stato riscontrato alcun impatto significativo sulle vendite di DVD di NBC su Amazon.com, indicando che la distribuzione digitale non ha necessariamente un effetto cannibalizzante sulle vendite fisiche[23]. Questo studio contribuisce in maniera significativa alla comprensione delle interazioni tra distribuzione digitale legittima e pirateria, nonché tra canali di distribuzione digitali e fisici. I risultati suggeriscono che i canali di distribuzione digitale legittimi possono competere efficacemente con quelli illegali, ma la disponibilità immediata di contenuti è cruciale per mitigare la pirateria. Inoltre, la distribuzione digitale non sembra compromettere le vendite fisiche, offrendo così un quadro più complesso delle dinamiche di mercato nell'era digitale.

La proliferazione della distribuzione digitale ha trasformato radicalmente il panorama dell'industria musicale, introducendo sia opportunità che sfide. Centrale in questa trasformazione è il problema della pirateria online, la quale rappresenta una preoccupazione economica di grande rilievo. La pirateria digitale, definita come la distribuzione e riproduzione non autorizzata di materiale protetto da copyright attraverso canali digitali, ha avuto un impatto profondo sull'industria musicale. La facilità con cui i file digitali possono essere copiati e condivisi ha portato a un sostanziale aumento dell'accesso non autorizzato alla musica, minando le fonti di reddito di artisti ed etichette discografiche. La pirateria digitale non solo riduce i costi per i consumatori, ma consente anche un accesso più ampio alla musica. Nonostante questi benefici per i consumatori, l'impatto negativo sui ricavi dell'industria musicale non può essere ignorato. La facilità con cui la musica digitale può essere riprodotta e distribuita ha facilitato la diffusione della pirateria ed ha reso difficile per l'industria controllare e monetizzare efficacemente i propri prodotti.

I metodi tradizionali per combattere la pirateria, come le restrizioni legali e le sanzioni, si sono dimostrati in gran parte inefficaci. I consumatori tendono a resistere alle misure proibitive e, la maggior parte delle volte, le considerano intrusive e controproducenti. Gli studiosi, invece, suggeriscono che l'industria musicale dovrebbe concentrarsi sull'adattamento alle nuove tecnologie e ai comportamenti dei consumatori. Ciò comporta la creazione di punti di accesso legali e convenienti per il consumo di musica che competono direttamente con i contenuti piratati. Ad esempio, servizi che offrono musica di alta qualità a basso costo e in formati user-friendly possono ridurre l'attrattiva

[23]**DANAHER B, DHANASOBHON S., SMITH D. M. e TELANG R.**, *Converting Pirates Without Cannibalizing Purchasers: The Impact of Digital Distribution on Physical Sales and Internet Piracy,* 2010.

della musica piratata. Inoltre, la possibilità di creare librerie musicali personalizzate e condividere musica con amici sono fattori significativi che possono incoraggiare l'uso di fonti di musica legale. In questo contesto entra in gioco SPOTIFY. Lanciata nel 2008, questa piattaforma ha rivoluzionato il modo in cui le persone consumano la musica e ha offerto un'alternativa legale e conveniente ai download illegali e ai Torrent. Il successo di SPOTIFY può essere attribuito al suo vasto catalogo di brani e alla sua interfaccia intuitiva. Questa applicazione ha permesso agli utenti di ascoltare milioni di canzoni gratuitamente, con la possibilità di passare ad un abbonamento premium per ulteriori funzionalità. Offre una piattaforma accessibile e a prezzo contenuto, e così facendo è riuscita ad attrarre milioni di utenti. Per l'industria musicale, l'ingresso di SPOTIFY ha rappresentato una speranza in un contesto dominato dalla pirateria. Con la sua proposta di un'alternativa legale, la piattaforma ha dato la possibilità di generare entrate ad artisti e case discografiche. Tuttavia, nonostante i benefici apportati, alcuni critici sostengono che il modello di pagamento della piattaforma non sia del tutto equo per gli artisti. I bassi tassi di royalty e i complessi sistemi di distribuzione hanno portato alcuni artisti a sentirsi insufficientemente compensati per il loro lavoro. Questo tema, infatti, continua ad essere oggetto di discussioni e negoziazioni tra artisti, case discografiche e piattaforme di streaming[24].

La pirateria musicale ha effetti di vasta portata che vanno oltre il semplice impatto economico sull'industria musicale. Questo fenomeno comporta una significativa perdita di entrate per artisti, etichette discografiche e altre parti coinvolte nella produzione e distribuzione musicale. Le vendite legali di musica vengono direttamente compromesse dalla disponibilità di copie illegali gratuite. Questo può ridurre i budget disponibili per investimenti in nuovi talenti e produzione musicale di qualità, danneggiando l'industria nel suo complesso. Inoltre, questa pratica illegale mina i diritti d'autore degli artisti e dei produttori. Il diritto d'autore è essenziale per garantire che gli artisti ricevano un compenso equo per il loro lavoro. La diffusione di copie non autorizzate compromette questo principio, riducendo l'incentivo per gli artisti a creare nuova musica e, di conseguenza, impoverendo il panorama musicale.

Le copie piratate spesso sono di qualità inferiore rispetto ai prodotti originali. La compressione dei file e la scarsa qualità di registrazione possono influire negativamente sull'esperienza di ascolto. Inoltre, le copie illegali possono essere accompagnate da malware o virus,

[24] **NEU M.,** *Understanding Music Piracy and its impact on the Industry,* Reprtoir, 2023 articolo disponibile su www.reprtoit.com

rappresentando un rischio per i dispositivi dei consumatori. La diffusione di copie illegali può danneggiare la reputazione degli artisti. Come abbiamo già precisato, vi è il rischio che i consumatori, quando accedono a musica di bassa qualità o incompleta, possano attribuire tale esperienza negativa all'artista stesso, anziché alla fonte piratata. Questo può influenzare negativamente la percezione pubblica e la popolarità degli artisti, oltre a comportare una riduzione delle entrate, la quale a sua volta può portare a tagli nel personale all'interno dell'industria musicale. Questo include non solo artisti e produttori, ma anche tecnici del suono, grafici, personale di marketing e molti altri professionisti che contribuiscono alla produzione e distribuzione della musica. La diminuzione delle opportunità di lavoro può avere un effetto a catena sull'intero settore culturale ed economico. La pirateria sfida la sostenibilità del modello economico tradizionale dell'industria musicale. Le etichette discografiche e gli artisti devono trovare nuovi modi per monetizzare la loro musica, spesso attraverso concerti, merchandising e licenze per l'uso della musica in altri media. Tuttavia, queste fonti di reddito alternative non sempre compensano le perdite derivanti dalla pirateria. In sintesi, mentre la distribuzione digitale ha aperto nuove opportunità per la fruizione della musica, la pirateria online rappresenta una minaccia significativa che richiede soluzioni innovative. Affrontare questa sfida comporta non solo l'implementazione di misure legali e tecnologiche, ma anche l'adattamento alle esigenze e ai comportamenti dei consumatori per creare un ecosistema musicale sostenibile e prospero. Un altro settore che subisce i danni della pirateria è quello televisivo. Negli ultimi anni la pirateria dei contenuti televisivi ha mostrato un andamento oscillante, evidenziando una serie di fattori complessi che influenzano questo fenomeno. Nonostante un calo degli accessi piratati ai contenuti televisivi in un primo periodo, a partire dalla seconda metà del 2021 si è osservato un aumento significativo. Questo fenomeno presenta una forma di consumo simile in molti Stati membri dell'Unione Europea, con importanti variazioni tra di essi e nel corso dei mesi all'interno dei vari paesi[25].

Uno studio recente dell'EUIPO – European Union Intellectual Property Office mostra che non ci sono stati cambiamenti di comportamento legati al Covid-19. Tuttavia nei mesi successivi alla crisi vi è stata un'inversione di tendenza al ribasso. Attualmente la tendenza è pressoché stabile con una media di circa cinque accessi piratati al mese per utente internet nell'UE27. Questo dato è significativamente inferiore al livello registrato nel 2017, ma è comunque superiore del 20% rispetto al minimo raggiunto nel 2020. Un'analisi più approfondita dei secondi trimestri di ciascun anno non

[25] **DARA V.,** *La pirateria registra ancora centinaia di miliardi di visite e genera danni ingenti per l'industria dei media,* 2022 articolo disponibile su www.insidemarketing.it

rivela un modello di comportamento diverso per il 2020. Tuttavia, il secondo trimestre del 2021 è stato caratterizzato da un notevole incremento della pirateria televisiva, iniziato nella seconda metà del 2020 e continuato fino alla fine del primo trimestre del 2022, stabilizzandosi successivamente. Questo indica che, sebbene il COVID-19 non abbia direttamente alterato i comportamenti di consumo illegale, il periodo immediatamente successivo alla crisi ha visto una ripresa della pirateria[26].

Secondo la rivista Economist, la pirateria dei prodotti televisivi attira meno attenzioni rispetto alla pirateria di prodotti musicali e prodotti cinematografici, ma è ugualmente diffusa. In termini economici, i download illegali sono il rimedio delle carenze causate dal fallimento del mercato. Scaricare contenuti in maniera illecita è un modo semplice per trovare materiale del mondo dell'intrattenimento che non sono immediatamente disponibili nel mercato di riferimento. La pirateria online di film e contenuti televisivi si divide in due principali categorie: scaricare l'intero file o usufruire di piattaforme di streaming. Il download di un film impiega pochi minuti, mentre lo streaming prevede l'inizio del film o del programma in pochi secondi. Entrambi i metodi utilizzano sistemi peer-to-peer (P2P) quali ad esempio BitTorrent. Queste due modalità di accesso a contenuti illegali generano la maggior parte del traffico su Internet.

L'industria televisiva ha subito numerosi danni legati alla pirateria. Le serie tv Dexter e Il Trono di Spade sono state piratate da tantissime persone, di fatti il numero di download illegali ha superato di gran lunga il numero degli spettatori legittimi. Il problema della pirateria cinematografica e televisiva, nonostante gli sforzi delle autorità anti-pirateria, sembra essere in aumento. Secondo i dati forniti dall'azienda britannica MUSO, specializzata nell'analisi del consumo di media non autorizzati e della domanda di pirateria globale, il fenomeno della pirateria è in piena espansione. Infatti, nel 2022 la pirateria cinematografica è aumentata del 38,6% rispetto all'anno precedente, mentre le visite ai siti di pirateria per contenuti televisivi sono cresciute dell'8,8%. MUSO ha riportato un totale di 215 miliardi di visite illegali ai siti di pirateria l'anno scorso. Questi dati suggeriscono che il fenomeno non solo persiste, ma sta crescendo rapidamente[27].

MUSO identifica diverse cause alla base di questa tendenza. Innanzitutto, l'azienda britannica identifica come prima causa l'aumento del volume dei contenuti Post Pandemia. La produzione dei contenuti è effettivamente aumentata dopo la crisi del Covid-19, con le numerose

[26] **EUIPO**, *Online Copyright Infringement in EU 2023*, 2023. https://www.euipo.europa.eu/it/publications/online-copyright-infringement-in-eu-2023

[27] **RAVI A., RAJAMANI K. e LEKSHMI R. S.,** *A study on movie piracy,* Researchgate, 2018 https://www.researchgate.net/publication/340953152_A_STUDY_ON_MOVIE_PIRACY

uscite di film e serie TV. La seconda causa è, invece, rappresentata dall'esclusività delle piattaforme di abbonamento. Molti contenuti sono disponibili su diverse piattaforme di streaming legale, le quali prevedono un abbonamento. Ciò può rendere difficile e costoso l'accesso a tutti i diversi contenuti desiderati. Infine, un'ultima causa è data dalle pressioni economiche globali: l'inflazione e le difficoltà economiche hanno ridotto la capacità di spesa dei consumatori, spingendoli verso l'accesso gratuito ai contenuti. Negli ultimi decenni il pubblico della pirateria è stato quasi sempre considerato di poco valore, di nicchia e irrilevante. Tuttavia, studi e sondaggi hanno trovato una correlazione tra la pirateria digitale e un aumento della spesa per contenuti legali. Molti pirati digitali, infatti, sono appassionati consumatori di media, i quali si rivolgono alla pirateria per accedere a contenuti non disponibili in quel momento nella propria area geografica, o comunque non accessibili al momento. Nonostante ciò, però, questi utenti quando ne hanno la possibilità spendono somme significative per contenuti legali[28].

La pirateria, infine, ha un peso rilevante anche per il settore dell'editoria. La pirateria editoriale, infatti, rappresenta un fenomeno complesso e diffuso che ha un impatto significativo sull'industria del libro. Secondo un rapporto presentato dall'Associazione Italiana Editori, alla popolazione italiana piace leggere libri, sia in formato cartaceo che in formato ebook, e ascoltare audiolibri per svago. Tuttavia la diffusione di piattaforme digitali e la facilità di accesso ai contenuti digitali ha contribuito all'aumento degli atti di pirateria. Il possesso di abbonamenti a piattaforme di ebook e audiolibri è in crescita, con Kindle Unlimited, Audible e altri servizi che stanno diventando pian piano sempre più popolari. Nonostante ciò, però è anche in aumento l'accesso illegale ai contenuti. La pirateria colpisce duramente il settore italiano e, infatti, solo nel 2023 ha causato perdite stimate di circa 423 milioni di euro.[29]

I testi universitari, spesso fotocopiati o scaricati illegalmente, hanno comportato perdite per circa 188 milioni di euro. Anche i libri e le banche dati professionali sono stati vittime di pirateria, con danni stimati di circa 94 milioni di euro. Complessivamente, il danno all'industria editoriale è quantificato in circa 705 milioni di euro, che rappresenta una perdita significativa rispetto ai 771 milioni di euro del 2021. Nonostante l'alta incidenza della pirateria, il livello di consapevolezza tra la popolazione riguardo alla gravità e alla legalità di questi atti è relativamente alto. L'84% delle persone è consapevole che la legislazione italiana considera questi comportamenti come illeciti. Tuttavia, solo

[28] **MUSO,** *The Publishing Piracy Report,* 2021 report disponibile su www.muso.com

[29] **CAPRIO G.,** *Il peso della pirateria nel mondo del libro*, 2024 https://www.pressenza.com/it/2024/03/il-peso-della-pirateria-nel-mondo-del-libro/

una minoranza ritiene che sia probabile che questi reati vengano scoperti e puniti. Questo evidenzia una discrepanza tra la consapevolezza del problema e la percezione della sua perseguibilità, che potrebbe influire negativamente sulla deterrenza della pirateria. Gli studenti universitari sono tra i maggiori fruitori di contenuti piratati. Circa il 78% degli studenti universitari ammette di aver compiuto almeno un atto di pirateria nell'ultimo anno. Le pratiche più comuni includono il download di articoli e libri di testo da internet, la ricezione di materiali digitali da compagni di corso, e la stampa di libri in formato elettronico. Questi comportamenti non solo causano perdite economiche significative per gli editori, ma minano anche il valore percepito dei materiali didattici. Anche i professionisti non sono immuni dal fenomeno della pirateria. Circa il 49% dei liberi professionisti ha compiuto atti di pirateria, con una prevalenza di accessi illegali a banche dati e libri professionali in formato digitale. Questo segmento della pirateria non solo danneggia gli editori, ma ha anche implicazioni legali e professionali per coloro che utilizzano materiali non autorizzati[30].

Le perdite economiche derivanti dalla pirateria non si limitano agli editori, ma si estendono all'intero sistema economico. Il rapporto stima che il danno complessivo al sistema paese, considerando fatturato, fisco e perdita occupazionale, ammonti a circa 1,75 miliardi di euro. Inoltre, si stima una perdita di circa 12.000 posti di lavoro, di cui 4.900 nel settore del libro. Questo impatto negativo sul mercato del lavoro evidenzia l'importanza di affrontare il problema della pirateria in modo efficace e sistematico. La pirateria nel mondo del libro rappresenta una sfida complessa che richiede un approccio multi-faccettato. È essenziale aumentare la consapevolezza riguardo alle conseguenze legali ed economiche della pirateria, migliorare la percezione della probabilità di perseguibilità e promuovere l'accesso legale ai contenuti digitali. Solo attraverso sforzi concertati tra editori, autorità legali e consumatori si potrà ridurre l'incidenza della pirateria e mitigare i suoi effetti dannosi sull'industria editoriale e sull'economia nel suo complesso[31].

3. CYBERCRIME E LE SUE IMPLICAZIONI NELLA PIRATERIA ONLINE

Il Cybercrime è la minaccia invisibile che sta cambiando il mondo. Quando si parla di Cyber crime o crimine informatico ci si riferisce generalmente a un’attività criminosa caratterizzata

[30] **AIE,** *La pirateria nel mondo del libro,* 2024 report disponibile su www.aie.it
[31] Ibidem

dall'abuso di componenti tecnologiche informatiche, sia hardware che software. I crimini legati alla Cybersecurity sono generalmente legati all'attacco alla sicurezza di figure come hacker o pirati informatici. Il quadro del Cybercrime però è ben più ampio e complesso. Esso, infatti, si riferisce all'azione di un individuo, chiamato cybercriminale, che compie attacchi informatici per motivi illeciti, come estorcere denaro o rubare informazioni cruciali per un'organizzazione, agendo da solo o in associazione con altri attraverso Internet. Il Cyber crime è una specifica forma di attacco informatico, ma non l'unica. C'è anche l'hacktivismo, praticato da chi utilizza la pirateria informatica per perseguire obiettivi sociali e politici. Il termine *hacktivism* nasce dalla fusione di *hacking* e *activism.*

Le minacce più significative spesso provengono da attori esterni all'azienda. Tuttavia, secondo la ricerca dell'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano, molte minacce informatiche hanno origine anche all'interno dell'azienda stessa. Tra i soggetti pericolosi per la sicurezza informatica ci sono anche persone che hanno rapporti stretti e continui con l'azienda, come i dipendenti attuali, collaboratori e consulenti. Questo perché, nel compiere i loro crimini, gli hacker sfruttano non solo le vulnerabilità dei sistemi informatici, ma anche le debolezze e le disattenzioni dei dipendenti. Questo tipo di Cyber crime è legato al fattore umano. Tra i principali pericoli della Cybersecurity troviamo diversi tipi di Cyber crime, i quali rappresentano una minaccia significativa per individui, aziende e istituzioni governative. Vi sono diverse categorie di Cybercrime, tra cui infezioni di malware, attacchi ransomware, attacchi di phishing e Social Engineering, Spamming, Attacchi DoS/DDoS, APT e Zero-Day[32].

Il termine malware identifica applicazioni dannose finalizzate ad arrecare danno informatico alla vittima. Queste applicazioni tentano di accedere segretamente a un particolare dispositivo senza che l'utente ne sia a conoscenza per raccogliere informazioni, creare malfunzionamenti o criptare i dati. Il malware può assumere diverse forme, tra cui virus, worm, trojan, spyware e adware[33], ciascuno con specifiche modalità di infezione e obiettivi. Il virus informatico è un tipo di malware che, quando eseguito, si attacca ad altri programmi o file, incorporando il proprio codice per diffondersi da un programma all'altro, causando infezioni durante il transito. Analogamente ai virus biologici, i virus informatici possono variare in gravità: alcuni provocano lievi fastidi, mentre altri possono causare

[32] **OSSERVATORIO CYBERSECURITY E DATA PROTECTION POLITECNICO DI MILANO,** *Cybersecurity, data protection e gestione del rischio cyber: i principali trend.* Video dell'evento e atti disponibili su www.osservatori.net

[33] **ANTONIELLI A.,** *Cyber Crime: cos'è, come affrontarlo e difendersi in azienda*, Politecnico di Milano, 2024 https://blog.osservatori.net/it_it/cybercrime-definizione-italia

danni significativi all'hardware, al software o ai file. La maggior parte dei virus informatici è associata a file eseguibili, il che significa che il virus può essere presente sul tuo computer senza infettarlo finché non si clicca, esegue o apre il programma dannoso. È importante notare che un virus non può diffondersi senza un intervento umano e l'uso di tecniche di ingegneria sociale, come cliccare su un link nocivo o eseguire un programma infetto. Le persone, spesso inconsapevolmente, continuano a diffondere virus informatici condividendo file infetti o inviando email con allegati contenti virus. Altra tipologia di malware che si replica autonomamente e si diffonde attraverso le reti sfruttando le vulnerabilità dei sistemi è il worm. A differenza dei virus, i worm non necessitano di attaccarsi a file eseguibili per propagarsi. Una volta infettato un sistema, un worm può continuare a diffondersi ad altri sistemi senza alcun intervento umano, causando un rapido aumento del traffico di rete e rallentamenti significativi. Un Trojan, o Cavallo di Troia, invece, è un tipo di malware che si presenta come un software legittimo o utile per ingannare gli utenti a installarlo. Una volta installato, il trojan esegue azioni dannose nascoste, come rubare informazioni sensibili, creare backdoor per l'accesso non autorizzato o scaricare altri tipi di malware. I trojan non si replicano autonomamente, ma spesso sono distribuiti attraverso download ingannevoli, e-mail di phishing o siti web compromessi. Lo spyware è un'altra tipologia di malware progettato per raccogliere informazioni sull'utente senza il suo consenso. Può monitorare le attività online, raccogliere dati sensibili come password e numeri di carte di credito, e trasmettere queste informazioni a terzi. Lo spyware può essere installato attraverso download infetti, allegati e-mail o vulnerabilità del browser. Oltre a violare la privacy, lo spyware può rallentare le prestazioni del sistema e causare instabilità. L'adware è un tipo di software che visualizza annunci pubblicitari indesiderati sul dispositivo infetto. Sebbene non sia necessariamente dannoso, l'adware può diventare invasivo e compromettere l'esperienza dell'utente. Alcuni tipi di adware possono anche raccogliere dati sull'utente per personalizzare gli annunci visualizzati. L'adware è spesso distribuito insieme a software gratuiti o shareware come parte di un pacchetto di installazione. Comprendere le diverse tipologie di malware è essenziale per implementare misure di sicurezza efficaci e proteggere i sistemi informatici da queste minacce. Utilizzare software antivirus aggiornato, mantenere i sistemi operativi e le applicazioni aggiornate, e praticare una navigazione sicura sono tutti passi importanti per ridurre il rischio di infezioni da malware[34].

[34] **ANTONIELLI A.,** *Cyber Crime: cos'è, come affrontarlo e difendersi in azienda*, Politecnico di Milano, 2024 https://blog.osservatori.net/it_it/cybercrime-definizione-italia

Il ransomware, invece, è un tipo particolare di malware che, dopo aver limitato o impedito del tutto l'accesso al sistema infettato, ad esempio criptando i file presenti su un dispositivo, richiede una somma di denaro per la sua rimozione. Questo tipo di attacco offre un importante vantaggio ai cybercriminali, poiché le vittime sono spesso inclini a pagare il riscatto per rientrare in possesso dei propri dati e dispositivi, comportando una perdita monetaria relativamente contenuta rispetto ai danni potenziali di una completa perdita di dati. Il phishing e il social engineering sono pratiche molto diffuse nel cyber crime. Il phishing si riferisce ai tentativi di frode informatica volti a carpire i dati sensibili degli utenti tramite l'invio di e-mail ingannevoli che simulano comunicazioni di entità affidabili. Gli attacchi di phishing spesso invitano la vittima a fornire informazioni riservate come password, codici di accesso o dati della carta di credito. Il social engineering, invece, è una tecnica di manipolazione psicologica mirata a ottenere informazioni confidenziali tramite l'inganno e la persuasione. Un'altra categoria di Cybercrime è lo spamming, il quale è definito come l'invio massiccio e indiscriminato di messaggi di posta elettronica senza il consenso del destinatario, solitamente con contenuto pubblicitario. Anche se spesso considerato un fastidio minore, lo spam può diventare pericoloso se utilizzato per diffondere malware o phishing. Vi sono anche gli attacchi DoS (Denial of Service) e DDoS (Distributed Denial of Service). Essi mirano a interrompere la continuità di servizio rendendo inaccessibili i servizi presi di mira. Questi attacchi vengono eseguiti generando un numero eccessivo di richieste al server o un volume di traffico maggiore rispetto alla banda disponibile, sturando le risorse a disposizione. Gli attacchi DDoS sono particolarmente devastanti poiché sfruttano una rete di dispositivi infetti, conosciuta come botnet, per coordinare l'attacco. Atra tipologia sono gli APT – Advanced Persistent Threat. Si tratta di attacchi informatici particolarmente sofisticati e mirati a sottrarre dati sensibili, sabotare sistemi critici o eseguire attività di spionaggio informatico. Questi attacchi sono caratterizzati dalla loro persistenza e capacità di rimanere inosservati per lunghi periodi, compromettendo la sicurezza delle vittime in modo subdolo e continuo. Infine, vi sono gli attacchi Zero-day i quali sfruttano la vulnerabilità nei software o nei sistemi informatici che non sono ancora state scoperte o risolte. Queste vulnerabilità, essendo sconosciute agli sviluppatori del software, offrono agli hacker un'opportunità unica di infiltrarsi nei sistemi senza essere rilevati. Gli attacchi Zero-day sono particolarmente pericolosi perché non esistono contromisure disponibili per contrastarli[35].

[35] **OSSERVATORIO CYBERSECURITY & DATA PROTECTION**, *Cos'è la cybersecurity e perché è importante in azienda,* Politecnico di Milano. Articolo disponibile su https://blog.osservatori.net/it_it/cose-cyber-security-significato-principi-tecnologie

I Cybercrime non solo rappresentano un danno economico diretto ma comportano anche conseguenze indirette significative, come la perdita di fiducia dei clienti, danni alla reputazione e costi elevati per il ripristino dei sistemi compromessi. Per le aziende e le istituzioni governative, gli attacchi informatici possono minacciare la sicurezza nazionale, compromettendo infrastrutture critiche e rubando informazioni sensibili. Per contrastare queste minacce, è essenziale adottare misure di sicurezza informatica avanzate tra cui aggiornamenti regolari del software, formazione del personale sulla sicurezza informatica, implementazione di sistemi di rilevamento delle intrusioni e backup regolare dei dati. Solo attraverso una strategia di sicurezza proattiva e integrata è possibile mitigare efficacemente i rischi associati ai cyber crime. Oggi siamo tutti quanti esposti alle minacce del Cyber Crime per diversi motivi, tra cui per esempio, la diffusione della digitalizzazione, l'interconnessione globale, l'aumento dei dati online e le carenze nella sicurezza. L'uso crescente delle tecnologie digitali per le attività quotidiane, il lavoro e le comunicazioni aumenta inevitabilmente l'esposizione al cyber crime. Ogni aspetto della nostra vita quotidiana è ormai interconnesso con il mondo digitale, dagli acquisti online alla gestione delle finanze, dall'uso dei social media alla domotica. Questa pervasività offre numerosi vantaggi, ma amplifica anche le possibilità di attacco per i criminali informatici. Internet, inoltre, collega dispositivi a livello mondiale, creando numerosi punti di accesso per i cybercriminali. Ogni dispositivo connesso, che sia un computer, uno smartphone, una smart Tv o un sistema di controllo industriale, rappresenta una potenziale porta d'ingresso per gli attaccanti. La globalizzazione delle reti e la dipendenza dalle infrastrutture digitali internazionali aumentano ulteriormente i rischi, che possono provenire da qualsiasi parte del mondo.

Le nuove tecnologie, come l'Intelligenza Artificiale, stanno rendendo il cybercrime e gli attacchi informatici sempre più personali, veloci ed efficaci. Gli hacker utilizzano l'AI per automatizzare e potenziare i loro attacchi, rendendoli più difficili da rilevare e contrastare. Ad esempio, l'AI permette ai cybercriminali di creare malware sofisticati e di condurre attacchi di phishing altamente mirati, sfruttando le vulnerabilità umane e tecnologiche. L'aumento costante dei dati online, sia personali che aziendali, li rende preziosi obiettivi per i cybercriminali. Le informazioni personali, come dati bancari, numeri di previdenza sociale e dettagli sanitari, sono estremamente appetibili. Allo stesso tempo, le aziende accumulano enormi quantità di dati sui loro clienti, dipendenti e operazioni. Se compromessi, questi dati possono causare gravi danni economici e reputazionali. In aggiunta a ciò, molte organizzazioni e individui non adottano adeguate misure di sicurezza, nonostante la crescente consapevolezza dei rischi. Spesso mancano investimenti sufficienti

in tecnologie di sicurezza avanzate e in formazione del personale. Password deboli, assenza di aggiornamenti regolari dei software e mancanza di piani di risposta agli incidenti sono solo alcune delle lacune comuni che i cybercriminali possono sfruttare.

L'era digitale offre enormi opportunità, ma comporta anche significativi rischi in termini di sicurezza informatica. È fondamentale che tutti, dai singoli individui alle grandi organizzazioni, adottino un approccio proattivo alla Cyber Security. Questo include l'implementazione di misure di protezione robuste e il mantenimento costante dell'aggiornamento sulle nuove minacce e tecnologie di difesa. La pirateria online è una forma significativa di cybercrime, la quale comporta gravi implicazioni tecnologiche, economiche, legali e sociopsicologiche. Questa partica causa notevoli perdite economiche per le industrie creative, inclusi i settori dell'editoria, della musica, del cinema e del software. Ad esempio, la pirateria di e-book può costare agli editori statunitensi fino a 315 milioni di dollari all'anno, mentre gli autori possono perdere circa 300 milioni di dollari annualmente. Anche nell'UE, le perdite stimate per la pirateria di e-book ammontano a circa 376 milioni di dollari all'anno[36]. Le tecniche di pirateria variano, ma comunemente includono la rimozione della gestione dei diritti digitali (DRM) dai contenuti acquistati legalmente, che poi vengono distribuiti illegalmente attraverso vari canali online. I pirati possono anche scansionare fisicamente i libri per creare versioni digitali, che vengono poi condivise su piattaforme di file hosting o vendute tramite marketplace online. La pirateria di software, film e musica è altrettanto prevalente. I pirati spesso utilizzano piattaforme di file sharing e Torrent per distribuire copie non autorizzate di software costosi e contenuti multimediali, privando i creatori e le aziende dei loro diritti di proprietà intellettuale e dei relativi ricavi. Le campagne anti-pirateria mirano a contrastare queste pratiche, ma possono avere effetti controproducenti, specialmente tra determinati gruppi demografici. Ad esempio, i messaggi di avvertimento possono aumentare la propensione alla pirateria tra gli uomini a causa di una reazione piscologica nota come reattanza[37].

Le aziende colpite dalla pirateria, inoltre, possono subire danni reputazionali significativi. La diffusione di prodotti contraffatti e non autorizzati può influire negativamente sulla percezione del marchio e sulla fiducia dei consumatori. Si prevedono anche delle implicazioni legali quali violazioni del copyright. Di fatti, la pirateria online costituisce una violazione diretta delle leggi sul copyright.

[36] **MANDAL S.**, *How an e-book is pirated, its implications for the stakeholders, and the extent of the problem,* 2023 https://goodereader.com/blog/e-book-news/how-an-e-book-is-pirated-its-implications-for-the-stakeholders-and-the-extent-of-the-problem

[37] **WHITMAN K. et al**, *Psychological reactance to anti-piracy Messages explained by gender and attitudes,* Journal of Business Ethics, 2024 DOI: 10.1007/s10551-023-05597-5

Le sanzioni per la distribuzione e l'uso di contenuti piratati possono essere severe e possono prevedere multe elevate e pene detentive. Le autorità perseguono attivamente i responsabili, collaborando a livello internazionale per contrastare il fenomeno. Possono anche essere effettuate delle azioni legali contro le piattaforme che ospitano contenuti piratati, come i siti di file sharing e i marketplace online. Gli operatori di queste piattaforme rischiano, inoltre, incriminazioni e sanzioni legali.

La pirateria online comporta anche implicazioni sociali e psicologiche, legate soprattutto ai comportamenti degli utenti. Le campagne anti-pirateria possono avere effetti contrastanti. Studi hanno dimostrato che i messaggi di avvertimento possono in alcuni casi aumentare la propensione alla pirateria, specialmente tra gli uomini. Questo fenomeno indica la necessità di strategie di comunicazione più efficaci e mirate. Infine, vi sono delle implicazioni tecnologiche. I pirati informatici utilizzano tecnologie avanzate per eludere le protezioni e diffondere contenuti illegali. La rimozione della gestione dei diritti digitali e l'uso di piattaforme decentralizzate rendono difficile il controllo e l'intervento da parte delle autorità. Per combattere la pirateria, le aziende investono in tecnologie di DRM, sistemi di rilevamento delle violazioni e collaborazioni con le forze dell'ordine. Questi strumenti sono essenziali per proteggere i contenuti digitali e ridurre le perdite economiche.

Oggigiorno gli hacker sono numerosi e distribuiti in tutto il mondo. Agenzie governative e private come l'FBI, la CIA e la polizia statale lavorano per individuarli. In ogni caso, però, è essenziale proteggere i dati personali dalle frodi online. È cruciale informare le persone meno istruite riguardo l'uso di carte di debito o di credito, internet e computer. La cattura degli hacker è complicata poiché operano da un paese attaccando computer in un altro, rendendo la vigilanza la miglior difesa. Internet è fondamentale per la sicurezza nazionale. Sebbene il progresso nella risoluzione dei problemi sia lento, è essenziale prevenire l'uso criminale della rete. Il governo, le ONG e le aziende produttrici di software devono collaborare per promuovere la sicurezza digitale e l'alfabetizzazione informatica. È imperativo iniziare dalla base, educando negli istituti, nei centri informatici e nelle scuole. I crimini basati sulla tecnologia richiedono una risposta urgente e il rispetto delle leggi è fondamentale per prevenire abusi. Ognuno ha il diritto di vivere in un ambiente sicuro, sia nella vita reale che online, dato l'impatto su milioni di utenti.

4. DIMENSIONE ECONOMICA DEL FENOMENO

La contraffazione e la pirateria rappresentano attività illegali che favoriscono le organizzazioni criminali. Queste pratiche producono e distribuiscono articoli spesso di qualità scadente e potenzialmente pericolosi, i quali creano rischi per la salute e la sicurezza che vanno dal lieve al grave. Questi fenomeni minacciano anche l'innovazione, fondamentale per la crescita economica complessiva. Date la portata e le conseguenze della contraffazione e della pirateria, è essenziale un'imponente e continua azione da parte dei governi, delle imprese e dei consumatori. È cruciale intensificare le misure repressive e ottenere un forte sostegno dell'opinione pubblica. Maggiore cooperazione tra governi e settore privato, insieme a una migliore raccolta dei dati, potrebbe rivelarsi particolarmente utile in questo contesto. Il mercato dei prodotti contraffatti e piratati può essere suddiviso in due segmenti cruciali. Nel mercato primario, i consumatori acquistano inconsapevolmente prodotti contraffatti e pirata, credendo di acquistare articoli autentici. I rischi associati all'uso di tali prodotti possono variare da leggeri a gravi danni alla salute dei consumatori. Nel mercato secondario, invece, i consumatori sono consapevoli di star acquistando prodotti contraffatti e pirata, spinti spesso dalla ricerca di affari vantaggiosi. Le politiche e le misure per contrastare la contraffazione e la pirateria differiscono nei due mercati, pertanto è cruciale valutare l'entità delle minacce poste da ciascuno di essi quando si formulano strategie relative e specifici prodotti.

La contraffazione e la pirateria presentano effetti socio-economici diffusi, influenzando diversi aspetti, quali il commercio, gli investimenti diretti dall'estero, innovazione e crescita, occupazione, ambiente e attività criminale[38]. Le pratiche di contraffazione e pirateria possono distorcere il commercio legittimo, compromettendo la competitività delle aziende che rispettano le normative. I regimi deboli di protezione della proprietà intellettuale possono scoraggiare gli investimenti stranieri diretti, poiché le imprese potrebbero essere riluttanti a investire in paesi con alti livelli di contraffazione e pirateria.

La contraffazione e la pirateria possono minare gli incentivi per l'innovazione, poiché riducono i ricavi che le imprese potrebbero reinvestire in ricerca e sviluppo. Sebbene possano creare

[38] **AGENZIA DELLE DOGANE**, *L'impatto economico della contraffazione e della pirateria,* 2010 https://www.adm.gov.it/portale/documents/20182/901640/2010-06-OCSE-IMPATTO_ECONOMICO_CONTRAFFAZIONE.pdf/9d74ef5e-7802-4dda-9e2b-0607036bce58

occupazione nel settore della contraffazione, spesso a costo di lavoro non regolamentato e sfruttato, queste attività possono anche danneggiare i settori legittimi che offrono occupazione formale. La produzione e il commercio di prodotti contraffatti possono avere impatti ambientali negativi a causa di pratiche di produzione non regolamentate e di materia di bassa qualità. Infine, la contraffazione e la pirateria possono alimentare altre forme di criminalità, come il riciclaggio di denaro e il finanziamento di organizzazioni illegali. I settori cinematografici, musicale e dei software sono quelli più colpiti dalla pirateria digitale. Si stima, infatti, che il valore commerciale della pirateria online nel settore cinematografico ammonti a 160 miliardi di dollari, solo nel 2015[39].

La maggior parte dei ricercatori ritiene che la pirateria cinematografica sostituisca le vendite legali di film e che, quindi, vada a danneggiare l'industria cinematografica. L'introduzione di BitTorrent tra il 2003 e il 2004 ha coinciso con un punto di svolta nello sviluppo dei ricavi dell'industria cinematografica. I ricavi delle vendite e dei noleggi di film pre-registrati negli Stati Uniti sono diminuiti di oltre il 20% tra il 2005 e il 2010, dopo essere aumentati costantemente fino a quel momento. I ricavi del botteghino sono rimasti relativamente costanti nello stesso periodo, sebbene un aumento graduale del 47% nel decennio precedente al 2002 avrebbe potuto suggerire che il trend di crescita sarebbe continuato. Sembra quindi plausibile attribuire a BitTorrent la responsabilità di questi sviluppi negativi. Tuttavia, è probabile che altri sviluppi nel mercato, tra cui l'emergere di piattaforme di streaming come Netflix, abbiano anche giocato un ruolo nel declino di altre modalità di consumo dei film. Nel 2011 uno studio ha stimato l'impatto della pirateria cinematografica sull'economia australiana, basandosi su un sondaggio condotto su 3.500 adulti. Lo studio ha rilevato che alcune persone piratano film, ma guardano successivamente versioni autorizzate e che solo il 45% dei pirati afferma che avrebbe pagato per guardare versioni autorizzate se non avessero avuto accesso a una versione pirata. Lo studio ha concluso che l'industria cinematografica australiana ha subito almeno 575 milioni di dollari australiani di perdite dirette nella spesa dei consumatori nei 12 mesi fino al terzo trimestre del 2010. Aggiungendo gli impatti indiretti o indotti su altre industrie, è emerso che la pirateria cinematografica ha causato perdite all'intera economia australiana di almeno 1,3 miliardi di dollari in produzione lorda, e quindi, di vendite e 6.100 posti di lavoro equivalenti a tempo pieno. In poche parole, si è consapevoli che la pirateria online danneggi l'industria cinematografica. Ne emergono due domande: quanto grande è il danno? Quanto

[39] **FRONTIER ECONOMICS**, *The Economic Impacts of Counterfeiting and Piracy – Report prepared for BASCAP and INTA,* 2017 https://iccwbo.org/wp-content/uploads/sites/3/2017/02/ICC-BASCAP-Frontier-report-2016.pdf

è diffusa la pirateria cinematografica? Uno studio recente di NetNames[40] ha posto lo stesso focus. Lo studio rileva che nel 2012, l'uso di banda per attività illecite in Nord America, Europa e Asia ha rappresentato il 23,8% del totale della banda consumata. L'enorme portata della pirateria è illustrata dal fatto che solo nel gennaio 2013, 432 milioni di utenti Internet hanno cercato materiale illecito.

La rete P2P è il metodo più popolare per l'acquisizione illecita di film e BitTorrent è di gran lunga la più grande rete P2P. tuttavia, ci sono altri modi per scaricare illegalmente film, tra cui lo streaming e l'utilizzo di Cyberlocker. Lo studio NetNames sopra citato suggerisce che il 39% delle attività di pirateria avviene su BitTorrent. Tramite questo dato si può stimare che solo nel 2015 ci sono stati 47.8 miliardi di download illegali di film. Per quanto riguarda il settore discografico, si stima che il valore commerciale complessivo della pirateria online in questo settore, nel 2015, è stato di 29 miliardi di dollari. Negli ultimi anni ci sono stati diversi cambiamenti: per la prima volta nella storia, i ricavi digitali hanno superato quelli fisici e ha avuto atto una rapida espansione delle piattaforme di streaming come Spotify, Rdio e Pandora. Ad esempio, i Nielsen Year End Music Reports del 2014 e del 2015 hanno mostrato che lo streaming musicale on-demand è triplicato tra il 2013 e il 2015, raggiungendo i 317,2 miliardi. In confronto, i download digitali permanenti hanno totalizzato un miliardo di singoli e 0,1 miliardi di album, mentre le unità fisiche al dettaglio sono stato solo 0,1 miliardi nel 2015. La quota dei ricavi totali della musica negli Stati Uniti proveniente dallo streaming è aumentata dal 9% nel 2011 al 34% nel 2015, Da un lato, lo streaming cannibalizza le vendite di musica poiché la disponibilità permanente di una vasta collezione musicale rende quasi superfluo l'acquisto di singoli brani o album. La diminuzione del 23% dei download digitali permanenti e delle unità fisiche spedite negli Stati Uniti tra il 2013 d il 2015 fornisce prove empiriche di questa ipotesi. D'altra parte, lo streaming sembra erodere la pirateria musicale perché soddisfa la domanda dei consumatori di accesso economico, o addirittura gratuito, e conveniente alla musica. La diminuzione dei download illegali di musica tramite condivisione di file P2P da 3,2 miliardi nel 2013 a 2,5 miliardi nel 2015 sembra supportare questo argomento. Ulteriori prove sono fornite da un recente studio dell'American Assembly che riporta che il 48% delle persone coinvolte sia nello streaming che nella pirateria negli Stati Uniti afferma di piratare meno musica grazie alla crescita dei servizi di streaming. In Germania, la percentuale è del 52%[41].

[40] **PRICE D.,** *Sizing the piracy universe,* NetNames, 2013 https://creativefuture.org/wp-content/uploads/2016/01/netnames-sizing_piracy_universe-FULLreport-sept2013.pdf

[41] **KARAGANIS J. e RENKEMA L.,** *Copy culture in the US and Germany,* The American Assembly, 2013 https://www.researchgate.net/publication/263565520_Copy_Culture_in_the_US_and_Germany

Alcuni sperano che lo streaming possa commercializzare il volume di musica che attualmente viene piratato. Ciò si traduce in quello che la International Federation of the Phonographic Industry (IFPI) chiama il "gap di valore" e che i gruppi del settore musicale dicono debba essere risolto affinché l'industria musicale possa sperimentare una crescita sostenuta in futuro[42]. Ciò che è particolarmente rilevante riguardo lo streaming è che cambia rapidamente il modo in cui le persone accedono o ascoltano la musica, con conseguenti difficoltà per i ricercatori nel monitorare i modelli di consumo legale della musica e il comportamento della pirateria. La crescita della pirateria musicale sembra rallentare nonostante la portata complessiva della pirateria rimanga ampia. Inoltre, la direzione e l'entità del legame tra pirateria musicale e vendite legali sono ancora più dibattute rispetto a quelle per i film. Recenti studi mostrano che la maggioranza della letterature ritiene che la pirateria su Internet danneggi le vendite dei media. Liebowitz (2013) conferma questo risultato per gli studi che si concentrano specificamente sulla musica. La conclusione della sua analisi è notevole: "In media, i risultati per la musica indicano che l'intero calo delle vendite dal 1999 è dovuto alla pirateria, e questi valori tendono a situarsi intorno al 50%-70% quando i dollari sono misurati in unità adeguate all'inflazione." In contrasto, il Joint Research Centre della Commissione Europea trova che l'impatto della pirateria sulle vendite sia piccolo e positivo. Utilizzando dati clickstream, trovano che un aumento del 10% dei clic su siti di download illegale causa un aumento dello 0,2% dei clic su siti di acquisto legale. Ciò suggerisce che i consumatori non considerano la musica piratata come un sostituto per gli acquisti legali. Analogamente, è stato riscontrato che i pirati sono grandi consumatori di musica legale[43].

Uno studio leggermente più datato di Oxera fornisce una possibile, ma parziale spiegazione per i risultati nel paragrafo precedente elencando "Ascolta prima di comprare" come uno dei quattro principali motivi economici della pirateria musicale. In questo caso, è possibile che la pirateria aumenti le vendite legali perché alcune persone potrebbero voler essere sicure di apprezzare una specifica canzone o album prima di acquistarlo. Tuttavia, l'elenco completo dei motivi per la pirateria comprende la riluttanza a pagare, ascolta prima di comprare, non voler un intero album e non disponibile per l'acquisto[44].

---

[42] **IFPI**, *Global Music Report,* 2016 https://ifpicr.cz/ifpi-global-music-report-2016

[43] **AGULAR L. e MARTENS B.,** *Digital Music Consumption on the Internet: Evidence from Clickstream Data*, JRC Technical Reports, Institute for Prospective Technological Studies Digital Economy Working Paper 2013/04, Joint Research Centre, European Commission, 2013 http://www.consumatoridirittimercato.it/wp-content/uploads/2013/03/Digital-Music-Consumption-on-the-Internet.pdf

[44] **OXERA,** *Competing with 'free'? The damages of music piracy,* 2011 https://www.oxera.com/insights/agenda/articles/competing-with-free-the-damages-of-music-piracy/

A maggio 2016, l'EUIPO ha pubblicato un rapporto sul costo della pirateria musicale in Europa. Applicando diversi modelli di previsione ai dati sulle vendite di musica registrata dell'IFPI per 19 paesi europei nel periodo 2005-2014, hanno considerato le differenze tra le vendite previste e quelle effettive come perdite e hanno cercato di spiegare queste perdite con variabili esplicative tra cui la crescita del PIL, il PIL pro capite e la volontà di piratare musica. Con questo metodo, hanno trovato che nel 2014, la pirateria musicale ha causato una perdita del 5,2% dei ricavi, pari a 170 milioni di euro, per l'industria della musica registrata in Europa. Ha anche avuto effetti su altre industrie, inclusi 336 milioni di euro di perdite di vendite per l'economia dell'UE e, infine, ha causato la perdita di 2.155 posti di lavoro e 63 milioni di euro di entrate governative[45]. Si stima, infine, che il valore commerciale complessivo della pirateria online, nel 2015, nel settore dei software sia di 24 miliardi di dollari.

Nel 2015 i consumatori hanno speso 444 miliardi di dollari in software in tutto il mondo. Sembra esserci un simile spostamento dal fisico al digitale. Per esempio, mentre le vendite di software fisico negli Stati Unito sono diminuite del 13% tra il 2014 e il 2015, le vendite globali di videogiochi digitali sono cresciute dell'8%. La pirateria del software è aumentata nell'ultimo decennio. Secondo la Business Software Alliance (BSA, il valore commerciale del software non autorizzato installato sui computer a livello mondiale è passato da 40 miliardi di dollari nel 2006 a 52 miliardi di dollari nel 2015, con un picco di 63 miliardi di dollari nel periodo 2011-2013. Il tasso di installazione di software non autorizzato nel 2015 era del 39%. Ulteriori prove della prevalenza della pirateria del software provengono dalla versione del 2013 del Tracker sull'Infrazione del Diritto d'Autore Online di Kantar Media, preparato per l'Ufficio delle Comunicazioni del Regno Unito (Ofcom). Secondo lo studio, il 20% degli utenti internet nel Regno Unito di età pari o superiore ai 12 anni afferma di aver utilizzato software piratato almeno una volta nella vita. Il 12% ha ammesso di averlo fatto negli ultimi tre mesi. Interessante è il fatto che il 39% degli utenti che avevano pagato per qualsiasi software per computer negli ultimi tre mesi ha dichiarato di aver precedentemente avuto accesso a parte di esso gratuitamente. Il 22% ha persino affermato di aver avuto accesso a tutti i prodotti gratuitamente prima di acquistarli. Sembra essere un analogo del motivo "Ascolta prima di comprare" nella pirateria musicale. Ciò significa che per alcuni utenti il software piratato non è un sostituto del software autorizzato.

[45] **EUIPO**, *The Economic Cost of IPR Infringement in the Recorded Music Industry, 2016* https://euipo.europa.eu/tunnelweb/secure/webdav/guest/document_library/observatory/resources/research-and-studies/ip_infringement/study7/Music_industry_en.pdf

Tuttavia, come nel settore dei film e della musica, è probabile che per molti utenti il software piratato costituisca un sostituto del software autorizzato e quindi danneggi l'industria del software spostando le vendite legali. Infatti, nel 2010 BSA ha stimato che ridurre il tasso pirateria del software per PC di 10 punti percentuali in quattro anni creerebbe 142 miliardi di dollari in nuova attività economica. Più dell'80% di queste attività sarebbe beneficio diretto per l'industria del software. Inoltre, BSA ha scoperto che se la pirateria diminuisse a un ritmo più veloce, i guadagni economici sarebbero notevolmente più alti. Oltre a danneggiare l'offerta causando perdite commerciali dovute allo spostamento delle vendite, il software piratato o contraffatto ha anche sostanziali conseguenze negative sul lato della domanda. Quando si pirata il software, e soprattutto quando lo si scarica da Internet, gli utenti corrono un alto rischio di contrarre malware come virus, Trojan o keylogger. Secondo IDC la possibilità di incontrare malware quando si utilizza software contraffatto è di 1/3. Nel marzo 2013, IDC ha stimato che durante l'anno i consumatori avrebbero sprecato 1,5 miliardi di ore a causa del malware proveniente dal software contraffatto; i costi diretti per le imprese ammonterebbero a 114 miliardi di dollari[46].

Il BSA Global Software Survey regolarmente pubblicato quantifica il valore del software non licenziato installato sui PC in tutto il mondo in un dato anno. I principali input dell'edizione 2016 del rapporto sono un sondaggio globale condotto da IDC su oltre 20.000 utenti di computer e un sondaggio di 2.200 responsabili IT in 22 paesi. I sondaggi sono utilizzati per determinare il volume e il tipo di software installato su computer domestici e aziendali e le opinioni degli utenti PC verso la proprietà intellettuale e l'acquisizione illecita di software. Sulla base di questi dati, la BSA trova un tasso totale mondiale di installazioni di software pirata del 39%, corrispondente a un valore di 52 miliardi di dollari. Questo numero comprende una vasta gamma di software: dai sistemi operativi, pacchetti di sicurezza e applicazioni aziendali a software consumer come finanza personale. Inoltre, non cerca di distinguere tra i diversi modi in cui tale software è stato acquisito, il che significa che la sua copertura è più ampia del valore della pirateria digitale, che è l'obiettivo specifico di questo capitolo. Per trasformare la stima BSA della pirateria totale del software in un valore di pirateria digitale del software, ci basiamo su informazioni da un sondaggio IDC del 2013: basandoci sulle classificazioni delle fonti principali di software piratato fornite dai rispondenti, IDC stima che il 45% del software piratato provenga da fonti online come reti P2P o sistemi di condivisione file DDL.

[46] **IDC,** *The Dangerous World of Counterfeit and Pirated Software*, White Paper, 2013 https://news.microsoft.com/download/presskits/antipiracy/docs/IDC030513.pdf

Applicando questo numero per ridimensionare la cifra BSA, stimiamo che il valore della pirateria digitale nel software sia di 24 miliardi di dollari[47].

II. IL CONTRASTO ALLA PIRATERIA ONLINE: STRUMENTI TECNOLOGICI

1. LA TECNOLOGIA DRM: ASPETTI ECONOMICI, POLITICI E TECNOLOGICI

Nel corso degli anni è diventato sempre più semplice scaricare contenuti dal web senza dover pagare un singolo centesimo. L'industria dei contenuti digitali, infatti, a causa di questa pratica illegale, reclama la perdita di miliardi di euro all'anno. Teme, inoltre, che la creatività e l'innovazione possano subire un notevole declino e di conseguenza si vedano diminuite le ricompense finanziarie. Una soluzione possibile a questa problematica potrebbe essere la gestione dei diritti digitali. La gestione dei diritti digitali (DRM), in inglese Digital Rights Management, è un sistema progettato per proteggere i diritti di proprietà intellettuale nel contesto digitale. Utilizzando tecnologie avanzate, i sistemi DRM implementano misure volte a controllare e gestire l'accesso a contenuti digitali protetti da copyright. L'obiettivo principale dei sistemi DRM è impedire la distribuzione non autorizzata dei materiali digitali e limitare le modalità con cui i consumatori possono copiare i contenuti acquistati. Questo viene realizzato inserendo codici specifici all'intendo dei file digitali, che ne impediscono la duplicazione e determinano la durata dell'accesso ai contenuti. Inoltre, i sistemi DRM limitano il numero di dispositivi su cui è possibile riprodurre i media protetti. La questione DRM ha assunto rilevanza con la crescita di Internet negli anni 90, periodo in cui la pirateria ha compromesso le vendite di CD e i video online sono diventati popolari. Ha raggiunto, poi, il suo apice nei primi anni 2000, quando vari paesi hanno tentato di rispondere alla problematica con leggi e regolamenti specifici, per poi dissiparsi negli anni 2010, quando i social media e i servizi di streaming hanno

[47] **BSA**, *Seizing Opportunity Through License Compliance*, Global Software Survey, 2016 https://www.bsa.org/files/reports/BSA_GSS_US.pdf

sostituito in gran parte la pirateria e i fornitori di contenuti hanno elaborato modelli di business di nuova generazione[48].

Nel 1983, Ryuichi Moriya, un ingegnere giapponese, ideò il primo esempio di tecnologia DRM: il Software Service System (SSS). Poco tempo dopo, questa tecnologia verrà perfezionata con il nome di *superdistribution.* L'SSS si basava sulla crittografia e prevedeva l'utilizzo di un hardware specifico in grado di controllare la decrittazione e consentire l'invio di pagamenti al detentore del copyright. Il principio fondamentale era che la distribuzione fisica dei prodotti digitali crittografati doveva essere completamente libera, incoraggiando gli utenti a condividere tali prodotti[49].

Uno dei primi sistemi DRM è il Content Scramble System (CSS). Il CSS utilizzava un algoritmo di crittografia per proteggere i contenuti sul disco DVD. I produttori di lettori DVD dovevano ottenere una licenza per questa tecnologia e implementarla nei loro dispositivi per poter decrittare i contenuti. Il contratto di licenza CSS include restrizioni su come i contenuti del DVD possono essere riprodotti, inclusi quali output sono consentiti e come tali output possono essere resi disponibili, mantenendo intatta la crittografia mentre i contenuti vengono visualizzati[50]. Nel maggio 1998 viene approvato il Digital Millenium Copyright Act (DMCA). IL DMCA è una legge statunitense che implementa due trattati sull'Organizzazione Mondiale della Proprietà Intellettuale (WIPO) del 1996: il Trattato sul diritto d'autore e il Trattato sulle interpretazione ed esecuzioni e sui fonogrammi. La legge si suddivide in cinque titoli principali, ognuno dei quali tratta diversi aspetti legati al diritto d'autore in ambito digitale[51].

Il DMCA, firmato dal presidente Clinton nel 1998, ha l'obiettivo di aggiornare la normativa sul diritto d'autore alla luce delle nuove tecnologie digitali e di internet. Il Titolo I adatta la normativa statunitense ai requisiti dei trattati WIPO, includendo due nuove proibizioni nel Titolo 17 del Codice degli Stati Uniti: una sullo scavalcamento delle misure tecnologiche di protezione delle opere e una sulla manipolazione delle informazioni di gestione del diritto d'autore. Sono previste, poi, sanzioni civili e penali per le violazioni di queste proibizioni. Il Titolo II, noto come Online Copyright

[48] **STANIMIROVIC U.,** *A publisher Guide to DRM. What is DRM, How does it works, and when do publisher need it,* Video Technology, 2023. Articolo disponibile su https://target-video.com/what-is-drm/

[49] **THE USENIX ASSOCIATION**, *Proceedings of the 10th USENIX Security Symposium,* 2001, https://web.archive.org/web/20201031040253/https://www.usenix.org/legacy/publications/library/proceedings/sec01/craver.pdf

[50] **KESDEN G.**, *Content Scrambling System (CSS): Introduction, 2000.* https://www.cs.cmu.edu/~dst/DeCSS/Kesden/index.html

[51] **U.S COPYRIGHT OFFICE SUMMARY,** *The Digital Millennium Copyright Act of 1998,* 1998 *https://www.copyright.gov/legislation/dmca.pdf*

Infringement Liability Limitation Act, stabilisce limitazioni alla responsabilità dei fornitori dei servizi online per violazioni del diritto d'autore commesse dagli utenti. Prevede un sistema di notice and takedown che consente ai detentori dei diritti di richiedere la rimozione di contenuti illeciti. Il Titolo III, invece, crea un'eccezione che permette la copia di programmi per computer durante la manutenzione o riparazione di un computer, a condizione che tali copie siano distrutte al termine del processo. Il Titolo IV contiene sei disposizioni varie che riguardano le funzioni dell'Ufficio del Copyright, l'educazione a distanza, le eccezioni per le biblioteche, le registrazioni effimere e la protezione per la progettazione degli scafi delle imbarcazioni. Infine, il Titolo V, noto come Vessel Hull Design Protection Act, introduce una nuova forma di protezione per il design degli scafi delle imbarcazioni[52].

Nel linguaggio informatico ed economico, la sigla DRM assume diversi significati. Nella sua accezione più ampia, però, DRM indica dei sistemi tecnologici progettati per definire, gestire, proteggere e applicare le regole di accesso e utilizzo di contenuti digitali, come ad esempio, testi, suoni, immagini e video[53]. Digital Rights Management è quindi il termine più in voga per descrivere una specifica modalità di distribuzione e fruizione di contenuti digitali, ovvero informazioni, che è protetta da tecnologie software e hardware. Questa forma di distribuzione e utilizzo dei contenuti digitali non si basa esclusivamente su Internet, sebbene questo rimanga il principale mezzo di valorizzazione, ma include anche reti dedicate e vari dispositivi come Personal Digital Assistant (PDA) e telefoni digitali. Il DRM non si limita a una singola tecnologia, ma si fonda sull'integrazione di diverse tecnologie, le quali sono in costante e rapida evoluzione. Le imprese che forniscono contenuti digitali a pagamento aspirano a utilizzare una rete globale che supporti un sistema DRM unico e inviolabile. Questo sistema è un fenomeno complesso con implicazioni economiche, giuridiche e sociali, il quale rappresenta un modello di business che stabilisce una serie di regole. Tutti i soggetti della catena di produzione e distribuzione dei contenuti digitali devono attenersi a queste regole per ottenere l'accesso a delle specifiche modalità di fruizione del contenuto stesso.

Uno dei modelli teorici di maggiore successo definisce il DRM come le modalità attraverso le quali un determinato contenuto può essere utilizzato da terzi, quali rivenditori, intermediari o utenti finali, in cambio di una qualche forma di remunerazione. Questo modello suddivide i diritti di utilizzo

[52] **U.S COPYRIGHT OFFICE SUMMARY,** *The Digital Millennium Copyright Act of 1998,* 1998 https://www.copyright.gov/legislation/dmca.pdf

[53] **CASO R.,** *Digital Right Management, Il commercio delle informazioni digitali tra contratto e diritto d'autore*, 2006

del contenuto digitale in tre principali gradi di libertà: il trasferimento del contenuto, il suo riutilizzo da parte di soggetti intermedi, le modalità di fruizione finale[54]. Ogni grado di libertà di utilizzo comprende diverse ulteriori possibilità di fruizione. Ad esempio, il trasferimento include: la duplicazione, cioè il diritto di due o più utenti di fruire in modo indipendente del contenuto, lo spostamento, ovvero il diritto di cedere il contenuto o l'accesso ad esso ad altri utenti rinunciando alla propria possibilità di fruirne e, infine, il prestito il quale consente di cedere temporaneamente il contenuto a terzi privandosi della possibilità di accedervi fino alla restituzione.

Per quanto riguarda le modalità di fruizione finale, quali copia permanente, visione ed esecuzione, ciascuna di esse può essere articolata in una combinazione di tre fattori: estensione dei diritti in termini di tempo (giorni, mesi, etc.) e quantità (numero di copie, esecuzioni, etc.); categoria di utenti finali, che possono essere paganti o non paganti, con prezzo ridotto o che hanno diritto solo a una demo con funzionalità limitate o a tempo determinato; contraccambio, ovvero la prestazione richiesta per ottenere i diritti di accesso e fruizione, che non deve necessariamente consistere nel pagamento di una somma di denaro (ad esempio, alcuni siti web offrono accesso in cambio della registrazione e dei dati personali dell'utente)[55].

I modelli teorici di DRM vengono poi tradotti in un complesso di tecnologie software, implementate sui vari elementi della catena distributiva. Innanzitutto, è necessario un sistema che informi queste diverse componenti sulle regole specifiche con cui un utente può accedere a un determinato contenuto. Queste regole devono essere descritte in un linguaggi interpretabile da un computer, ovvero in modo preciso, completo, non ambiguo e comprensibile da tutte le componenti del sistema DRM utilizzato. Questo tipo di linguaggio è noto come Rights Expression Language (REL). Il tema del REL è collegato a un'altra promessa della rete: lo sviluppo del cosiddetto Web semantico. Inoltre, l'implementazione di un modello di DRM può essere anche vista come l'organizzazione di un'architettura di un sistema informativo basato su diverse componenti. Ciascuna di queste componenti ha dei compiti precisi, le quali interagiscono tra loro utilizzando formati, protocolli e linguaggi comuni. Una tipica architettura DRM ridotta all'essenziale è, infatti, costituita da una serie di componenti distribuite nei sistemi informativi del produttore-distributore dei contenuti, e quindi nei sistemi di chi si occupa delle licenze sui contenuti e nei sistemi dell'utente.

[54] **CASO R.,** *Digital Right Management, Il commercio delle informazioni digitali tra contratto e diritto d'autore*, 2006

[55] **TRIPALDI G.,** *Digital Rights Management: come affrontare la salvaguardia del Diritto d'autore nell'era digitale,* 2002

1.1 LE COMPONENTI DEI SISTEMI DRM

Le principali componenti di un sistema DRM sono: a) componenti come i content packagers e i DRM controllers; b) protocolli di comunicazione tra le varie componenti; c) formati dei file in cui sono riversati i contenuti; d) metadati, cioè informazioni sui contenuti come regole contrattuali; e) componenti che garantiscono la protezione del contenuto[56]. L'intero sistema si basa principalmente su quest'ultima categoria di componenti. Le tecnologie di protezione includono vari nomi come tecnologie di controllo della copia, controllo dell'accesso, controllo dell'integrità, tracciamento del traditore, autenticazione e così via. Tuttavia, queste tecnologie possono essere ricondotte a poche tecnologie di base, essenzialmente crittografia, watermarking e fingerprinting digitali. Le tecnologie DRM possono essere applicate alla produzione e distribuzione protetta dei contenuti digitali come musica, filmati, videogiochi, software ed e-book. La protezione copre tutto il ciclo di vita del contenuto, dalla produzione fino alla fruizione da parte dell'utente. Il sistema DRM gestisce e applica i contratti relativi ai contenuti stessi, ed in più, esprime il massimo delle sue potenzialità se almeno uno dei suoi passaggi avviene attraverso Internet. In questo contesto, può consentire molteplici forme di fruizione, sia con che senza pagamento. Ad esempio, nel caso della distribuzione di file musicali, il sistema potrebbe gestire sia l'acquisizione da parte di privati di beni scaricabili, per un utilizzo limitato senza pagamento, sia l'acquisizione da parte di altre entità, quali aziende dello spettacolo, degli stessi brani, ma per un utilizzo più ampio e dietro pagamento.

Le limitazioni all'utilizzo possono riguardare il tempo, il numero delle forme di utilizzo e, anche, i soggetti a cui è possibile distribuire il contenuto digitale. Un sistema di DRM può, inoltre, facilitare la gestione dei diritti relativi a servizi multimediali frutto della collaborazione di più soggetti. Ad esempio, una rivista online che produce direttamente solo i testi degli articoli, ma acquista le foto da freelance, può utilizzare un sistema DRM per gestire i diritti delle immagini. In ogni caso, gli studiosi di business model ritengono che i sistemi DRM possano essere utilizzati anche per contenuti digitali non protetti da diritti di proprietà intellettuale[57]. Ad esempio, i sistemi DRM possono gestire contenuti che non sono legati all'intrattenimento. In quest'ottica, un sistema DRM

[56] **CASO R.,** *Digital Right Management, Il commercio delle informazioni digitali tra contratto e diritto d'autore*, Ristampa digitale, Trento, 2006

[57] Ibidem

può supportare la gestione di documenti riservati all'interno di un'azienda o di dati circolanti in una rete di strutture sanitarie. In teoria, questi sistemi possono agevolare la conformità dei dati alle prescrizioni legislative e regolamentari. Ad esempio, un'azienda che fornisce informazioni finanziarie potrebbe utilizzare un sistema DRM per certificare che il trattamento dei dati avviene in conformità con le normative di riferimento.

Moltissime software-house stanno investendo nel mercato dei sistemi DRM e alcune di queste sono leader nel proprio settore di riferimento. Per citare solo alcuni esempi rilevanti, si possono menzionare aziende come RealNetworks, Adobe e Microsoft. In particolare, quest'ultima persegue una politica aggressiva di affermazione dei propri sistemi DRM. La strategia di Microsoft sembra finalizzata, da un lato, a sviluppare dei sistemi capaci di gestire diverse tipologie di contenuti digitali, come audio e video, e dall'altro, a integrare sempre più il Digital Rights Management nel proprio sistema operativo di Windows. Tuttavia, questo mercato è ancora giovane e frammentato, soprattutto a causa della grande plasmabilità dei business model su cui si basano. Questa flessibilità permette l'emergere di imprese con modelli di business molto diversi tra loro. In ogni caso, però, esistono imprese che offrono diversi sistemi DRM, così come imprese che offrono servizi tradizionali di gestione delle licenze sui contenuti digitali.

Per comprendere il funzionamento di un sistema di questo tipo, si può prendere in considerazione l'esempio di Microsoft[58]. Da qualche anno, Microsoft sviluppa sistemi DRM integrandoli nell'ambiente Windows, in quanto fondamentali per lo sviluppo del mercato dei contenuti digitali. L'obiettivo dell'implementazione è quello di superare il timore di vedere i contenuti illegittimamente riprodotti. Il sistema DRM presuppone l'integrazione con le tecnologie Windows Media, le quali verranno suddivise in varie componenti. Alcune saranno destinate alle imprese che operano nel mercato dei contenuti, come Windows Media Encoder o Windows Software Development Kit, e altre ad utenti, come Windows Media Player. Pertanto, il DRM deve essere incorporato sia nei siti web delle imprese che commercializzano i contenuti, sia nelle applicazioni installate sui computer degli utenti. La tecnologia alla base della protezione dei contenuti è la crittografia. In pratica, il DRM di Microsoft consente al titolare del contenuto di crittografarlo e di tradurlo nei formati basati sulle tecnologie Windows Media. L'utente, per utilizzare il contenuto (ad

[58] **CASO R.,** *Digital Right Management, Il commercio delle informazioni digitali tra contratto e diritto d'autore*, Ristampa digitale, Trento, 2006

esempio, ascoltare una canzone tramite Windows Media Player installata sul proprio computer) deve ottenere una licenza che contiene anche la chiave di decrittazione[59].

La licenza incorpora le regole, e quindi i diritti, che l'utente deve rispettare, come la regione del mondo in cui il file audio può essere ascoltato, quante volte può essere ascoltato e fino a quando. Può essere gestita in diversi momenti della relazione contrattuale tra l'impresa fornitrice del contenuto e l'utente, a seconda del modello di business scelto dall'impresa stessa. Il contenuto rimane protetto indipendentemente dalla forma di distribuzione scelta dal suo titolare. La caratteristica più impressionante dell'architettura DRM di Microsoft è la pervasività della crittografia, la quale richiede all'utente di relazionarsi ripetutamente ai siti web di riferimento per rendere effettive le proprie possibilità di fruizione. Diversamente dalla fruizione tradizionale delle opere dell'ingegno, che ha nell'acquisto anonimo il momento iniziale e terminale della relazione con il distributore (come ad esempio l'acquisto di un libro o di un vinile), nel contesto del DRM di Microsoft la relazione contrattuale tra il provider dei contenuti e l'utente finale è costituita da una serie continua di atti, come la registrazione dell'utente o dell'applicazione, il rilascio o il rinnovo della licenza, e così via. Prima dell'avvento dell'era digitale, il diritto d'autore assicurava un equilibrio tra i diritti dei creatori (per incentivare e remunerare il loro sforzo creativo) e quello degli utilizzatori (per promuovere la diffusione della conoscenza e della cultura, in modo da favorire lo sviluppo del capitale sociale). La società dell'informazione ha destabilizzato questo equilibrio e i modelli di business su cui si basava.[60]

1.2 EVOLUZIONE DEL DRM: LA PROTEZIONE DEI CONTENUTI DIGITALI E NUOVI MODELLI DI BUSINESS NEL MERCATO GLOBALE

Attualmente, il quadro giuridico internazionale presenta delle disparità nelle legislazioni applicabili ai servizi della società dell'informazione. Questa situazione comporta una notevole insicurezza giuridica. Di fatti, la mobilitazione in alcuni stati verso una nuova legislazione rischia di creare divergenze negli approcci e di frammentare i mercati. Sebbene ci siano iniziative legislative

[59] **CASO R.,** *Digital Right Management, Il commercio delle informazioni digitali tra contratto e diritto d'autore*, Ristampa digitale, Trento, 2006

[60] Ibidem

per armonizzare le norme, sono sempre presenti alcune discrepanze nello scenario internazionale[61]. Ad esempio, in Italia il DMCA è stato recepito, mentre altri stati europei sono ancora in fase di definizione dell'implementazione di tali normative. In questo contesto possono sorgere differenze nell'interpretazione delle norme, soprattutto per quanto riguarda l'elusione dei meccanismi dui controllo dell'accesso, come quelli impiegati nella codifica delle regioni dei DVD.

Negli Stati Uniti il Fair Use è una dottrina legale che consente l'utilizzo limitato di opere protette da copyright senza il permesso del titolare, per scopi quali la critica, il commento, l'informazione giornalistica, l'insegnamento e la ricerca. In altri paesi, esistono dei concetti simili, ma le eccezioni al diritto d'autore variano notevolmente. Alcune legislazioni potrebbero, infatti, essere più restrittive o, anche, più permessivi rispetto agli Stati Uniti. Le variazioni nella legge sul Fair Use tra i paesi creano incertezze per le piattaforme che distribuiscono contenuti su internet. Ciò significa che un servizio online deve adattarsi alle leggi di ogni paese in cui opera. Bisogna però comunque tenere conto degli interessi degli autori delle opere dell'ingegno. Di fatti, se le eccezioni al diritto d'autore in un paese sono troppo ampie, i detentori dei diritti potrebbero essere meno motivati a rendere disponibili i loro contenuti online in quel mercato, per timore di perdite economiche o pirateria[62]. Le leggi che regolano il diritto d'autore e i contratti non sono uniformi in tutto il mondo. Sebbene ci siano somiglianze tra vari paesi, ci sono anche differenze significative nell'applicazione di queste leggi, specialmente quando si tratta di contenuti digitali. In Europa, le associazioni di categoria legate all'industria musicale, come i fonografici, hanno avviato diverse iniziative per fermare la condivisione illegale di file su piattaforme peer to peer. Per rafforzare l'applicazione dei diritti di proprietà intellettuale, l'UE ha emanato la direttiva 2004/48/CE chiamata *Direttiva IPR Enforcement.* L'obiettivo principale è quello di garantire che in tutta l'Unione Europea siano disponibili strumenti uniformi per permettere a creatori e innovatori di tutelare e far valere i propri diritti di proprietà intellettuale. Questo mira a creare un sistema giuridico omogeneo in grado di proteggere le opere creative e innovative in modo coerente in tutti i paesi membri[63]. L'implementazione di questa normativa, però, non è stata particolarmente efficace. Ciò significa che l'UE non è riuscita a creare un sistema solido per far rispettare il copyright nel mondo digitale.

---

[61] **MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE, DIPARTIMENTO PER L'INNOVAZIONE E LE TECNOLOGIE**, *Relazione Informativa Digital Rights Management*, 2004 https://www.interlex.it/testi/pdf/drmfull.pdf

[62] Ibidem

[63] **DIRETTIVA 2004/48/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO** del 29 aprile 2004 sul rispetto dei diritti di proprietà intellettuale

Un'ulteriore criticità nell'implementazione dei sistemi di Digital Rights Management è la protezione dei dati personali. Di fatti, molti modelli di business e soluzioni DRM prevedono la registrazione di dati personali, il che comporta complicanze legate alla gestione e tutela di tali dati e rischi di accesso non autorizzato. Inoltre, esiste una preoccupazione politica relativa alla riservatezza dell'accesso a contenuti che potrebbero rivelare informazioni sensibili sugli utenti.

La gestione dei diritti digitali è importantissima nel nascente mercato dei beni immateriali. Questa tecnologia non solo protegge i diritti di titolari e distributori, ma facilita anche l'accesso e l'utilizzo dei contenuti da parte dei consumatori, creando così un rapporto di fiducia tra produttori, distributori e consumatori di contenuti. Il DRM si è evoluto dalla pura tecnologia anti-copia degli anni 90 a un sistema complesso che integra aspetti tecnologici e legali per garantire l'uso corretto dei contenuti digitali e la tutela dei diritti associati. Esso include vari aspetti fondamentali, quali l'identificazione e la descrizione dei diritti di proprietà intellettuale nella catena del valore del contenuto, dalla produzione alla fruizione, il tracciamento delle licenze d'uso e dell'utilizzo effettivo del contenuto e le misure tecniche che assicurano le restrizioni di uso. Il mercato dei beni protetti dal diritto di autore deve affrontare sfide significative, tra cui nuove tecnologie, ubiquità dei contenuti e nuovi modelli di business. L'ampia cornice giuridica, a livello mondiale e comunitario, tutela il diritto d'autore come elemento fondamentale per incentivare creativi e produttori. Tuttavia, i contratti di licenza spesso impongono comportamenti più restrittivi rispetto al diritto d'autore stesso. Esistono spazi e necessità di armonizzazione delle eccezioni d'uso, delle limitazioni del diritto d'autore e dei contratti, soprattutto in presenza di posizioni dominanti in altri mercati, quali, ad esempio, fornitori di sistemi operativi, operatori TLC, distributori di contenuti. Il mercato è caratterizzato dalla presenza di vari standard di riferimento, ma manca ancora uno standard unico indipendente dalle tecnologie di distribuzione e accesso. Le soluzioni proprietarie e verticali attualmente disponibili non garantiscono interoperabilità e facilità d'uso, e nessuna tecnologia può dichiararsi a prova di pirateria. Sono necessari investimenti significativi sia in tecnologie DRM che in sistemi contigui, come content management, gestione clienti, rendicontazione e fatturazione.

La creazione di nuovi modelli di business è vista come una possibile soluzione al problema della protezione dei contenuti digitali. Ad esempio, nel settore musicale, i negozi online come iTunes di Apple, Sony Connect, OD2 e l'atteso Microsoft Janus rappresentano implementazioni interessanti di nuovi modelli. Tuttavia, nessuno di questi modelli è ancora considerato una soluzione ottimale, sebbene condividano alcune caratteristiche comuni.

I modelli innovativi di DRM si trovano attualmente in fasi sperimentali e la loro validità finale è ancora difficile da valutare. Vi sono però alcuni approcci semplificativi, come il modello compensativo in fase di sperimentazione in Brasile, i quali meritano particolare attenzione. Questo modello potrebbe rappresentare un vero salto di paradigma, in quanto elimina il concetto di pirateria digitalizzata: con l'adozione di tale modelli, non esisterebbe nulla da piratare[64]. D'altro canto, modelli come il Copyleft, sebbene innovativi, presentano delle complessità applicative. Il Copyleft consente la distribuzione libera e la modifica dei contenuti, ma la sua applicazione pratica è problematica. Richiede che l'autore definisca quali utenti possano accedere ai contenuti e che esistano tecnologie capaci di gestire tali restrizioni.

Il DRM ha applicazioni significative anche nel settore pubblico, sia per la gestione interna dei contenuti che per l'interazione con il pubblico. Il settore pubblico, con la sua omogeneità di requisiti e standard, rappresenta un ottimo campo di sperimentazione per le soluzioni DRM. In particolare, l'implementazione di sistemi DRM in ambienti chiusi, come biblioteche e scuole, potrebbe rivelare rapidamente le difficoltà e permettere un'adozione efficace dei servizi pubblici basati su Internet. Le aree potenziali per l'uso delle soluzioni DRM includono: amministrazioni centrali e locali, per la gestione sicura dei documenti e dei dati; istruzione, per la protezione dei materiali didattici e dei contenuti educativi; servizi sanitari e sociali, per garantire la sicurezza dei dati sensibili; musei archivi e librerie, per la protezione e la gestione dei beni culturali e storici; e infine, la difesa, per la sicurezza delle informazioni e delle risorse strategiche. In Italia, l'applicazione delle tecnologie DRM è di particolare interesse nel settore dei beni culturali e artistici. La crescente evoluzione delle tecnologie e della domanda di servizi ha incrementato notevolmente il valore dei diritti di proprietà intellettuale detenuti da biblioteche, archivi, siti archeologici e musei[65].

Il mercato italiano dei contenuti online presenta attualmente una disponibilità medio-bassa di contenuti pronti all'uso. Le nuove produzioni sono generalmente digitali, ma spesso non sono gestito con infrastrutture di DRM avanzate. Gli archivi storici sono in gran parte analogici, con alcune eccezioni di rilevo. Le potenzialità per l'uso dei contenuti italiani all'estero sono limitate per i contenuti Media & Entertainment, ma promettenti per i beni culturali. Questi contenuti possono essere

[64] **MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE, DIPARTIMENTO PER L'INNOVAZIONE E LE TECNOLOGIE**, *Relazione Informativa Digital Rights Management*, 2004 https://www.interlex.it/testi/pdf/drmfull.pdf

[65] Ibidem

utilizzati in vari ambiti come cultura, didattica, turismo, giochi e realtà virtuale, e rappresentano una grande opportunità per lo sviluppo del mercato dei contenuti italiani e dell'industria locale.

I principali attori nel mercato online sono gli operatori di telecomunicazioni (TLC) e i Content Providers. Questi ultimi però sono ancor maggiormente concentrati sul business tradizionale e sulla valorizzazione dei propri contenuti, anche se distribuiti attraverso terzi. Il settore DRM in Italia non sembra offrire molte opportunità di sviluppo a causa della mancanza di attori di rilievo internazionale nei settori del software e dei dispositivi di accesso. Attualmente, i sistemi DRM avanzati sono stati introdotti principalmente dagli operatori TLC, i qualisi occupano della distribuzione di contenuti.

2. DRM E DIRITTO D'AUTORE

Il diritto d'autore nasce come una risposta normativa a un fallimento del mercato, in cui i normali meccanismi non riescono a garantire un'efficiente allocazione delle risorse. Nel caso dei beni di proprietà intellettuale, questa situazione si verifica a causa della loro natura: sono beni pubblici, caratterizzati da non rivalità e non escludibilità. Da sempre, si è cercato di trovare un equilibrio tra le esigenze degli autori e degli editori di proteggere le loro opere e quelle degli utenti di accedere liberamente a queste per scopi di informazione pubblica, libera discussione, diffusione della cultura e studio. Questi, infatti, sono tutti diritti costituzionalmente garantiti. Per questo motivi sono stati introdotti dei correttivi al diritto d'autore, i quali sono rappresentati dalle cosiddette eccezioni e limitazioni, dalla limitazione temporale del diritto e dal principio di esaurimento del diritto (c.d. first sale doctrine) Secondo questo principio, il titolare del copyright perde il diritto di controllare la distribuzione successiva alla prima vendita dell'opera. È noto come *first sale doctrine* ed è presente nella sezione 109(a) del titolo 17 dell'U.S.C. In base alla sezione 109(a), l'acquirente di una copia dell'opera può liberamente disporne senza dover chiedere l'autorizzazione del titolare del diritto di distribuzione. Nel 1984, il legislatore statunitense ha introdotto un'eccezione alla first sale doctrine, mantenendo al titolare del diritto di distribuzione il potere di autorizzare il noleggio, leasing o prestito

per scopi di vantaggio commerciale diretto o indiretto di fonogrammi e programmi per elaboratore. In Italia, la disciplina è rinvenibile negli articoli 17 e 18-bis della l. 633/41[66].

L'avvento delle opere digitali, e quindi delle opere dell'ingegno in formato digitale, ha rimesso in crisi questo equilibrio già poco stabile. Le tecnologie moderne permettono infatti di effettuare con facilità e con costi contenuti, copie non autorizzate e perfettamente identiche all'originale, delle opere digitali protette da diritto d'autore, e di distribuirle per via telematica. Inoltre, queste tecnologie sono alla portata di tutti e danno luogo a una pirateria domestica, la quale rappresenta un grave pericoli. Le tecnologie dell'informazione e della comunicazione hanno contribuito al raggiungimento di grandi traguardi, portando però a delle conseguenze sia negative che positive. Infatti, hanno contribuito al sorgere della società dell'informazione e dell'economia della conoscenza, rafforzando il ruolo dei diritti di proprietà intellettuale, ma hanno anche messo a disposizione di tutti degli strumenti più semplici ed economici per violare questi diritti. Non è sufficiente, quindi, affrontare queste problematica solo sul piano giuridico in quanto la disciplina del diritto d'autore è inadeguata rispetto alle nuove tecnologie. Si pensa quindi di combattere la tecnologia con la tecnologia stessa, mediante l'utilizzo di sistemi per impedire i comportamenti lesivi del diritto d'autore e la fruizione illegale del contenuto digitale[67].

2.1 LE MISURE TECNOLOGICHE DI PROTEZIONE E IL DIRITTO D'AUTORE NELL'ERA DIGITALE

In questo contesto, viene introdotta a livello nazionale e internazionale una forte tutela giuridica delle cosiddette Misure Tecnologiche di Protezione (MTP), le quali vengono utilizzate per proteggere i diritti di proprietà intellettuale sulle opere dell'ingegno. Queste misure vengono definite dalla legge sul diritto d'autore all'art. 102 quater come *tutte le tecnologie, i dispositivi o i componenti destinati a impedire o limitare atti non autorizzati dai titolari dei diritti*. La legge tutela solo le misure efficaci, ossia quelle che consentono ai titolari di controllare l'uso dell'opera tramite dispositivi di accesso o procedimenti di protezione, come la cifratura, la distorsione o qualsiasi altra trasformazione

[66] **AUTERI P.** *Il contenuto del diritto di autore,* in AA. VV., *Il diritto industriale,* 7 ed., Giappichelli, 2023, p. 625 ss.

[67] **FLORIO A.,** *I sistemi di Digital Rights Management (DRM),* 2009 https://www.dirittodellinformatica.it/diritto-autore/copyright-focus/i-sistemi-di-digital-rights-management-drm.html/

dell'opera, oppure mediante meccanismi di controllo delle copie[68]. Le MTP possono essere contenute anche nei sistemi di Digital Rights Management, le quali sono in grado di gestire in forma digitale tutti i diritti e non solo quelli sulle opere digitali. L'uso di queste tecnologie non riguarda, quindi, solo il diritto d'autore, ma anche la gestione digitale di altri diritti, come la gestione dei documenti aziendali e delle informazioni, di contenuti relativi ai dati sensibili e di applicazioni in campo sanitario e medico, nell'E-Governement e nel settore dei beni culturali. In ogni caso, però, le opere digitali rappresentano il campo di applicazione più significativo[69].

I sistemi di DRM possono essere utilizzati per identificare e negoziare i diritti sulle opere, monitorare il loro utilizzo e proteggerle contro usi non consentiti. Vi sono tre generazioni di sistemi DRM legati alle opere digitali: la prima generazione visualizza semplici informazioni relative all'opera e al titolare dei diritti; la seconda generazione aggiunge funzionalità di protezione, identificazione e accesso ai contenuti, nonché funzioni di Content Management; la terza generazione è in grado di gestire i rapporti tra tutti i soggetti coinvolti nell'amministrazione dell'opera e dei diritti relativi. Gli attuali sistemi DRM sono complessi e composti da sottosistemi. Questi sistemi, secondo alcuni sostenitori, dovrebbero facilitare la circolazione delle opere, offrendo ai titolari dei diritti una maggiore sicurezza contro usi non autorizzati. Inoltre, la WIPO considera questi sistemi necessari per la creazione di un mercato telematico delle opere digitali. Ci sono, però, preoccupazione e critiche da chi sostiene l'accesso libero alle opere dell'ingegno. Le MTP espandono oltre i limiti legali i poteri degli autori, creando uno squilibrio tra gli interessi degli autori ed editori e gli interessi degli utenti. Queste misure creano inoltre anche problemi per i consumatori e la privacy[70].

Secondo il principio di esaurimento del diritto, il titolare dei diritti d'autore su un'opera perde il diritto di controllare l'ulteriore distribuzione di un esemplare dell'opera dopo la sua prima vendita. Questo principio è considerato di norma imperativa e non è derogabile contrattualmente. Inoltre, implica che le Misure Tecnologiche di Protezione e i sistemi di Digital Rights Management che permettono ai titolari di controllare le distribuzioni dell'opera, anche successiva alla prima messa in circolazione, vengano considerati illeciti. La l. 633/41 prevede delle limitazioni a questi principio. L'art. 17, c. 2, infatti, sancisce che il principio di esaurimento non opera nel caso di messa a

[68] **SENA G., FRASSI A. E. P., D'AMMASSA G., GIUDICI S., MINOTTI D., MORRI F.,** *Diritto d'autore e diritti connessi nella società dell'informazione,* IPSOA, 2003

[69] **SPEDICATO G.**, *I Digital Rights Management System tra produzione e diffusione di opere dell'ingegno. Quale nuovo aspetto per il diritto d'autore?,* in Ciberspazio e diritto, vol. 5, n. 3, 2004, pp. 273-302.

[70] **FLORIO A.,** *I sistemi di Digital Rights Management (DRM),* 2009 https://www.dirittodellinformatica.it/diritto-autore/copyright-focus/i-sistemi-di-digital-rights-management-drm.html/

disposizione del pubblico di opere in modo che ciascuno possa avervi accesso dal luogo e nel momento scelti individualmente, anche nel caso in cui sia consentita la realizzazione di copie dell'opera. Quindi, l'articolo esclude dal campo di applicazione del principio di esaurimento la circolazione delle opere digitali attraverso reti telematiche. Seguendo questa logica, le MTP e i sistemi DRM che attribuiscono ai titolari il potere di controllare ogni distribuzione dell'opera, anche successiva alla prima messa in circolazione, sarebbero illegittimi. Però, con l'esclusione delle opere digitali distribuite in via telematica dall'ambito di applicazione del principio di esaurimento, la legge crea una distinzione tra opere fisiche e digitali. Questa distinzione riflette le difficoltà giuridiche ed economiche nel bilanciare i diritti delle opere e quelli degli utenti nell'era digitale, dove la distribuzione e la copia di contenuti possono essere eseguite con estrema facilità. Di conseguenza, le MTP e i DRM rimangono strumenti controversi, ma rilevanti per la protezione dei diritti d'autore in un contesto tecnologico in continua evoluzione[71].

Il controllo esercitato attraverso le Misure Tecnologiche di Protezione può ledere le eccezioni e limitazioni al diritto d'autore. Le eccezioni sono disposizioni legislative che consentono agli utenti di svolgere determinate attività, normalmente vietate dal diritto d'autore, senza necessitare di una preventiva autorizzazione del titolare dei diritti. I sistemi DRM comuni, infatti, non sono in grado di distinguere i diversi contesti di utilizzo delle opere. Secondo l'art. 71, l. 633/4, i titolari dei diritti d'autore devono adottare idonee soluzioni per consentire l'esercizio di alcune eccezioni, ma solo su espressa richiesta dei beneficiari e a condizione che questi ultimi abbiano acquisito il possesso legittimo delle opere e del materiale protetto o vi abbiano avuto accesso legittimo ai fini del loro utilizzo, nel rispetto delle disposizioni sulle eccezioni e limitazioni, inclusa la corresponsione dell'equo compenso. Tuttavia, le idonee soluzioni non sono richieste quando, in base ad accordi contrattuali, le opere o il materiale protetto sono messi a disposizione del pubblico in modo che ciascuno vi possa avere accesso dal luogo o nel momento scelti individualmente. Questa previsione spesso non garantisce agli utenti l'esercizio delle loro prerogative, poiché le condizioni sono spesso eccessivamente onerose rispetto alle esigenze dell'utente medio[72].

Tra le eccezioni e limitazioni rientra anche la questione della copia privata. L'art. 71-sexies comma 3 della Legge 633/41 stabilisce che la copia privata per uso personale non è consentita per le

[71] **SPEDICATO G.**, *I Digital Rights Management System tra produzione e diffusione di opere dell'ingegno. Quale nuovo aspetto per il diritto d'autore,* in Ciberspazio e diritto, vol. 5, n. 3, 2004, pp. 273-302.

[72] Ibidem

opere o i materiali protetti messi a disposizione del pubblico in modo che ciascuno possa avervi accesso dal luogo e nel momento scelti individualmente, quando l'opera è protetta dalle misure tecnologiche di cui all'articolo 102-quater ovvero quando l'accesso è consentito sulla base di accordi contrattuali. Questo crea un conflitto tra il diritto alla copia privata, considerato un diritto dell'utente, e le disposizioni relative alle MTP. Il legislatore cerca di risolvere questo conflitto, in modo insufficiente, tramite il comma 4, dell'articolo 71 sexies: "*fatto salvo quanto disposto dal comma 3, i titolari dei diritti sono tenuti a consentire che, nonostante l'applicazione delle misure tecnologiche di cui all'articolo 102-quater, la persona fisica che abbia acquisito il possesso legittimo di esemplari dell'opera o del materiale protetto, ovvero vi abbia avuto accesso legittimo, possa effettuare una copia privata, anche solo analogica, per uso personale, a condizione che tale possibilità non sia in contrasto con lo sfruttamento normale dell'opera o degli altri materiali e non arrechi ingiustificato pregiudizio ai titolari dei diritti.*" Il DRM, quindi, può rappresentare una effettiva limitazione anche alla possibilità di effettuare copie per uso privato, creando ulteriori ostacoli per gli utenti nel godere pienamente dei diritti concessi dalle eccezioni al diritto d'autore[73].

Mentre i diritti morali relativi al diritto d'autore non sono soggetti a limitazioni temporali, e dopo la morte dell'autore possono essere esercitati dagli eredi (art. 23 L. 633/41), i diritti di utilizzazione economica dell'opera sono soggetti a precisi limiti di durata. Secondo l'art. 25 L. 633/41, i diritti di utilizzazione economica dell'opera durano tutta la vita dell'autore e sino al termine del settantesimo anno solare dopo la sua morte. Anche questa norma, come il principio di esaurimento, è considerata una norma imperativa, non derogabile contrattualmente. Questo implica che le MTP e i DRM che proteggono l'opera oltre questo limite, sono da considerare illeciti. Tuttavia, i DRM attualmente utilizzati per proteggere le opere digitali non considerano questo limite di tempo. L'utilizzo dei DRM, infatti, continua a limitare l'accesso e l'utilizzo delle opere digitali anche dopo che i diritti di utilizzazione economica sono scaduti, violando così il principio che stabilisce la durata dei diritti patrimoniali sul diritto d'autore. Questo crea un conflitto tra la protezione tecnologica delle opere e le disposizioni legali che regolano la durata dei diritti d'autore, evidenziando la necessità di un allineamento tra le tecnologie di protezione e il quadro normativo esistente[74].

[73] **SPEDICATO G.**, *I Digital Rights Management System tra produzione e diffusione di opere dell'ingegno. Quale nuovo aspetto per il diritto d'autore?,* in Ciberspazio e diritto, vol. 5, n. 3, 2004, pp. 273-302.

[74] **FLORIO A.,** *I sistemi di Digital Rights Management (DRM),* 2009 https://www.dirittodellinformatica.it/diritto-autore/copyright-focus/i-sistemi-di-digital-rights-management-drm.html/

Per affrontare il problema dell'eccesiva facilità di riproduzione delle opere dell'ingegno in formato digitale è stato introdotto a livello internazionale un sistema di tassazione sui supporti vergini, quali CD, DVD, etc., noto in inglese come levies. L'introduzione dei sistemi di Digital Rights Management ha sollevato dubbi sulla legittimità di questa tassazione in quanto la logica alla base dei levies è stata minata dalla possibilità di controllare la copia privata grazie ai DRM. Questi due meccanismi, pur avendo finalità diverse, finiscono per gravare sugli utenti-consumatori due volte: quando acquistano i supporti vergini e quando acquistano opere protette da DRM, i quali impediscono la copia privata, comportando così un'ulteriore costo da sopportare[75]. La normativa sul diritto d'autore attualmente in vigore sembra inadeguata a regolare le transazioni riguardanti i contenuti digitali. Nell'era delle nuove tecnologie, è necessario trovare un nuovo equilibrio tra gli interessi contrapposti nel campo del diritto d'autore. Questo bilanciamento potrebbe essere raggiunto, almeno in parte, attraverso una riforma della legge sulle opere dell'ingegno e mediante l'applicazione di norme a tutela dei consumatori[76].

2.2 LA PROTEZIONE DEI CONSUMATORI E LA PRIVACY NEI SISTEMI DRM

Attualmente, non esiste una normativa comunitaria specifica che affronti direttamente i sistemi DRM in relazione alla tutela dei consumatori. Per garantire una protezione adeguata contro tali sistemi, è fondamentale considerare vari aspetti del problema e fare riferimento alle diverse normative applicabili, tra cui la protezione dei consumatori, le clausole vessatorie e la privacy. Data la diffusione delle opere digitali protette da DRM attraverso reti telematiche, è importante prestare particolare attenzione alle norme sui contratti a distanza e sul commercio elettronico. Una questione rilevante in questo contesto è la validità giuridica dei contratti click-wrap, i quali consentono di esprimere la propria volontà contrattuale relativa a software o a siti web mediante la pressione di un pulsante o di un click. Questi contratti possono includere clausole riguardanti i sistemi DRM, sollevando problematiche di compatibilità non solo con la normativa sulle clausole vessatorie, ma anche con il diritto d'autore. Ad esempio, la validità delle esclusioni delle eccezioni e limitazioni del diritto d'autore e le clausole contrattuali che limitano i diritti dell'utente potrebbero risultare

[75] **FLORIO A.,** *I sistemi di Digital Rights Management (DRM),* 2009 https://www.dirittodellinformatica.it/diritto-autore/copyright-focus/i-sistemi-di-digital-rights-management-drm.html/

[76] **SPEDICATO G.**, *Le misure tecnologiche di protezione del diritto d'autore,* Gedit, Bologna, pp. 171-244, 2006.

vessatorie. La trasparenza delle informazioni riguardanti l'uso dei sistemi DRM è essenziale per consentire ai consumatori di fare scelte informate. Il funzionamento di un sistema DRM potrebbe non essere sempre chiaro, creando nel consumatore aspettative errate sul prodotto. È quindi necessario che i professionisti forniscano in modo chiaro e comprensibile informazioni su come i sistemi DRM interagiscono con l'opera, le apparecchiature e i dati personali del consumatore, inclusi i termini e le condizioni, il realizzatore del sistemi e i contatti disponibili. L'omissione di informazioni rilevanti può configurarsi come una pratica commerciale ingannevole se induce il consumatore medio a prendere una decisione che altrimenti non avrebbe preso. Inoltre, secondo la normativa sulla vendita di beni di consumo, il venditore è tenuto a consegnare beni conformi al contratto di vendita e può essere ritenuto responsabile in caso di difformità[77].

Le tecnologie DRM hanno la capacità di identificare e monitorare gli utenti, registrando i contenuti che leggono, guardano o ascoltano. Sebbene alcuni utenti possano beneficiare di prezzi più bassi o di servizi personalizzati grazie a una possibile discriminazione dei prezzi, è innegabile che i sistemi DRM possono invadere la privacy degli utenti in modo significativo, trattando i loro dati personali per vari scopi, anche senza il consenso esplicito degli interessati. Questo solleva importanti questioni relative alla protezione della privacy. La direttiva europea sulla privacy 95/46/CE non affronta esplicitamente la protezione contro i sistemi DRM. Però, la direttiva 2001/29/CE sul diritto d'autore, fa riferimento alla protezione della privacy nel Considerando 57, il quale afferma che le misure tecnologiche in oggetto devono presentare, nelle loro funzioni tecniche, meccanismi di salvaguardia della vita privata, come previsto dalla direttiva 95/46/CE. Secondo il Codice italiano in materia di protezione dei dati personali, nello specifico Artt. 11 e 13 del Decreto legislativo 196/ 2003, il trattamento dei dati deve avere una finalità specifica e deve essere chiaramente comunicato all'interessato. È previsto anche il diritto dell'interessato di opporsi al trattamento dei propri dati personali per scopi di marketing diretto e profilazione (Art. 7 punto 4 lettera b del Decreto legislativo 196/ 2003.). Tuttavia, garantire la protezione effettiva di questi diritti può essere complesso. Per questo motivo, si è pensato di ricorrere alla tecnologia stessa per rafforzare la protezione della privacy e prevenire l'uso illecito dei dati personali, attraverso l'uso dei cosiddetti PETs (Privacy Enhancing Technologies). Questi strumenti mirano a migliorare la tutela della privacy implementando soluzioni

[77] **ROSENBLATT B., TRIPPE B. e MOONEY S.,** *Digital Rights Management. Business and Technology,* John Wiley & Sons, 1 ed., 2001.

tecniche che limitano la raccolta e l'uso dei dati personali, cercando di bilanciare l'esigenza di protezione dei diritti degli utenti con le necessità di gestione e protezione dei contenuti digitali.[78]

Per costruire un rapporto di fiducia tra i consumatori e le nuove tecnologie, è essenziale sviluppare standard tecnologici per i sistemi DRM. Così facendo, è possibile ottenere l'interoperabilità tra dispositivi e servizi tecnologici, la quale riguarda la capacità di accedere a contenuti digitali utilizzando diversi dispositivi e software[79]. Queste pratiche però preoccupano l'industria culturale, la quale è del parere che la standardizzazione dei DRM possa rendere le proprie opere più vulnerabili alla pirateria. Proprio, per questo motivo, spinge affinché i sistemi DRM limitino l'interoperabilità tra i dispositivi. Questa posizione è spesso e volentieri supportata dalle legislazioni che proteggono l'integrità dei sistemi DRM. Bisogna però prendere in considerazione la riduzione della concorrenza nel mercato e creare un ambiente meno competitivo. I DRM non interoperabili hanno conseguenze negative sul mercato dei contenuti digitali e sul mercato dei computer. Alcuni esperti, infatti, avvertono che tali DRM potrebbero portare alla fine dei computer general-purpose[80], rendendo difficile per i consumatori utilizzare i loro dispositivi per scopi diversi. Inoltre, l'incapacità di utilizzare un contenuto digitale su dispositivi diversi o di utilizzare contenuti di fornitori diversi su un unico dispositivo potrebbe sollevare problemi legali anche se non violano direttamente le normative sul diritto d'autore. Tali limitazioni possono influenzare negativamente la protezione dei consumatori, in particolare per quanto riguarda: gli obblighi informativi, in quanto i consumatori devono essere informati in modo chiaro e trasparente sulle restrizioni imposte dai DRM; le clausole vessatorie, le quali potrebbero essere ritenute ingiuste in quanto limitano in modo eccessivo l'uso dei contenuti; le pratiche commerciali ingannevoli, in quanto la mancanza di chiarezza sulle restrizioni potrebbe ingannare i consumatori, portandoli a fare acquisiti che non soddisfano le loro aspettative; ed infine la garanzia e la conformità, infatti se un prodotto non rispetta le promesse fatte o le aspettative di interoperabilità, il venditore potrebbe essere ritenuto responsabile per difformità rispetto al contratto di vendita. Per affrontare questi problemi, è necessario introdurre nuove normative, in grado di garantire un equilibrio tra protezione dei diritti d'autore e necessità di

[78] **MONTAGNANI M. L. e BORGHI M.,** *Proprietà digitale. Diritti d'autore, nuove tecnologie e digital rights management,* EGEA, 2006.

[79] **LUCCHI N.,** *The Unfair play of DRM Technologies: Rereading the rules of the Game from the Consumer's Persopective*, Papers. Paper 50, New York University School of Law, 2007.

[80] Un computer general-purpose è un sistema di elaborazione programmabile, progettato per eseguire una vasta gamma di programmi. Trattandosi di un macchina universale, è in grado di risolvere qualsiasi problema per cui esista un algoritmo, purchè sia utilizzato un linguaggio di programmazione sufficientemente potente e adatto allo scopo..

interoperabilità, senza soffocare l'innovazione. È inoltre, necessaria la standardizzazione volontaria: bisogna promuovere standard comuni per i DRM in modo da risolvere i problemi di interoperabilità senza l'innovazione tecnologica. La collaborazione per la creazione e lo sviluppo di questi standard è cruciale per mantenere un mercato equo e competitivo. In poche parole, quindi, la soluzione è l'adozione di standard tecnologici per i DRM e la creazione di normative che bilancino la protezione dei diritti d'autore con i diritti dei consumatori, garantendo un mercato aperto e innovativo[81].

I sistemi DRM possono installare sul computer dell'utente, anche a sua insaputa, software destinati a limitare l'accesso non autorizzato ai contenuti. Questi programmi possono causare conflitti con i driver, interferire con altre applicazioni, compromettere le funzioni del computer, o addirittura aprire porte che potrebbero essere sfruttare da hacker per infettare il sistema con virus, worm e trojan. Questo comportamento potrebbe violare l'art. 615 quinquies del Codice penale. Questo articolo punisce la diffusione di programmi destinati a danneggiare o interrompere un sistema informatico. Se queste azioni causano effettivamente danni al sistema informatico, si potrebbe applicare l'art. 635-bis c.p., il quale sanziona il danneggiamento di sistemi informatici e telematici[82].

2.3 SCENARI FUTURI DEI SISTEMI DRM NEL CONTESTO DEL DIRITTO D'AUTORE

Nel contesto dell'evoluzione futura dei sistemi di gestione delle opere digitali, è possibile delineare cinque possibili scenari riguardanti l'interazione tra le opere digitali e il diritto d'autore. Il primo scenario è lo Stallo Normativo. Secondo questa visione, le normative recenti non risolvono i conflitti esistenti, ma al contrario portano ad un clima di incertezza. Gli attori coinvolti si concentrano sull'osservazione del conflitto di interessi, monitorano le iniziative legali sui contenuti digitali, valutano l'efficacia dei sistemi DRM sul mercato e analizzano i nuovi modelli di business emergenti, senza giungere a soluzioni concrete. Il secondo scenario è quello del Blocco Tecnologico. In questo scenario i diritti degli utenti finali non sono considerati. Le restrizioni legali e i sistemi DRM offrono ai titolari dei diritti d'autore un totale controllo sui media digitali, andando oltre le limitazioni previste dalla normativa sul copyright. Questo potrebbe portare a un ambiente dove le libertà degli utenti sono

[81] **LUCCHI N.,** *The Unfair play of DRM Technologies: Rereading the rules of the Game from the Consumer's Persopective*, Papers. Paper 50, New York University School of Law, 2007.

[82] Ibidem

molto limitate. Il terzo scenario è quello degli Ostacoli Tecnologici e Legali, in cui è previsto lo sviluppo del commercio elettronico per la distribuzione online dei contenuti digitale come soluzione alla crisi dei media digitali. Il successo dei servizi di media online è dovuto ad una combinazione di restrizioni tecnologiche, legali e sociali. In questo contesto, la pirateria e il file-sharing vengono completamente sconfitti. Tuttavia, il successo è correlato alla capacità dei servizi online di attrarre più utenti rispetto ai network peer-to-peer. Questo scenario riflette i modelli di business prevalenti, come i negozi digitali online. Il quarto scenario è quello della Compensazione Alternativa. Qui gli utenti pagano in base all'uso dei media digitali e i creatori vengono ricompensati in base alla popolarità delle loro opere. Questo sistema si basa su due elementi principali: la registrazione delle opere e un prelievo che genera fondi per il sistema. I creatori registrano le loro opere presso un'agenzia governativa, la quale fornisce l'infrastruttura per il download e applica un marchio elettronico per monitorare la trasmissione online. Il prelievo viene applicato su dispositivi e servizi necessari per l'accesso a internet, come i masterizzatori o player MP3. I proventi raccolti vengono distribuiti tra i creatori in base alla popolarità delle loro opere. In questo scenario la pirateria non esiste e il DRM si limita a raccogliere informazioni sulla popolarità delle opere. Il quinto e ultimo scenario è quello della Cooperativa di Intrattenimento. Per certi versi è molti simile al quarto scenario, però presenta una grande differenza: la partecipazione non è volontaria. I creatori devono registrale le proprie opere presso un'organizzazione privata e i fondi per il sistema derivano dalle quote di iscrizione dei membri. Questo modello implica una cooperativa dove i finanziamenti per il sistema provengono direttamente da chi partecipa[83].

Fino ai primi anni '90, vi era una chiara associazione tra formato e supporto: i testi si trovavano nei giornali e nei libri, l'audio, invece, era veicolato tramite radio, cassette, CD e i video attraverso televisione, cinema e videocassette. Questa struttura ha subito un cambiamento radicale con l'evoluzione delle tecnologie digitali. Le compagnie di telecomunicazione sono entrate a far parte del mondo della comunicazione, contribuendo così alla crescita di Internet. Inizialmente, Internet si basava su reti a banda stretta, solo dopo ha cominciato ad utilizzare connessioni a banda larga, sia per le linee fisse che per le linee mobili. Ad oggi, Internet è accessibile sia per le reti fisse che mobili e, di conseguenza, è in grado di leggere, ascoltare, visualizzare, manipolare e copiare testi, audio e contenuti multimediali in modo indiscriminato. L'introduzione di Internet ha portato a notevoli

[83] **GARTNERG2 e THE BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD LAW SCHOOL**, *Five scenarios for Digital Media in a Post-Napster World,* Research Publication No. 2003-07, 2003 https://cyber.harvard.edu/wg_home/uploads/286/2003-07.pdf

cambiamenti nel mondo dei media e questo, poi, ha condotto ad un nuovo paradigma: il passaggio dalla distribuzione e la vendita di beni tangibili alla distribuzione e la licenza di beni intangibili. Nell'era pre-Internet, molti contratti di gestione dei contenuti erano esclusivi. Questa esclusività diminuirà con l'introduzione dei contenuti digitali. Il legame formato-media viene meno a causa della maggiore virtualizzazione dei contenuti. In passato, l'esclusività era strettamente legata allo specifico media fisico e a specifici canali di distribuzione, quali cinema, giornali, libri, VSH etc. Ora invece, vi è l'emergenza di trovare un nuovo approccio ai contratti legati al copyright e alla distribuzione. Media, canali e modalità di consumo sono tantissimi e sono ancora da scoprire in termini di business. Vi sono, a tal proposito, due casi importanti: il caso Random House con RosettaBooks e il caso Tasini contro New York Times[84].

Il primo caso ebbe inizio nel febbraio 2000 quando RosettaBooks cominciò a vendere le pubblicazioni di diversi autori, tra cui William Styron, Kurt Vonnegut and Robert B. Parker, in formato elettronico. Random House, una compagnia che fa parte di Bertelsmann, che aveva in precedenza acquistato i diritti di pubblicazione delle opere di questi autori, decide di intentare una causa contro RosettaBooks. Analizzando i contratti tra Random House e gli autori, verrà fuori che la casa editrice aveva acquisito i diritti di stampare, pubblicare e vendere le opere degli autori nel formato tradizionale di libro e quindi inteso come "una collezione di pagine stampate legate assieme". Non c'era niente, quindi, in grado di impedire la pubblicazione di queste opere in formati diversi da parte di terzi. Di conseguenza, RosettaBooks venne scagionata. Per quanto riguarda, invece, il secondo caso, il New York Times fu uno tra i primi al mondo a creare il proprio sito web. In questo sito venivano pubblicati soprattutto articoli acquistati per essere pubblicati nei quotidiani New York Times e Newday, oltre che sulla rivista Sports Illustrated. Jonathan Tasini, che allora era il presidente del National Writers Unione (NWU), intentò una causa contro il New York Times. Nel 1999 la Corte, ribaltando una sentenza del 1997, sentenziò che i diritti per pubblicare online erano completamente diversi rispetto a quelli per pubblicare sui media tradizionali e quindi di conseguenza il quotidiano New York Times venne dichiarato colpevole.

Questi eventi e le loro conseguenze hanno reso Internet sempre più stabile fino a farlo diventare un media alla pari con quelli tradizionali. È stata messa anche in risaltò la necessità di identificare metodi, tecniche, regole, modelli e altri requisiti in modo da poter assicurare il corretto

[84] **MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE, DIPARTIMENTO PER L'INNOVAZIONE E LE TECNOLOGIE**, *Relazione Informativa Digital Rights Management*, 2004 https://www.interlex.it/testi/pdf/drmfull.pdf

funzionamento del mercato. Infatti, è cruciale proteggere i diritti dei diversi stakeholders della nuova catena di valore e garantire lo sviluppo di questo nuovo media. Le tecnologie digitali hanno introdotto nuove sfide che gli autori e gli editori devono saper affrontare. Uno dei rischi maggiori è la pirateria. In questo scenario è essenziale avere a disposizione sistemi avanzati di DRM, i quali rappresentano un fattore base per il mercato dei contenuti digitali. Il rapporto di fiducia tra i consumatori, produttori e distributori dei contenuti è uno dei prerequisiti per lo sviluppo di un mercato efficiente ed efficace. I Digital Rights Management (DRM) si sono evoluti nel tempo e da essere una mera tecnologia anti-plagio dei primi anni '90, sono diventati un sistema tecnologico legale. L'obiettivo dei DRM è quello di promuovere un utilizzo consapevole e corretto dei contenuti digitali e di assicurare una protezione dei diritti connessi a questi contenuti. Nel mercato attuale, i DRM assumono diversi significati a livello legale, tecnologico e sociale. Prima dell'avvento dell'era digitale, le leggi sul diritto d'autore assicuravano un equilibrio tra i diritti dei creatori, in modo da incentivare e premiare il loro sforzo creativo, e i diritti dell'utilizzatore, in modo da promuovere la diffusione della conoscenza e della cultura per lo sviluppo del capitale sociale. La società dell'informazione ha destabilizzato questo equilibro e il modello di business che si era creato attorno ad esso. Attualmente, gli studiosi si concentrano su cinque aree per definire un regolamento capace di mantenere questo equilibrio. Queste cinque aree sono il copyright, gli accordi contrattuali, le norme anti-elusione, il principio di esaurimento del diritto e i sistemi di compensazione[85].

Per quanto riguarda il copyright, l'attuale ordinamento giuridico europeo per la protezione del copyright nella società dell'informazione e per i DRM si basa sulla disciplina comunitaria sul diritto d'autore e, in particolare, sulle sette direttive adottate dal 1991 al 2001. Tra le più importanti c'è la Direttiva sul Copyright, la quale si concentra sulle misure di protezione tecniche senza obbligare i titolari dei diritti ad adottarle, anche se i legislatori sono incoraggiati a promuoverne l'adozione qualora sia opportuno. In ogni caso, l'adozione può risultare solo quando vi è un accordo tra le diverse parti: il detentore dei diritti, gli utilizzatori commerciali e l'utente finale. La direttiva dell'Unione Europea sull'Applicazione dei Diritti di Proprietà Intellettuale (IPR Enforcement) propone l'armonizzazione del contesto legale in modo da proteggere sia la proprietà intellettuale che quella industriale nel mercato dei beni fisici e digitali. Lo sviluppo della legislazione non ha considerato i bisogni e gli interessi degli utenti finali e la sua efficacia ne ha risentito, soprattutto per

[85] **MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE, DIPARTIMENTO PER L'INNOVAZIONE E LE TECNOLOGIE**, *Relazione Informativa Digital Rights Management*, 2004 https://www.interlex.it/testi/pdf/drmfull.pdf

quanto riguardo i beni immateriali. Di conseguenza, la direttiva manca di disposizioni chiare e decisi in materia di contenuti digitali, limitando la sua portata rispetto agli obiettivi iniziali[86].

Nell'Asia Orientale, in Europa e negli USA, le regole contrattuali per i media digitali utilizzano soluzioni come i contratti di licenza e i termini di servizio per disciplinare le modalità di gestione dei contenuti digitali da parte degli utenti finali. Questi contratti di licenza possono prevalere sui diritti che gli utenti finali avrebbero in base alle leggi sul copyright. In Europa e in Giappone, questi accordi spesso e volentieri impediscono agli utenti finali di rivendere, noleggiare o trasferire brani musicali, azioni tipicamente protette dalla dottrina della prima vendita nell'ambito del fair use. Per le transazioni online e per i supporti fisici soggetti a contratti di licenza, come ad esempio il software, il contratto e, soprattutto il contratto di licenza per l'utilizzo di determinati diritti relativi a un'opera o materiale protetto, assume un'importanza notevolmente maggiore rispetto ai tradizionali supporti preregistrati o ai biglietti per gli eventi. Il contratto di licenza diventa parte integrante del prodotto fornito al consumatore e le sue clausole possono avere un impatto sul godimento delle eccezioni da parte dei beneficiari. Questo impatto può essere immediatamente operativo attraverso l'applicazione di misure tecnologiche di protezione accanto alle clausole contrattuali, le quali limitano l'uso. Alcuni suggeriscono che il diritto d'autore nella trasmissione digitale potrebbe essere sostituito da accordi contrattuali combinati con barriere tecnologiche che regolano l'accesso ai materiali online. I fornitori di contenuti digitali utilizzano sempre di più misure tecniche di protezione per limitare l'uso di contenuti digitali. Queste misure sono spesso supportate da leggi che proibiscono l'elusione del DRM. Esistono, poi, segnali di convergenza internazionale relativi a dottrine quali il principio di esaurimento del diritto (first sale). Attualmente, l'Unione Europea e gli USA negano che questo principio possa essere applicato ai lavori digitali distribuiti attraverso Internet, nonostante alcune argomentazioni siano del parere opposto. Ad oggi, i trattati WIPO prevedono l'applicazione del principio di esaurimento del diritto a beni tangibili come libri o CD, ma non a contenuti intangibili distribuiti su Internet.

[86] **MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE, DIPARTIMENTO PER L'INNOVAZIONE E LE TECNOLOGIE**, *Relazione Informativa Digital Rights Management*, 2004 https://www.interlex.it/testi/pdf/drmfull.pdf

2.4 DRM ED EQUO COMPENSO: IMPLICAZIONI GIURIDICHE

Il rapporto tra i sistemi DRM e l'equo compenso è molto complesso e può risultare svantaggioso per gli utenti legittimi, i quali non solo pagano l'equo compenso, ma devono anche affrontare le restrizioni imposte dai sistemi di Digital Rights Management. Come abbiamo già detto, i sistemi DRM permettono ai titolari di diritto d'autore di poter distribuire contenuti digitali utilizzando tecnologie informatiche per prevenire usi illeciti. Tuttavia, l'implementazione di questi sistemi può annullare il valore dell'equo compenso pagato dagli utenti. La liceità dei sistemi di DRM deve essere valutata facendo riferimento al quadro giuridico, che in Italia si basa sulla legge sul diritto d'autore (l. 633/41). Questa legge ha subito varie modifiche nel corso degli anni, sia per iniziativa del legislatore italiano, sia per conformarsi a norme extranazionali. Il risultato è una normativa confusa, che pone numerosi problemi interpretativi, specialmente nel caso dei DRM, dove è presente un forte squilibrio a favore dei titolari dei diritti d'autore. L'ordinamento giuridico italiano consente ai titolari di diritti d'autore e diritti connessi di applicare misure tecnologiche di protezione sulle opere dell'ingegno, come brani musicali, film, software e così via. Queste misure consistono in tecnologie, dispositivi o componenti progettati per impedire o limitare atti non autorizzati dal titolare dei diritti durante il normale utilizzo delle opere. Le misure tecnologiche di protezione possono essere rimosse solo in specifici casi previsti dalla legge, come per motivi di sicurezza pubblica o per garantire il corretto svolgimento di procedimenti amministrativi, parlamentari o giudiziari[87].

È noto che i sistemi di DRM vengono frequentemente elusi. Infatti, la legge prevede delle sanzioni penali per queste violazioni. L'art. 171-bis, L. 633/41, al comma 1, punisce chiunque duplichi abusivamente programmi per elaboratore, per trarne profitto, oppure importi, distribuisca, venda, detenga a scopo commerciale o imprenditoriale, o conceda in locazione programmi contenuti in supporti non contrassegnati dalla Società Italiana degli Autori ed Editori (SIAE). La pena prevede la reclusione da sei mesi a tre anni e una sanzione amministrativa pecuniaria da 2.582 euro a 15.493 euro. La stessa pena si applica anche se il reato riguarda qualsiasi mezzo progettato per facilitare la rimozione arbitraria o l'elusione delle misure di protezione di programmi per elaboratore. Se il fatto è di rilevante gravità, la pena minima è di due anni di reclusione e la multa di 15.493 euro. Al comma 2, invece, l'art. 171-bis, punisce chiunque, al fine di trarne profitto, riproduca, trasferisca su altro

[87] **LAVAGNINI S.,** *Il diritto d'autore nel mercato unico digitale,* Giappichelli, 2022.

supporto, distribuisca, comunichi, presenti o dimostri in pubblico il contenuto di una banca dati non contrassegnata dalla SIAE, in violazione degli art. 64 quinquies e 64 sexies, oppure esegua l'estrazione o il reimpiego della banca dati in violazione degli articoli 102 bis e 102 ter, oppure distribuisca, venda o conceda in locazione una banca dati. È prevista, in questi casi, la reclusione da sei mesi a tre anni e una sanzione amministrativa pecuniaria da 2.582 euro a 15.493 euro. Anche in questo caso, se il fatto è di rilevante gravità, la pena minima sarà di due anni e la multa di 15.493 euro[88].

L'art. 171 ter, L. 633/41, al comma 1, prevede delle sanzioni per uso non personale a fini di lucro. Se il fatto è commesso per uso non personale e a fini di lucro, alla lettera a, viene punito chiunque duplica, riproduce, trasmette o diffonde abusivamente un'opera destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri, o supporti contenenti fonogrammi o videogrammi di opere musicali, cinematografiche, audiovisive o sequenze di immagini in movimento. Verrà punito chi riproduce, trasmette o diffonde abusivamente opere letterarie, drammatiche, scientifiche, didattiche, musicali, drammatico-musicali o multimediali e chi introduce nel territorio dello stato, detiene per la vendita o distribuzione, distribuisce, vende, noleggia, cede, proietta in pubblico, trasmette a mezzo televisivo o radiofonico duplicazioni o riproduzioni abusive di opere. Le stesse sanzioni sono previste per chi detiene per la vendita, distribuzione, commercio, noleggio o cede videocassette, musicassette o supporti contenenti fonogrammi o videogrammi di opere musicali, cinematografiche, audiovisive o sequenze di immagini in movimento, senza contrassegno SIAE o con contrassegno contraffatto o alterato. L'art. prevede delle punizioni anche per chi ritrasmette o diffonde un servizio criptato senza accordo con il legittimo distributore, per chi introduce nel territorio dello Stato, detiene per la vendita o distribuzione, distribuisce, vende, noleggia, cede, promuove, installa dispositivi di decodificazione speciale che consentono l'accesso a un servizio criptato senza pagamento. Infine, si prevedono ulteriori sanzioni per chiunque fabbrichi, importi, distribuisca, venda, noleggia, ceda, pubblicizzi o detenga per scopi commerciali attrezzature progettate per eludere misure tecnologiche di protezione o rimuova o alteri abusivamente le informazioni elettroniche poste sulle opere dell'ingegno. La pena prevede la reclusione da sei mesi a tre anni e una multa da duemila euro a quindici mila euro[89].

[88] **VALERIO E. e ALGARDI Z.,** *Il diritto d'autore. Commento teorico-pratico alla nuova legge italiana 22 aprile 1941, n. 633,* Milano, Giuffrè Editori, 1943.

[89] *Ibidem*

Al comma 2, sono previste sanzioni per abusi su larga scala. Viene punito chiunque riproduca, duplichi, trasmetti, diffonda, venda o ceda oltre cinquanta copie di opere tutelate dal diritto d'autore, chiunque comunichi al pubblico in un sistema di reti telematiche un'opera protetta dal diritto d'autore a fini di lucro, chiunque eserciti in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate e, infine, chiunque promuova o organizzi attività illecita. Anche in questo caso è prevista la reclusione da uno a quattro anni e una sanzione amministrativa da duemila euro a quindicimila euro. Il comma 3, prevede delle circostanze attenuanti secondo le quali la pena è diminuita se il fatto è di particolare tenuità. Al comma 4, invece, sono previste delle pene accessorie, secondo cui, le condanne per uno dei reati menzionati al comma 1 e al comma 2, comportano pene accessorie e di conseguenza, la sospensione di concessioni o autorizzazioni per un anno. Inoltre, può comportare la pubblicazione della sentenza e la sospensione della concessione o autorizzazione di diffusione radiotelevisiva per un anno. Infine, il comma 5, prevede la destinazione degli importi delle sanzioni, per cui gli importi derivanti dalle sanzioni pecuniarie sono versati all'Ente nazionale di previdenza ed assistenza per i pittori e scultori, musicisti, scrittori ed autori drammatici. Infine, sono previste le sanzioni per uso abusivo di opere protette e misure tecnologiche all'art. 174 ter, l. 633/41. L'art. prevede al comma 1, delle sanzioni per uso abusivo e violazione delle misure di protezione tecnologiche. Verrà punito chiunque utilizzi abusivamente, anche via etere o via cavo, chiunque duplici, metta a disposizione, riproduca, in tutto o in parte, con qualsiasi procedimento, chiunque si avvalga di strumenti atti ad eludere le misure tecnologiche di protezione, chiunque acquisti o noleggi supporti o servizi audiovisivi, fonografici, informatici o multimediali non conformi alla legge e, infine, chiunque possieda attrezzature, prodotti o componenti atti ad eludere misure di protezione tecnologiche. È prevista una sanzione pecuniaria amministrativa di 154 euro e, inoltre, sono previste delle sanzioni accessorie della confisca del materiale e della pubblicazione del provvedimento su un giornale quotidiano a diffusione nazionale. Si noti che la sanzione si applica a condizione che il fatto non concorra con i reati previsti dagli articoli 171, 171-bis, 171-ter, 171-quater, 171-quinquies, 171-septues e 171-octies della legge. Al comma 2, l'art. ci dice che in caso di recidiva o se il fatto è considerato grave per la quantità delle violazioni, per la quantità delle copie acquistate o noleggiate o per la quantità di opere o materiali protetti resi potenzialmente accessibili in maniera abusiva, allora è prevista una sanzione pecuniaria amministrativa aumentata fino a cinquemila euro, la confisca degli strumenti e del materiale, la pubblicazione del provvedimento su duo o più giornali quotidiani a diffusione nazionale o su uno o più periodici specializzati nel settore dello spettacolo, la revoca della concessione o

dell'autorizzazione di diffusione radiotelevisiva, la revoca dell'autorizzazione per l'esercizio dell'attività produttiva o commerciale se si tratta di attività imprenditoriale[90].

La legge stabilisce che la presenza di sistemi DRM non può impedire al legittimo proprietario di un'opera di effettuare una copia privata per uso personale. Di conseguenza, i detentori dei diritti d'autore devono garantire che questa possibilità sia effettivamente praticabile (art. 71-sexies, co. 4, l. 633/41). Per compensare i titolari dei diritti d'autore per l'uso privato delle loro opere, la legge introduce il cosiddetto equo compenso. Quest'ultimo sarebbe una somma aggiunto al prezzo di dispositivi che permettono la registrazione di contenuti audio o video (come masterizzatori, videoregistratori, radioregistratori e periferiche di memorie come le schede di memoria) e sui relativi supporti vergini. Tale somma viene raccolta dalla SIAE, la quale successivamente la distribuisce ai titolari dei diritti d'autore. Nel caso del software, la legge prevede che la l'utente legittimo di un programma possa realizzarne una copia di riserva, qualora questa sia necessaria per l'utilizzo del programma stesso (art. 64-ter, co.2, l. 633/41). Tuttavia, è ritenuto paradossale che chi utilizza un masterizzatore, un videoregistratore o una fotocamere digitale debba compensare altri soggetti. Infatti, sembra quasi assurdo pagare ad altri una somma per i propri diritti d'autore. In ogni caso, però, solo alcune categorie possono ottenere il rimborso di questo compenso come ad esempio le imprese e le pubbliche amministrazioni. Ai consumatori non è possibile ottenere questo privilegio. Inoltre, quando i dispositivi e i supporto sono utilizzati per creare una copia analogica di un supporto digitale, si finisce per pagare più volte l'equo compenso ottenendo così una copia con una bassa qualità dell'opera acquistata legalmente[91]. Dal punto di vista giuridico, la coesistenza dell'equo compenso e dei sistemi di DRM è inaccettabile. Di fatti, la presenza dell'equo compenso dovrebbe rendere illegittimi questi sistemi, in quanto, si costringe un soggetto a pagare sempre e comunque senza però mai ottenere una contropartita adeguata. Il problema principale è che la struttura normativa italiana è inadeguata e datata e ancora più grave la legge 633/41 è sbilanciata a favore dei titolari dei diritti d'autore a scapito dei legittimi possessori.

[90] **VALERIO E. e ALGARDI Z.,** *Il diritto d'autore. Commento teorico-pratico alla nuova legge italiana 22 aprile 1941, n. 633,* Milano, Giuffrè Editori, 1943.

[91] **GAUDENZI SIROTTI A.,** *Il nuovo diritto d'autore. La tutela della proprietà intellettuale nell'era dell'intelligenza artificiale,* 12 ed., Maggioli Editore, 2024.

III. IL CONTRASTO ALLA PIRATERIA ONLINE: ASPETTI LEGALI E PROCEDURE

1. LE OPERE TUTELATE DAL DIRITTO D'AUTORE CON PARTICOLARE RIFERIMENTO A QUELLE NEL MONDO DIGITALE

Fino a non molto tempo fa, nell'organizzazione universitaria italiana, il diritto d'autore non esisteva come materia autonoma. Solo con l'introduzione della riforma che ha portato a un sistema basato su esami più brevi e numerosi, insieme a crediti formativi, il diritto d'autore ha iniziato a essere insegnato in alcuni corsi universitari come disciplina a sé stante. Prima di questa riforma, il diritto d'autore veniva studiato all'interno del Diritto Industriale. Questa materia tradizionalmente copriva anche i brevetti, i marchi, la concorrenza tra imprese, il diritto della pubblicità, e più recentemente, il diritto legato alle nuove tecnologie informatiche, come i contratti telematici, la privacy e la gestione delle reti. Alcuni giuristi, invece, preferiscono raggruppare il diritto d'autore, dei brevetti e quello dei marchi sotto l'etichetta di Diritto della proprietà intellettuale. Tuttavia, questa scelta viene criticata da altri per ragioni di carattere dogmatico e dottrinale, in quanto ritengono che il concetto di proprietà intellettuale sia una forzatura concettuale. Proprio per questo motivo, infatti, si tende a parlare più frequentemente di proprietà industriale, anche se questo termine non riesce a coprire tutte le attività a cui si rivolgono le tre aree tematiche menzionate. Inoltre, si sente sempre più spesso parlare di Diritto della concorrenza, il quale rappresenta un concetto ancora più ampio rispetto a quello di Diritto industriale. Il diritto della concorrenza, infatti, non si limita ai rapporti giuridici strettamente legati all'attività industriale, ma abbraccia anche tutto il settore dei beni immateriali e il mercato dei servizi[92].

Questa strutturazione sistematica e la divisione degli ambiti tematici si riflettono chiaramente nella normativa vigente. Fino a qualche anno fa, la situazione legislativa era la seguente: il Regio Decreto n. 1127 del 1939, noto come "Testo delle disposizioni legislative in materia di brevetti per invenzioni industriali", costituiva il riferimento principale per la regolamentazione dei brevetti; la legge n. 633 del 1941, intitolata "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio", la quale regolava il diritto d'autore; e il Regio Decreto n. 929 del 1942, "Testo sulle

[92] **ALIPRANDI S.,** *Capire il copyright. Percorso guidato nel diritto d'autore,* Ledizioni, 2012

disposizioni legislative in materia di marchi registrati", il quale, invece, disciplinava la norma sui marchi. Nel 2005, tuttavia, una riforma significativa ha unificato le normative riguardanti brevetti e marchi in un unico testo legislativo comunemente chiamato Codice della proprietà industriale. Questo nuovo quadro normativo è stato introdotto dal Decreto Legislativo n. 30 del 2005. In materia di diritto d'autore, il riferimento normativo principale rimane la L. n. 633/41, anche nominata LDA (Legge Diritto Autore). Nonostante questa legge sia in vigore dal 1941, è stata sottoposta a varie revisioni e integrazioni nel corso degli anni, soprattutto a seguito delle direttive europee. Tra le modifiche più significative si possono menzionare il Decreto Legislativo n. 518/1992, il quale ha recepito la direttiva 91/250/CEE sulla tutela giuridica dei programmi per elaboratore, il Decreto Legislativo n. 154/1997 che ha attuato la direttiva 93/98/CEE per armonizzare la durata della protezione del diritto d'autore e dei diritti connessi, il Decreto Legislativo n. 169/1999 il quale ha implementato la direttiva 96/9/CEE riguardante la tutela giuridica delle banche dati, la Legge n. 248/2000 che ha introdotto nuove norme per la protezione del diritto d'autore, il Decreto Legislativo n. 95/2001, il quale ha recepito la direttiva 98/71/CE sulla protezione giuridica dei disegni e modelli, il Decreto Legislativo n. 68/2003 il quale ha attuato la direttiva 2001/29/CE per l'armonizzazione di alcuni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, ed infine, il Decreto Legislativo n. 140/2006 il quale ha dato attuazione alla direttiva 2004/48/CE sul rispetto dei diritti di proprietà intellettuale[93].

Chi desidera proteggere un'opera della propria creatività spesso si chiede come poter ottenere i diritti sulla propria opera. Questo aspetto può generare confusione, poiché è comune credere che i diritti d'autore si acquisiscano tramite una formalità specifica, come il deposito dell'opera presso la SIAE. A differenza dei brevetti, che richiedono una registrazione formale presso uffici competenti, il diritto d'autore è automaticamente attribuito all'autore nel momento in cui l'opera viene creata. Questo principio è stabilito dall'art. 2576 c.c., che riprende l'art. 6 della L. n. 633/41. L'art. 2576 c.c., e di conseguenza l'art. 6 LDA, spiega che il diritto d'autore sorge con la creazione dell'opera, considerata come un'espressione particolare del lavoro intellettuale. Pertanto, l'intervento della SIAE o di altri enti certificatori non è necessario per acquisire i diritti d'autore. Qualsiasi opera che rispetti i requisiti minimi di originalità e creatività è automaticamente protetta dalla legge sul diritto d'autore, e l'autore gode di tutti i diritti previsti. La legge sul diritto d'autore, all'art. 105, prevede l'obbligo di depositare una copia dell'opera presso un ufficio istituito presso la Presidenza del Consiglio. Tuttavia,

[93] **AUTERI P.,** *Diritto di autore,* in AA.VV., *Il diritto industriale,* 7 ed., Giappichelli, 2023, p. 649 ss.

l'art. 106 chiarisce che il mancato deposito non pregiudica né l'acquisizione né l'esercizio dei diritti d'autore[94].

All'art. 2 e successivi della legge sul diritto d'autore viene fornita una classificazione delle opere tutelate, che non deve essere considerata come un elenco esaustivo. Questo significa che i principi del diritto d'autore possono estendersi anche a nuove forme di creatività non specificamente menzionate dalla legge, purché presentino caratteristiche proprie delle opere dell'ingegno. L'art. 2 della legge sul diritto d'autore definisce le categorie di opere che beneficiano della protezione giuridica. Tra queste, rientrano le opere letterarie, scientifiche, didattiche, religiose, che possono essere sia scritte che orali. Sono incluse anche le opere e le composizioni musicali, sia con che senza parole, così come le opere drammatico-musicali e le variazioni musicali considerate originali. La legge tutela inoltre le opere coreografiche e pantomimiche, insieme alle opere di scultura, pittura, disegno, incisione e altre arti figurative simili, comprensive della scenografia. Sono protetti anche i disegni e le opere di architettura, nonché le opere cinematografiche, siano esse mute o sonore. Le opere fotografiche e quelle realizzate con tecniche analoghe alla fotografia sono anch'esse protette. I programmi per elaboratore sono inclusi nella tutela purché siano espressioni originali della creazione intellettuale dell'autore. Le banche dati, intese come raccolte sistematiche di opere, dati o altri elementi, sono protette se accessibili tramite mezzi elettronici o altri metodi. Infine, sono comprese le opere del disegno industriale che mostrano carattere creativo e valore artistico. Tuttavia, alcune opere moderne, come quelle create grazie alle nuove tecnologie informatiche e telematiche possono combinare caratteristiche di più categorie tradizionali e sono spesso designate con il termine generico di opere multimediali[95]. L'art. 3 LDA elenca altre classificazioni delle opere tutale. Tra queste vi sono le opere collettive, le quali sono costituite dalla combinazione di opere o parti di opere che, pur mantenendo un carattere di creazione autonoma, sono riunite attraverso una selezione e un coordinamento mirati a un fine specifico, che può essere letterario, scientifico o artistico. Il successivo art. 4 riguarda le elaborazioni creative, ovvero quelle attività di rielaborazione di opere esistenti che presentano un contributo creativo significativo e autonomo. Queste includono traduzioni in altre lingue, trasformazioni in forme letterarie o artistiche diverse, modifiche e aggiunte che costituiscono una revisione sostanziale dell'opera originale, nonché adattamenti, riduzioni, compendi e variazioni che non sono considerate opere originali. Infine, l'art. 10 si riferisce alle opere in comunione, ovvero

[94] **UBERTAZZI L. C.,** *I diritti d'autore e connessi. Scritti,* 2 ed., Giuffrè Editore, 2003
[95] **AUTERI P.,** *Diritto di autore,* in AA.VV., *Il diritto industriale,* 7 ed., Giappichelli, 2023, p. 649 ss.

quelle create con il contributo indistinguibile e inscindibile di più persone. In questo caso, salvo prova contraria, il diritto d'autore appartiene a tutti i coautori seguendo le regole della comunione[96].

Ai giorni d'oggi, vi è un quesito molto importante a cui bisogna saper rispondere in maniera esaustiva: quali sono le opere tutelate dal diritto d'autore nel mondo digitale?

Nel mondo digitale, il concetto di copyright e diritto d'autore è essenziale per garantire la protezione e il rispetto delle opere creative online. Copyright e diritto d'autore spesso e volentieri vengono utilizzati come sinonimi e di fatti si riferiscono ad un insieme di leggi e principi che regolano l'uso e la distribuzione delle opere intellettuali. Il termine copyright è particolarmente comune nei sistemi giuridici anglosassoni e indica i diritti legali che autori, artisti e detentori di proprietà intellettuale possiedono su opere creative, come testi, immagini, musica, film e software. Il copyright viene automaticamente attribuito all'autore al momento della creazione dell'opera e rimane in vigore per un periodo determinato dopo la sua morte, generalmente per 70 anni. Questo diritto conferisce all'autore il controllo sulla riproduzione dell'opera, consentendogli di copiare l'opera stessa, e sulla sua distribuzione, permettendogli di vendere o distribuire copie. Inoltre, il copyright include il diritto di eseguire pubblicamente l'opera, come nel caso di musica o rappresentazioni teatrali, e di esibirla pubblicamente, come avviene per film e opere d'arte. Infine, l'autore ha anche il diritto di creare opere derivate, cioè nuove opere basate su quella originale[97].

Nel contesto odierno, il diritto d'autore acquisisce un'importanza particolarmente rilevante a causa della facilità con cui le opere possono essere condivise e riprodotte online. Questo scenario solleva numerosi interrogativi legali ed etici riguardanti la protezione della proprietà intellettuale, la privacy e la libertà di espressione. A livello globale, diverse normative e trattati regolano la protezione delle opere nel mondo digitale. Tra questi, la Convenzione di Berna stabilisce gli standard internazionali per la tutela delle opere letterarie e artistiche, mentre il Digital Millennium Copyright Act (DMCA) si occupa della protezione delle opere digitali negli Stati Uniti. Nel contesto del web, molte piattaforme hanno sviluppato strumenti per tutelare il copyright. Youtube, ad esempio, utilizza il sistema Content ID per identificare e bloccare i contenuti protetti da copyright che vengono caricati senza autorizzazione. Altri strumenti tecnologici, come gli algoritmi di rilevamento dei contenuti pirata, l'autenticazione a due fattori e le app di autenticazione, contribuiscono a rafforzare la

[96] **UBERTAZZI L. C e AMMENDOLA M.,** *Il diritto d'autore,* UTET Università, 1993
[97] **AUTERI P.,** *Diritto di autore,* in AA.VV., *Il diritto industriale,* 7 ed., Giappichelli, 2023, p. 649 ss.

protezione dei diritti d'autore. Nonostante queste misure avanzate, il dibattito su quanto il web riesca effettivamente a garantire una protezione adeguata del copyright è ancora in corso. La vasta accessibilità a una grande quantità di contenuti tramite internet offre indubbi vantaggi, ma crea anche sfide significative per l'applicazione e l'enforcement dei diritti di proprietà intellettuale. La facilità con cui i contenuti possono essere condivisi e duplicati online rende difficile eliminare completamente le violazioni, e le problematiche legali nel perseguire i trasgressori si complicano ulteriormente quando le attività avvengono al di fuori delle giurisdizioni nazionali. Nonostante i progressi tecnologici, la protezione del copyright sul web rimane una questione in continua evoluzione, che richiede uno sforzo congiunto da parte di creatori, piattaforme, legislatori e utenti. La sfida di mantenere l'integrità dei diritti d'autore è un processo dinamico che richiede aggiornamenti costanti e un impegno continui da tutte le parti coinvolte[98].

Le opere digitali protette dal diritto d'autore comprendono una vasta gamma di creazioni che spaziano dal software e programmi per computer, inclusi sistemi operativi, applicazioni e giochi, fino alle banche dati, che sono organizzate in modo sistematico e accessibili attraverso vari mezzi elettronici. Anche le opere multimediali che combinano testo, audio, video, immagini e animazioni, rientrano nella protezione del diritto d'autore; esempi tipici sono i videogiochi, le presentazioni interattive e i prodotti educativi multimediali. Le fotografie digitali, scattate e conservate in formato digitale, sono anch'esse tutelate, così come la musica distribuita in formato digitale, ad esempio file MP£ o attraverso servizi di streaming. I libri elettronici e le pubblicazioni digitali, accessibili online o scaricabili, rientrano nel campo della protezione del copyright. Analogamente, i video e i filmati digitali, che includono cortometraggi e film distribuiti online, sono coperti dal diritto d'autore. Anche le opere grafiche e le illustrazioni create o diffuse in formato digitale godono di protezione. Così come i contenuti presenti sui siti web, quali testi, immagini, layout, e altri elementi creativi. Tutte queste opere, per essere protette, devono soddisfare i requisiti di originalità e creatività previsti dalla legge[99].

2. LE NORME E GLI STRUMENTI DI TUTELA CIVILISTICI

[98] **UBERTAZZI L. C.,** *Diritto d'autore. Estratto da Commentario breve alle leggi su proprietà intellettuale e concorrenza,* 4 ed., CEDAM, 2007.

[99] **AUTERI P.,** *Diritto di autore,* in AA.VV., *Il diritto industriale,* 7 ed., Giappichelli, 2023, p. 649 ss.

Il diritto d'autore è regolamentato da un insieme di norme che mirano a proteggere le opere dell'ingegno. Esso cerca di garantire agli autori il controllo sulla diffusione e l'utilizzo delle loro creazioni. In Italia, la legge fondamentale in materia è la L. n. 633/41, conosciuta, come abbiamo già detto, come Legge sul Diritto d'Autore (LDA), la quale disciplina i diritti esclusivi riconosciuti agli autori e ad altri soggetti, come gli artisti, i produttori e gli editori. Le principali norme del diritto d'autore riguardano la protezione delle opere originali, che includono opere letterarie, musicali, artistiche, cinematografiche, fotografiche, software, banche dati e altre espressioni creative. Le opere sono protette automaticamente dal momento della loro creazione, senza necessità di registrazione formale. I diritti conferiti agli autori si suddividono principalmente in due categorie: diritti morali e diritti patrimoniali. I diritti morali sono inalienabili e perpetui, mentre quelli patrimoniali sono di natura economica[100].

Il funzionamento del diritto d'autore si basa sull'attribuzione di un valore economico e commerciale allo sfruttamento delle opere dell'ingegno. Questo sfruttamento è regolato da una serie di diritti patrimoniali che la legge conferisce all'autore o, in alcuni casi, ad altri soggetti. Tali diritti, denominati diritti di utilizzazione economica, nell'ordinamento italiano operano come diritti esclusivi e sono disciplinati anche loro dalla L. n. 633/41 negli articoli compresi tra il 12 e il 19. Tra i principali diritti di utilizzazione economica vi è il diritto esclusivo di riproduzione, che consente all'autore di moltiplicare in copie, in tutto o in parte, la sua opere attraverso vari mezzi, come la stampa, la fotografia o la cinematografia. Inoltre, l'autore detiene il diritto esclusivo di trascrizione, che riguarda la trasformazione di un'opera orale in una scritta. Un altro diritto fondamentale è quello di esecuzione pubblica, che autorizza l'autore a eseguire, rappresentare o recitare la sua opere in pubblico, indipendentemente dal fatto che tale attività sia gratuita o a pagamento. Il diritto esclusivo di comunicazione al pubblico permette all'autore di diffondere la sua opera attraverso mezzi di trasmissione a distanza, come la radio o la televisione, inclusa la comunicazione via satellite e la ritrasmissione via cavo. Il diritto di distribuzione consente invece la messa in commercio o la circolazione dell'opera, rendendola disponibile al pubblico con qualsiasi mezzo. Inoltre, l'autore ha il diritto esclusivo di tradurre la sua opera in altre lingue, di elaborarla e modificarla, e di pubblicarla in raccolta. Inoltre, il diritto esclusivo di noleggio e prestito garantisce all'autore la possibilità di autorizzare il noleggio della sua opera. Tutti questi diritti di utilizzazione economica durano per tutta la vita dell'autore e fino al termine del settantesimo anno solare dopo la sua morte, come stabilito

[100] **AUTERI P.,** *Diritto di autore,* in AA.VV., *Il diritto industriale,* 7 ed., Giappichelli, 2023, p. 649 ss.

dall'articolo 25 della legge sul diritto d'autore. La durata dei riditti di utilizzazione economica delle opere protette dal diritto d'autore, che è riconosciuta anche a livello internazionale, è stata estesa con la riforma del 1996. Prima di questa modifica, la legge italiana prevedeva che tali diritti durassero cinquant'anni dalla morte dell'autore. Con la riforma, il termine è stato allungato a settant'anni dalla morte dell'autore, allineandosi agli standard internazionali. La legge prevede inoltre alcune particolarità. Ad esempio, l'art. 26, comma 1, stabilisce che per le opere realizzate da più autori, come le opere in comunione o quelle drammatico-musicali, coreografiche e pantomimiche, la durata dei diritti di utilizzazione economica viene calcolata sulla base della vita del coautore che muore per ultimo. Al contrario, per le opere collettive, in cui i contributi degli autori sono distinti e separabili, l'art. 26, comma 2, prevede che la durata dei diritti di utilizzazione economica venga determinata in base alla vita di ciascun collaboratore singolarmente. Infine, l'art. 27 disciplina la durata dei diritti per le opere anonime o pseudonime, nelle quali l'autore originario dei diritti non è identificabile direttamente. Queste disposizioni garantiscono che il diritto d'autore sia adeguatamente tutelato in diverse circostanze, riflettendo la varietà di situazioni in cui possono essere create le opere artistiche e intellettuali.[101]

La legge del diritto d'autore prevede, poi, i diritti morali. Questi diritti appartengono alla sfera personale dell'autore e apportano all'opera creata un valore aggiunto, un valore di tipo morale strettamente collegato al rispetto dell'onore e della reputazione dell'autore. Sono diritti perpetui, di fatti dopo la morte dell'autore dell'opera, questi vengono gestiti dagli eredi. Inoltre, non possono essere ceduti e sono indisponibili. L'autore non può liberarsi di questi diritti e grazie ad essi può sempre mantenere il controllo sull'opera, anche nel caso in cui abbia ceduto i diritti di sfruttamento economico. I diritti morali sono previsti dagli artt. 20-24 della Legge sul Diritto d'autore. Sono previsti il diritto a rivendicare la paternità dell'opera, anche nel caso in cui l'autore sia anonimo o abbia uno pseudonimo e il diritto di opporsi a eventuali mutilazioni dell'opera che vadano a pregiudicare l'onore e la reputazione dell'autore. In più, è previsto il diritto di ritirare l'opera dal commercio per gravi ragioni morali. Questo diritto è disciplinato dagli artt. 142 e 143 LDA. L'art. 142 LDA, al comma I, ci dice, infatti, che l'autore ha il diritto di ritirare l'opera dal commercio e ha, di conseguenza, l'obbligo di indennizzare coloro che hanno acquistato i diritti di riprodurre, diffondere, eseguire, rappresentare o spacciare l'opera medesima. Questo diritto è personale e non può essere trasmesso. L'ordinamento giuridico prevede, poi, i diritti connessi. Essi sono legati a

[101] **AUTERI P.,** *Diritto d'autore,* in AA.VV., *Il Diritto industriale,* 7 ed., Giappichelli, 2023, p. 649 ss.

soggetti diversi dall'autore dell'opera, i cui diritti sono però connessi all'esercizio dei diritti d'autore in quanto si riferiscono ad importanti attività intellettuali e commerciali. I diritti connessi vengono disciplinati dagli artt. 72 e seguenti e riguardano l'incisione e la produzione di fonogrammi, la produzione di opere audiovisive e cinematografiche, l'emissione radiofonica e televisiva e artisti interpreti ed esecutori[102].

Nel Titolo III, Capo III, la legge sul diritto d'autore prevede un sistema articolato di protezioni e sanzioni civili per salvaguardare i diritti del titolare in caso di violazioni. Queste misure sono comprese negli artt. 156-170 e sono state aggiornato dal Decreto Legislativo del 16 marzo 2006, n. 140, il quale ha recepito la Direttiva 2004/48/CE relativa alla tutela dei diritti di proprietà intellettuale. Il sistema di protezione si suddivide in due parti principali: la prima, che va dall'artt. 156-167 e si concentra sulla difesa dei diritti di utilizzazione economica dell'opera; la seconda, che include gli artt. 168-170, riguarda invece la tutela dei diritti morali dell'autore. Queste due categorie di diritti possono essere difese separatamente o congiuntamente, nel caso in cui una violazione incida su entrambe. L'art. 168 prevede infatti, che, qualora sia lesa la sfera patrimoniale che quella morale, l'azione legale può tutelare entrambi i diritti, purché sia compatibile con la natura del diritto morale. Inoltre, l'art. 19 LDA stabilisce che il ricorso per la difesa di uno dei diritti patrimoniali non impedisce di esercitare in maniera esclusiva gli altri diritti connessi. Le azioni legali contemplate includono l'accertamento della titolarità del diritto, la richiesta di cessazione dell'attività illecita, la rimozione e distruzione dei materiali frutto della violazione, oltre al risarcimento dei danni subiti[103].

Per quanto riguarda i diritti di utilizzazione economica sono previste dagli artt. 156, 156-bis e 156-ter LDA le azioni di accertamento e interdizione, le quali cercano di trovare un rimedio per gli autori che abbiano un motivo di temere la violazione di un diritto a loro spettante o che vogliano impedire la continuazione di una violazione già avvenuta. L'autore in questi casi può agire in giudizio per ottenere l'accertamento del diritto e la cessazione della violazione. Quindi, con l'azione di accertamento i titolari del diritto d'autore possono ottenere una pronuncia di accertamento, mentre con l'azione di interdizione il titolare mira alla cessazione dell'illecito attraverso una pronuncia giudiziale. Le sanzioni sono regolate dalle norme del codice di procedura civile. Entrambe le azioni possono essere esercitate anche quando il timore di una violazione è basato su elementi concreti e non solo dopo che la violazione sia effettivamente avvenuta. In ogni caso, questa funzione si

[102] **AUTERI P.,** *Diritto d'autore,* in AA.VV., *Il Diritto industriale,* 7 ed., Giappichelli, 2023, p. 649 ss.
[103] **D'AMMASSA G.,** *Le difese e le sanzioni civili,* 2014, disponibile su dirittodautore.it

caratterizza per la sua funzione di prevenzione, oltre ad avere lo scopo di giungere ad una condanna da parte dell'organo giudicante[104].

L'art. 156-bis, relativo al processo di discovery, prevede che una parte possa ottenere dal giudice l'ordine di esibizione di documenti, elementi o informazioni detenuti dalla controparte, qualora abbia presentato prove solide che rendano plausibili le proprie richieste. Se questi indizi suggeriscono la violazione di diritti protetti dalla legge, il giudice può ordinare la presentazione di tali prove. Inoltre, la parte richiedente può chiedere al giudice di obbligare la controparte a fornire informazioni utili per identificare i soggetti coinvolti nella produzione e distribuzione di prodotti o servizi che violano i diritti in questione. Nel caso in cui la violazione sia avvenuta su scala commerciale, il giudice può anche disporre, su richiesta della parte, l'esibizione di documentazione bancaria, finanziaria e commerciale in possesso della controparte. Durante questo processo, il giudice è tenuto a prendere le misure necessarie per proteggere le informazioni riservate, assicurandosi che la controparte sia ascoltata. Infine, il giudice può trarre prove dalle risposte fornire dalle parti o dall'eventuale rifiuto ingiustificato di ottemperare agli ordini del tribunale. L'art. 156-ter della legge sul diritto d'autore, invece, stabilisce che l'autorità giudiziaria, sia in sede cautelare che di merito, può ordinare, su richiesta giustificata e proporzionata del richiedente, di ottenere informazioni relative all'origine e alle reti di distribuzione di merci o servizi che violano i diritti previsti dalla legge. Questo rodine può essere emesso non solo contro l'autore diretto della violazione, ma anche contro la persona che: a) sia stata trovata in possesso di merci che violano un diritto su scala commerciale; b) sia stata sorpresa a utilizzare servizi coinvolti nella di un diritto su scala commerciale; c) sia stata sorpresa a fornire, sempre su scala commerciale, servizi utilizzati in attività che violano un diritto; d) sia stata indicata come coinvolta nella produzione, fabbricazione o distribuzione di tali prodotti o nella fornitura di servizi associati alla violazione. Le informazioni richieste possono includere anche il nome e l'indirizzo di produttori, fabbricanti, fornitori e altri detentori precedenti di prodotti o servizi, nonché grossisti e dettaglianti. Inoltre, si può chiedere di ottenere dati riguardanti le quantità prodotto, fabbricate, consegnate, ricevute o ordinate, e i prezzi dei prodotti o servizi in questione. Queste informazioni sono acquisite tramite interrogatori dei soggetti coinvolti, specificamente individuati dalla parte richiedente, la quale deve anche indicare i fatti specifici su cui ciascun soggetto deve essere interrogato[105].

[104] **CUNEGATTI B.,** *Manuale del diritto d'autore,* Editrice Bibliografica, 2020.
[105] **D'AMMASSA G.***, Le difese e le sanzioni civili,* 2014 disponibile su dirittodautore.it

L'art. 157 LDA prevede la proibizione della rappresentazione o esecuzione di un'opera adatta a pubblico spettacolo. È previsto un intervento amministrativo tramite una richiesta indirizzata al Prefetto. Si mira all'ottenimento della proibizione della rappresentazione o esecuzione ogni qual volta manchi la prova scritta del consenso prestato dall'autore. Questo provvedimento ha la natura di una misura cautelare, concepita per proteggere i diritti delle parti in attesa di eventuali provvedimenti successivi da parte dell'autorità giudiziaria. L'obiettivo è di impedire ulteriori danni o violazioni nel periodo precedente alla decisione finale, garantendo che le informazioni cruciali siano raccolte e preservate per il corretto svolgimento del processo[106].

Tra i diritti di utilizzazione economica sono previsti, poi, dagli artt. 158, 159 e 160 LDA le azioni di distruzione di rimozione. L'art. 158 prevede azioni finalizzate alla distruzione dei prodotti utilizzati in violazione dei diritti e alla rimozione delle condizioni che hanno determinato tale violazione. Queste azioni, che possono essere attivate separatamente o congiuntamente, mirano a garantire che il titolare dei diritti possa godere pienamente di questi ultimi, andando così a ripristinare la situazione antecedente alla violazione. Possono essere richieste anche nei confronti di terzi che detengano i prodotti contraffatti, indipendentemente dalla loro buona fede. L'art. 159 disciplina le modalità di esecuzione di queste azioni, specificando che possono riguardare esclusivamente gli esemplari o copie illecitamente riprodotte o diffuse, nonché gli apparecchi impiegati per la riproduzione o diffusione, a condizione che questi non siano utilizzati prevalentemente per scopi legittimi. Se i prodotti in questione possono essere modificati per un utilizzo lecito, il giudice può ordinarne il ritiro temporaneo dal mercato, con la possibilità di reinserirli successivamente, una volta apportate le modifiche necessarie a garantire il rispetto dei diritti d'autore. Inoltre, se una parte dell'apparecchio può essere utilizzata per scopi legittimi, l'interessato può richiedere, a proprie spese, che questa parte venga separata per il proprio uso. Nel caso in cui l'apparecchio abbia un valore artistico o scientifico significativo, il giudice può disporne il deposito in un museo pubblico. Il danneggiato, titolare dei diritti, può inoltre richiedere che i prodotti soggetti a distruzione gli siano assegnati ad un prezzo stabilito, a titolo di risarcimento. Bisogna ricordare che, in ogni caso, i provvedimenti di distruzione non si applicano agli esemplari o alle copie contraffatte acquistate in buona fede per uso personale. L'applicazione di queste misure deve essere, ovviamente, proporzionata alla gravità della violazione e tenere conto degli interessi dei terzi coinvolti. Inoltre, la rimozione e la distruzione non possono essere richieste se l'opera è nell'ultimo anno di protezione

[106] **CUNEGATTI B.,** *Manuale del diritto d'autore,* Editrice Bibliografica, 2020.

(art. 160 LDA), ma può essere ordinato il sequestro fino alla scadenza del termine di protezione. Se i danni causati dalla violazione sono stati risarciti, il sequestro può essere autorizzato anche prima della scadenza[107].

Sempre l'art. 158, comma 2, LDA prevede la possibilità di intraprendere un'azione legale per ottenere il risarcimento del danno subito. Affinché il risarcimento venga riconosciuto, è necessario che il danno esista realmente, e spetta al soggetto leso l'onere di dimostrarlo. Inoltre, è richiesto che il comportamento illecito sia stato doloso o colposo, e che il danno causato abbia avuto un impatto di natura patrimoniale. Il danno morale, invece, secondo quanto stabilito dall'art. 2059 c.c., può essere risarcito solo se è conseguenza di un atto penalmente rilevante. È indispensabile anche dimostrare il nesso causale tra il comportamento illecito e il danno subito, applicando i principi generali della responsabilità civile previsti dagli artt. 2043 e seguenti del Codice Civile. Il risarcimento viene calcolato in base alle disposizioni degli artt. 1223, 1226 e 1227 c.c., e il lucro cessante, quindi il guadagno che il danneggiato non ha potuto realizzare. Questo viene valutato dal giudice ai sensi dell'art. 2056, comma 2, c.c., considerando anche gli utili che l'autore della violazione ha ottenuto in maniera illecita. Il giudice ha inoltre la facoltà di determinare il risarcimento in via forfettaria, basandosi sull'importo che l'autore della violazione avrebbe dovuto pagare se avesse richiesto l'autorizzazione per l'utilizzo del diritto. Ciò viene effettuato seguendo il criterio del *prezzo del consenso.* Questo criterio era già pienamente utilizzato dalla giurisprudenza italiana, ancor prima di essere introdotto formalmente attraverso la Direttiva 2004/48/CE. Esso rappresenta, infatti, un parametro consolidato per la liquidazione dei danni. Infine, sono dovuti anche i danni non patrimoniali, così come stabilito dall'art. 2059 c.c. L'azione per il risarcimento del danno deve essere esercitata entro cinque anni dal giorno in cui il fatto dannoso si è verificato, secondo quanto stabilito dall'art. 2947 c.c. Inoltre, è ammesso il concorso tra l'azione di risarcimento del danno e le azioni di distruzione e rimozione, qualora una delle due non sia sufficiente ad eliminare completamente gli effetti della violazione.

Il nostro ordinamento prevede, poi, anche delle misure cautelari agli artt. 161, 162, 162-bus, 162-ter e 163 LDA. Questi provvedimenti cautelari sono volti a garantire la tutela dei diritti di utilizzazione economica e la preservazione delle prove di eventuali violazioni. Le misure prevedono la descrizione dettagliata di beni o oggetti che potrebbero costituire una violazione del diritto d'autore,

[107] **GRECO P. e VERCELLONE P.,** *I diritti sulle opere dell'ingegno,* in VASSALLI, *Trattato di diritto commerciale,* UTET, Torino, 1974.

al fine di raccogliere prove senza alterare lo stato delle cose, l'accertamento il quale permette di eseguire verifiche tecniche per accertare l'esistenza di una violazione, la perizia la quale viene disposta per ottenere una valutazione tecnica su questione specifiche legate alla presunta violazione, il sequestro che prevede il blocco o la conservazione di beni ritenuti in violazione del diritto d'autore o necessari per garantire il risarcimento del danno. Vi sono diverse forme di sequestro: sequestro conservativo, che tutela il diritto al risarcimento del danno e garantisce che i beni del presunto violatore non vengano dispersi e, il sequestro dei beni in violazione, che riguarda in maniera specifica i prodotti, le copie o gli apparecchi impiegati per la riproduzione o diffusione illecita. Infine, è prevista l'inibitoria, la quale consente di bloccare immediatamente le attività illecite in violazione del diritto d'autore, anche nei confronti degli intermediari che facilitano tali attività. Il giudice può richiedere le misure cautelari, le quali vengono disposte secondo le norme del codice di procedura civile. Secondo l'art. 162 LDA, riformato dalla legge n. 248/2000 e dal D. Lgs. 140/2006, i procedimenti relativi a descrizione, accertamento e perizia devono essere disciplinati dalle norme del codice di procedura di civile in materia di sequestro e istruzione preventiva. Gli atti di descrizione e sequestro sono eseguiti da un ufficiale giudiziario, spesso e volentieri con l'assistenza di periti e mezzi tecnici. Se si tratta di pubblici spettacoli, le limitazioni di giorni e ore previste dal codice di procedura civile non si applicano. Il sequestro non può essere concesso in opere derivanti dal contributo di più persone, salvo casi di particolare gravità o quando tutti i coautori sono responsabili della violazione. In casi particolarmente gravi, il giudice può anche disporre il sequestro dei proventi derivanti dall'opera o prodotto contestato. Il giudizio di merito deve iniziare entro venti giorni lavorativi o trentuno giorni di calendario dal rilascio del provvedimento cautelare, pena la perdita di efficacia dello stesso. Questa disposizione non si applica, tuttavia, ai provvedimenti d'urgenza, come quelli ex art. 700 c.p.c., i quali anticipano gli effetti della sentenza di merito. L'art. 162-ter, che è stato introdotto con la Direttiva 2004/48/CE, consente, invece, il sequestro conservativo dei beni del presunto autore della violazione, compreso il blocco dei conti bancari, nei casi di violazioni su scala commerciale, in modo da garantire il risarcimento del danno[108].

L'art. 163 LDA prevede la possibilità di chiedere l'inibitoria per bloccare qualsiasi attività che costituisca violazione del diritto d'autore. Il giudice che pronuncia l'inibitoria può anche fissare una somma dovuta per ogni futura violazione o ritardo nell'esecuzione del provvedimento. Lo stesso articolo, al comma 3, tutela i produttori di fonogrammi e gli artisti interpreti esecutori, stabilendo che

[108] **D'AMMASSA G.**, *Le difese e le sanzioni civili,* 2014, disponibile su dirittodautore.it

può essere disposta l'interdizione dall'utilizzo dei fonogrammi, oltre alla liquidazione del compenso, per un periodo da un minimo di undici giorni ad un massimo di centottanta, qualora in sede giudiziaria venga accertata il mancato pagamento del compenso relativo ai diritti citati dagli artt. 73 e 73-bis LDA. Il comma 4 dell'art. 163 LDA, stabilisce, invece, che se viene accertato in sede giudiziaria l'utilizzazione di fonogrammi che pregiudichino il produttore fonografico, ai sensi dell'art. 74 LDA, allora oltre alla interdizione definitiva del loro utilizzo, verrà emanata una sanzione amministrativa da un minimo di 260 euro ad un massimo di 5.200 euro. Infine, l'art. 166 LDA prevede un'altra misura: la pubblicazione della sentenza. Questa non sostituisce il risarcimento del danno e può essere ordinata su istanza della parte interessata o d'ufficio. Questa misura ha l'obiettivo di rendere di pubblico dominio il fatto lesivo e l'accoglimento dell'azione diretta a reprimerlo[109].

L'art. 168 LDA estende anche ai diritti morali l'applicabilità delle azioni e delle misure cautelari previste dagli artt. 156 e seguenti. I diritti morali dell'autore, come, ad esempio, il diritto alla paternità e all'integrità dell'opera, possono essere tutelati attraverso azioni come l'accertamento e l'interdizione, con la possibilità di richiedere le corrispondenti misure cautelari. Quando la violazione dei diritti morali è commessa da chi detiene i diritti economici sull'opera, il giudice deve valutare gli interessi contrapposti attentamente, in modo da garantire una protezione prioritaria ai diritti morali dell'autore. Le misure di rimozione e distruzione possono essere applicate anche ai diritti morali, ma con alcune limitazioni previste dagli artt. 169 e 170 LDA. Se la violazione riguarda il diritto di paternità, la rimozione e la distruzione dell'opera non possono essere ordinate se è possibile correggere l'errore tramite modifiche sull0opera stessa, come l'aggiunta o la soppressione delle indicazioni errate. Allo stesso modo possono essere evitate le violazioni che riguardano l'integrità dell'opera, se è possibile ripristinarla nella sua forma originaria, a spese della parte interessata. In parole povere, quindi, l'art. 168 conferma che le misure previste per i diritti di utilizzazione economica sono applicabili anche ai diritti morali, con gli adeguamenti necessari a rispettare la loro natura intrinseca.

Nelle azioni a tutela dei diritti di utilizzazione economica, è legittimato colui che detiene la titolarità del diritto violato, quindi l'autore dell'opera o i suoi aventi causa, così come stabilito dagli artt. 6 e 8 LDA. L'art. 167 LDA specifica che i diritti di utilizzazione economica posso essere fatti valere giudizialmente anche da chi ne sia in possesso legittimo o da chi possa agire in rappresentanza del titolare di tali diritti. Nel caso di opere creato con contributi distinti, come opere composte da

[109] **JARACH G. e POJAGHI A.,** *Manuale del diritto d'autore,* Ugo Mursia Editore, 2019

musica e testo letterario, la legittimazione spetta all'autore della parte musicale, secondo quanto stabiliti dall'art. 34 LDA. Se l'opera è, però, il risultato del contributo indistinguibile e inscindibile di più persone, il diritto d'autore appartiene in comune a tutti i coautori, come previsto dall'art. 10 LDA. Un autore che ha ceduto il diritto di utilizzazione economica, oggetto della violazione, mantiene il diritto di intervenire nei giudizi promossi dal cessionario, in modo da tutelare i propri interessi. Questo intervento è ammesso anche quando l'autore non detiene più la titolarità del diritto per motivi diversi da una cessione formale, come nel caso di un'opera realizzata su commissione o in base a un rapporto di lavoro subordinato. Un'ulteriore legittimazione è attribuita alla SIAE – Società Italiana degli Autori ed Editori, come stabilito dall'art. 164 LDA. La SIAE e altri enti di diritto pubblico, indicati negli artt. 180 e 184 LDA, possono promuovere azioni a tutela dei diritti d'autore senza necessità di mandato, basandosi solo sulla qualità del funzionario che rappresenta l'ente. In più, questi enti sono esonerati dall'obbligo di prestare cauzione per l'esecuzione di atti che normalmente la richiederebbero. La SIAE ha anche l'autorità di designare funzionari autorizzati a compiere attestazioni di credito relative al diritto d'autore. Tali attestazioni hanno efficacia di titolo esecutivo, ai sensi dell'art. 474 c.p.c. Come abbiamo già detto, la tutela del diritto morale è alienabile e la legittimazione attiva spetta all'autore. In caso di opere create con contributi distinti, ciascun autore ha il diritto di agire a difesa del proprio contributo. Se i contributi sono invece inscindibili e indistinguibili, ciascun coautore può esercitare la difesa individualmente, come previsto dall'art. 10, comma 3, LDA[110].

3. LE NORME E GLI STRUMENTI DI TUTELA PENALISTICI

La violazione del diritto d'autore rappresenta un fenomeno complesso con conseguenze significative tanto per gli autori quanto per il mercato. Quando un'opera viene plagiata, contraffatta o sfruttata senza l'autorizzazione del titolare dei diritti, non solo si va a danneggiare l'autore, ma si va a compromettere anche il sistema economico, in quanto i prodotti illeciti vengono spesso venduti a prezzi inferiori rispetto agli originali. Come già è ben risaputo, esistono varie tipologie di violazione del diritto d'autore, tra cui il plagio, la contraffazione e il plagio-contraffazione. Il plagio modifica totalmente o parzialmente un'opera tramite tecniche di copia-incolla o integrazione, con conseguente

[110]**D'AMMASSA G.**, *Le difese e le sanzioni civili,* 2014 disponibile su dirittodautore.it

attribuzione indebita della paternità. Quando il plagio è totale e fedele, allora si andrà a parlare di usurpazione. La contraffazione consiste nello sfruttamento economico di un'opera senza apportare delle modifiche. Un esempio emblematico può essere la vendita di copie illegali di CD musicali. Infine, si verifica il plagio-contraffazione quando l'opera viene sfruttata economicamente nella sua interezza combinando gli elementi di plagio e di contraffazione. Il web è ovviamente uno dei principali veicoli per la diffusione illecita di opere protette ed è una delle principali cause di diffusione dei rischi per la proprietà intellettuale. Le tecnologie digitali, infatti, nonostante abbiano aiutato gli autori a trovare numerose opportunità, hanno anche, purtroppo, reso più difficile individuare e perseguire chi commette questi reati. Per fortuna, però, vi sono diversi strumenti di contrasto, tra cui la vigilanza sul web, la promozione della cultura sulla legalità e ovviamente le azioni legali. Queste ultime, infatti, sono essenziali, sia in sede civile, ma soprattutto in sede penale, per far cessare le attività illecite e scoraggiare future violazioni[111].

Nel paragrafo precedente, si è detto, che la legge sul diritto d'autore, nella seconda sezione del Titolo III e Capo III, regola le ipotesi di reato contro il diritto di autore. Nello specifico, agli articoli 171 a 174-ter, disciplina le relative sanzioni penali. Le ipotesi previste sono state ampliate e, anche modificate, da diversi decreti legislativi. Uno degli interventi più rilevanti è il D. Lgs. n. 518/1992, seguito successivamente dal D. Lgs n. 685/1994, n. 204/1996 e n. 160/1999. Questi hanno apportato delle modifiche ad articoli già esistenti e hanno introdotto nuovi articoli, come il 171-bis, 171-ter e 171-quater, i quali hanno aggiornato e ampliato le ipotesi di violazione del diritto d'autore. La legge n. 248/2000 ha segnato un ulteriore passo in avanti e ha inasprito le sanzioni previste e introdotto nuovi articoli, quali il 171-quinquies, 171-sexies, 171-septies, 171-octies, 171-novies, 174-bis e 174-ter. Questa legge ha introdotto anche l'applicazione di sanzioni amministrative e accessorie, le quali si aggiungono a quelle penali già previste, e sono in grado così di aumentare il rigore del quadro sanzionatorio. Le modifiche però non si fermano qui: sono stati apportati ulteriori interventi legislativo con l'introduzione del D. lgs. n. 68/2003, il D. L. n. 7/2005 e i D. lgs. n. 118/2006 e n. 140/2006. Questi ultimi interventi hanno aggiornato nuovamente la normativa in materia di diritto d'autore e la hanno adeguata alle nuove e esigenze e sfide dell'evoluzione tecnologica e delle pratiche commerciali. I reati contro il diritto d'autore vengono perseguiti d'ufficio e, di conseguenza, non è necessaria una querela da parte della persona offesa per avviare un procedimento penale. Sarà sufficiente che le autorità competenti ricevano una denuncia per far partire l'azione penale. Questo

[111] **ANDRIULO L.** *Conseguenze penali e violazione diritto d'autore,* 2023, disponibile su: https://www.anplegal.eu/it/conseguenze-penali-violazione-diritto-dautore

rende il sistema di tutela del diritto d'autore particolarmente rigoroso, in quanto le autorità possono intervenire in maniera autonoma non appena vengano a conoscenza della violazione. Per quanto riguarda, invece, la prescrizione, il termine entro il quale è possibile presentare una denuncia per tali reati è di cinque anni. Il periodo decorre dal momento in cui è stato commesso il reato e una volta trascorso questo termine, il reato non è più perseguibile penalmente[112].

L'art. 171 LDA si occupa della protezione sia dei diritti di utilizzazione economica che dei diritti morali dell'autore. Al primo comma vengono stabiliti una serie di reati riguardanti l'utilizzazione economica delle opere. In particolare, vengono previste sanzioni per chiunque, senza averne diritto, e indipendentemente dallo scopo, o dalla forma, compia azioni quali la riproduzione, trascrizione, rappresentazione in pubblico, diffusione, vendita o messa in commercio di un'opera altrui, o ne rilevi il contenuto prima che questo sia reso pubblico. Inoltre, include la messa a disposizione del pubblico di un'opera protetta tramite reti telematiche, la rappresentazione o esecuzione pubblica di opere teatrali o musicali, e la riproduzione di un numero di esemplari superiore a quello autorizzato. Con il secondo comma viene introdotto la possibilità di estinzione del reato per chi commette la violazione prevista alla lettera a-bis del primo comma e quindi la messa a disposizione del pubblico di un'opera protetta su reti telematiche. Questo avviene attraverso il pagamento di una somma pari alla metà della multa massima prevista prima dell'apertura del dibattimento o dell'emissione del decreto penale di condanna, comprensiva delle spese del procedimento. Al comma 3, invece, il legislatore si concentra sui diritti morali dell'autore e prevede delle pene più severe per chi commette reati come l'usurpazione della paternità dell'opera o la deformazione, mutilazione o altre modifiche dell'opera che possa offendere l'onore o la reputazione dell'autore. Le sanzioni previste comprendono la reclusione fino a un anno e una multa non inferiore a 516 euro[113].

L'art. 171-bis LDA mette in risalto l'importanza della tutela dei diritti di proprietà intellettuale in ambito digitale e applica, di conseguenza, misure rigorose contro chi tenti di sfruttare indebitamente programmi per elaboratori e banche dati. Al comma 1, questo articolo punisce chiunque duplichi programmi per elaboratore, senza autorizzazione, per trarne profitto o che, con le stesse finalità, importi, distribuisca, venda o detenga a scopo commerciale o imprenditoriale, o conceda in locazione tali programmi contenuti in supporti non contrassegnati dalla SIAE. Le sanzioni

[112] **D'AMMASSA G.** *Le difese e le sanzioni penali,* 2014*,* disponibile su dirittodautore.it

[113] **FLOR R.,** *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di internet. Un'indagine comparata in prospettiva europea ed internazionale,* CEDAM, 2010

previste includono la reclusione da sei mesi a tre anni e una multa compresa tra 2.582,00 e 15.493,00 euro. La stessa pena si applica a chi facilita la rimozione o l'elusione di dispositivi di protezione dei programmi per elaboratore. Se il fatto è considerato grave, la pena minima aumenta a due anni di reclusione e la multa a 15,493 euro. Il comma 2 estende queste sanzioni a chi riproduce, trasferisce su un altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati senza rispettare le disposizioni legali, oppure esegue l'estrazione o il reimpiego di una banca di dati in violazione delle norme previste. Le pene previste sono simili a quelle previsti dal primo comma: reclusione da sei mesi a tre anni e multa da 2.582 euro a 15.493 euro se il fatto è particolarmente grave[114].

L'art. 171-ter LDA rappresenta una delle disposizioni più incisive del sistema giuridico italiano nella lotta contro la pirateria e la violazione dei diritti d'autore. Questa norma si applica a una vasta gamma di comportamenti illeciti che coinvolgono l'abusiva duplicazione, riproduzione, trasmissione o diffusione di opere dell'ingegno, specificatamente quando queste azione non sono compiute per uso personale, ma a fini di lucro. La disposizione stabilisce che chiunque, con l'intento di ottenere un profitto economico, si renda responsabile della duplicazione, riproduzione, trasmissione o diffusione non autorizzata, anche parziale, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio, è soggetto a una pena che varia da sei mesi a tre anni di reclusione, oltre a una multa compresa tra 2.582,00 euro a 15.493,00 euro. La norma include qualsiasi procedimento attraverso il quale queste opere, tra cui dischi, nastri o altri supporti contenenti fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive vengono abusivamente riprodotte o diffuse. Inoltre, la legge punisce anche chi, sempre con fini di lucro, riproduce, trasmette o diffonde in pubblico opere letterarie, drammatiche, scientifiche, didattiche, musicali o multimediali, anche se queste vengono inserite in opere collettive o banche dati. In questo modo, il legislatore ha inteso tutelare una vasta gamma di creazione intellettuali, riconoscendo la loro importanza culturale ed economica. La norma, poi, si estende a punire anche chi, pur non avendo direttamente partecipato alla duplicazione o riproduzione, introduce nel territorio italiano, detiene per la vendita o distribuzione, o comunque cede a qualsiasi titolo le opere riprodotte o duplicate abusivamente. Questa estensione della punibilità mira a colpire non solo i produttori, ma anche coloro che agevolano la diffusione di opere contraffatte, rendendo più efficace la protezione dei diritti d'autore. La legge interviene anche su un altro fronte e punisce chi, con fini di lucro, detiene, vende,

[114] **TERRACINA D.,** *La tutela penale del diritto d'autore e dei diritti connessi,* Giappichelli, Torino, 2006.

noleggia, o cede a qualsiasi titolo supporti contenenti opere audiovisive o musicali privi del contrassegno SIAE o con contrassegno contraffatto o alterato. Questo tipo di violazione colpisce direttamente il sistema di gestione e controllo della distribuzione delle opere tutelate, e contribuisce a fenomeni di contraffazione su larga scala[115].

Un'altra condotta sanzionata dall'art. 171-ter LDA riguarda, invece, la ritrasmissione o diffusione, senza accordo con il legittimo distributore, di servii criptati ricevuti mediante apparati atti alla decodificazione di trasmissioni ad accesso condizionato. In altre parole, chiunque intercetti e diffonda illegalmente trasmissioni protette da sistemi di accesso condizionato, senza pagare il canone previsto, commette un reato punibile con la stessa severità. In più, la legge sanziona chi introduce, vende, noleggia, o promuove dispositivi progettati per eludere misure tecnologiche efficaci, come quelle previste dall'art. 102-quater. Questi dispositivi, creati appositamente per aggirare le protezioni poste a tutela delle opere digitali, rappresentano una minaccia significativa per il rispetto dei diritti d'autore. La norma si applica anche a chi, abusivamente, rimuove o altera le informazioni elettroniche che identificano le opere protette, agevolando così la loro distribuzione illecita. Nei casi in cui la violazione coinvolga un numero significativo di opere, le pene previste dalle legge sono più gravi. Infatti, chi riproduce, duplica, trasmette o diffonde abusivamente, vende o importa oltre cinquanta copie o esemplari di opere tutelate, può essere punito con una pena di reclusione che va da uno a quattro anni, oltre alla multa già menzionata. È prevista, inoltre, una specifica sanzione per chi comunica al pubblico, tramite reti telematiche, opere protette dal diritto d'autore senza autorizzazione. Questo comportamento sta diventando sempre più rilevante con la diffusione delle tecnologie digitali e internet. In caso di condanna per i reati previsti dall'art. 171-ter, la legge impone anche l'applicazione di pene accessorie. Sono previste, infatti, la pubblicazione della sentenza e la sospensione per un anno delle concessioni o autorizzazione necessarie per l'esercizio di attività radiotelevisive o commerciali, secondo quanto previsto dall'art. 36 c.p. queste pene accessorie non solo puniscono il colpevole, ma servono anche a dissuadere altri dal commettere simili reati, colpendo la capacità di esercitare l'attività professionale o commerciale. Infine, i proventi derivanti dalle sanzioni pecuniarie imposte ai sensi dell'art. 171-ter sono destinati all'Ente nazionale di previdenza e assistenza per i pittori e scultori, musicisti, scrittori e autori drammatici – ENAP-PSMSAD, che è stato integrato nell'ENPALS e successivamente nell'INPS come Fondo PSMSAD. Questo fondo ha lo scopo di sostenere economicamente le categorie artistiche colpite dalle violazioni dei loro diritti e

[115] **GARCIA C. A.,** *Violazione del diritto d'autore: cosa si rischia,* 2023, disponibile su laleggeepertutti.it

di garantire così un minimo di protezione sociale ai creatori di opere dell'ingegno. L'art. 171-ter non reprime solamente le condotte illecite legate alla pirateria e alla violazione del diritto d'autore, ma cerca anche di tutelare e sostenere gli autori riconoscendo l'importanza del loro contributo culturale e artistico[116].

L'art. 171-quater LDA, invece, prevede sanzioni specifiche per chi commette determinate violazioni del diritto d'autore, con fine di lucro e senza autorizzazione. Vi è però una caratteristica non presente negli articoli precedentemente citati fino ad adesso, ovvero queste violazioni costituiscono una sanzione purché tali atti non vadano a costituire un reato più grave. Nello specifico, la norma si applica a chi concede in noleggio, o comunque cede in uso a qualunque titolo, originali, copie o supporti di opere tutelate dal diritto d'autore, ottenuti lecitamente. Quindi, questo significa che anche se i supporti in questione sono stati acquisiti in modo legale, il loro utilizzo a fini di lucro senza la dovuta autorizzazione dell'autore o del titolare dei diritti costituisce una violazione della legge. La norma estende la sua applicazione anche a chi esegue la registrazione su supporti audio, video o audiovisivi, delle prestazioni artistiche degli artisti o interpreti esecutori, come previsto dall'art. 80 LDA. Ad esempio, ciò può includere la registrazione non autorizzata di concerti, spettacoli teatrali o altre esibizioni artistiche, per poi concederle in noleggio o uso, ottenendo un guadagno illecito. Le sanzioni previste dall'art. 171-quater consisto nell'arresto fino ad un anno o nell'ammenda, la quale può variare da un minimo di 516,00 euro ad un massimo di 5.164,00 euro. L'applicazione di queste pene può variare a seconda della gravità del reato e delle circostanze specifiche in cui è stato commesso. Il legislatore, con questa norma, ha sia l'obiettivo di proteggere gli autori delle opere intellettuali, ma anche gli artisti esecutori. In questo modo garantisce loro il diritto esclusivo di decide in che modo e a quali condizioni le loro opere o esibizioni possono essere utilizzata e commercializzate[117].

Nel contesto della legge sul diritto d'autore, alcune specifiche transazioni commerciali sono equiparate alla concessione in noleggio. È considerata equivalente al noleggio la vendita di un'opera con patto di riscatto o sotto condizioni risolutiva quando le transazioni prevedono che, in caso di riscatto o di avveramento della condizione, il venditore debba restituire una somma inferiore a quella inizialmente pagata dall'acquirente. Quindi, in poche parole, se un'opera viene venduta con l'accordo che, al verificarsi di una specifica condizione, l'acquirente possa restituirla e ottenere un rimborso,

[116] **FLOR R.,** *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di internet. Un'indagine comparata in prospettiva europea ed internazionale,* CEDAM, 2010

[117] *Ibidem*

ma tale rimborso risulta essere inferiore al prezzo di vendita originario, tale operazione viene trattata alla stregua di una concessione in noleggio ai fini della legge sul diritto d'autore. Allo stesso modo, se l'acquirente paga al momento della consegna una somma inferiore al prezzo di vendita finale, magari a titolo di acconto, e tale somma risolta essere inferiore al valore totale, allora anche questa transazione sarà equiparata al noleggio. Tutto ciò viene disciplinato dall'art. 171-quinquies.

L'art. 171-sexies LDA disciplina le misure di distruzione e confisca del materiale coinvolto in violazione delle norme sul copyright. Secondo questo articolo, l'autorità giudiziaria ha la facoltà di ordinare la distruzione del materiale quando quest'ultimo è di dimensioni tali da rendere difficoltosa la custodia. Questo provvedimento deve essere preso in conformità con le disposizioni dell'art. 83 c.p.p., come anche stabilito dal D. Lgs. n. 271/1989. L'art. 171-sexies prevede, poi, che la confisca sia sempre disposta per gli strumenti e i materiali utilizzati o destinati a commettere reati previsti agli artt. 171-bis, 171-ter e 171-quater. La confisca riguarda, oltre agli strumenti, anche le videocassette, i supporti audio-visivi, fonografici, informatici o multimediali che siano stati abusivamente duplicati, riprodotti, ceduti, commercializzati, detenuti o introdotti nel territorio nazionale. Rientrano poi, nella confisca, quando richiesto anche tutti i supporti privi del contrassegno SIAE, o dotati di contrassegno SIAE contraffatto, alterato o destinato a un'opera diversa da quella dichiarata. La confisca viene disposta anche nel caso in cui la pena venga applicata su richiesta delle parti, secondo quanto disciplinato dall'art. 444 c.p.c. Ciò è noto come patteggiamento. Infine, le misure di confisca e distruzione possono essere applicate anche se i beni confiscati appartengono ad un soggetto giuridico diverso, purché uno dei partecipanti al reato abbia agito nell'interesse di tale soggetto[118].

Tra le sanzioni penali della legge sul diritto d'autore è prevista anche la pena di omissione della comunicazione. Secondo l'art. 171-septies sono previste le stesse pene indicate nell'art. 171-ter, c. 1, LDA ai produttori o importatori di supporti non soggetti al contrassegno SIAE, qualora essi omettano di comunicare alla SIAE i dati necessari per identificare tali supporti. Questi soggetti devono effettuare questa comunicazione entro trenta giorni dall'immissione in commercio o dall'importazione di questi supporti. Inoltre, a chi dichiari falsamente di aver adempiuto agli obblighi previsti dall'art. 181-bis, c. 2, LDA, verranno applicate le stesse sanzioni, salvo che il fatto non costituisca un reato più grave. L'art. 171-octies prevede delle pene per chiunque produca, venda, importi, promuova, installi, modifichi o utilizzi dispositivi atti a decodificare trasmissioni audiovisive

[118] **LEGGE SUL DIRITTO D'AUTORE (L. 633/1941)**

ad accesso condizionato. Queste azioni devono essere effettuate con fini fraudolenti. Le trasmissioni coinvolte sono quelle che possono essere viste solo da un gruppo selezionato di utenti, indipendentemente dal fatto che venga richiesto o meno un canone di pagamento. Per queste violazioni, la pena prevista è la reclusione da sei mesi a atre anni e una multa da 2.582,00 a 25.822,00 euro. Se il reato è particolarmente grave, la pena minima aumenta a due anni di reclusione e una multa di almeno 15.493,00 euro. Infine, vi sono gli artt. 171-octies-1 e 171-novies. Il primo punisce chiunque si rifiuti di rispondere alle domande del giudice senza un giustificato motivo e chiunque fornisca informazioni false, così come disciplinato anche dall'art. 156-ter. La pena prevista è la medesima prevista dall'art.372 c.p., che riguarda la falsa testimonia. L'unica differenza è che la pena è ridotta della metà. L'art. 171-novies prevede la diminuzione della pena in alcuni casi specifici. Ne prevede la diminuzione da un terzo alla metà per i reati previsti agli artt. 171-bis, 171-ter e 171-quater. Poi, prevede l'esclusione delle pene accessorie per chi denunci la violazione in modo spontaneo prima che essa le venga contestata o, comunque, chi fornisca informazioni utili per individuare l'organizzazione illecita, o per permettere il sequestro di significative quantità di supporti audiovisivi e fonografici o di strumenti usati per commettere il reato. Queste disposizioni però non verranno applicate al promotore o all'organizzatore dell'attività illecita[119]. Tra le sanzioni penali della legge sul diritto d'autore è importante citare anche l'art. 172, il quale prevede delle sanzioni amministrative per reati compiuti per colpa. Questo articolo prevede una sanzione fino a 1.032,00 euro per chiunque commetta per colpa i reati indicati nell'art. 171. La stessa pena si applica anche a chi esercita l'attività di intermediario in violazione delle disposizioni degli artt. 180 e 183 LDA.

Recentemente, invece è stata pubblicata sulla Gazzetta ufficiale la L. n. 93/2023, intitolata "*Disposizioni per la prevenzione e la repressione della diffusione illecita di contenuti tutelati dal diritto d'autore mediante le reti di comunicazione elettronica*". La normativa in materia di diritto d'autore ha visto l'introduzione di misure significative, comprese quelle di natura penale, finalizzate a contrastare il fenomeno della pirateria e della violazione dei diritti d'autore. Tra queste, l'art. 3 L. n. 93/2023 ha modificato sostanzialmente la disciplina sanzionatoria prevista dall'art. 171-ter L. n. 633/1941, la quale regola la protezione del diritto d'autore in Italia. Questa modifica ha comportato l'aggiunta di una nuova disposizione, indicata come lettera *h-bis,* all'art. 171-ter, c. 1. La nuova disposizione estende la punibilità a chi, anche mediante modalità specificate all'art. 85-bis Testo Unico delle Leggi di Pubblica Sicurezza (TULPS), c. 1, esegue la fissazione abusiva su supporti

[119] **D'AMMASSA G.** *Dizionario dei termini di diritto di autore,* 2023

digitali, audio, video o audio-video di opere cinematografiche, audiovisive o editoriali, oppure effettua la riproduzione, l'esecuzione o la comunicazione al pubblico delle fissazioni abusivamente eseguite. L'art. 85-bis TULPS riguarda principalmente l'introduzione, l'installazione o l'utilizzo non autorizzato nei luoghi di pubblico spettacolo di dispositivi o apparati che permettono la registrazione, la riproduzione, la trasmissione o la fissazione su supporti audio, video o audio-video, in tutto o in parte, delle opere intellettuali che vengono realizzate o diffuse. Per tali condotte, la sanzione prevista, qualora il fatto sia commesso per fini di lucro e non per uso penale, consiste nella reclusione da sei mesi a tre anni e in una multa da cinque a trenta milioni di lire, o comunque il corrispondente valore in euro, data la conversione valutaria. Questa integrazione normativa evidenzia l'intenzione del legislatore di inasprire le misure repressive contro la pirateria, rafforzando la tutela del diritto d'autore attraverso l'inclusione di nuove fattispecie di reato e l'applicazione di sanzioni più severe, in linea con gli sviluppi più recenti del diritto d'autore. Al secondo comma dello stesso articolo, viene, invece, apportata una modifica importante all'art. 132-bis, c.p. Quest'ultimo disciplina la causa di non punibilità per particolare tenuità del fatto e la modifica, in particolare, introduce un'eccezione alla regola generale stabilita da questa articolo. Viene aggiunto il numero *4-bis* al terzo comma dell'art. 131-bis c.p. Questa aggiunta stabilisce che l'offesa non può essere considerata di particolare tenuità nei casi di reati previsti dalla Sezione II del Capo III, Titolo III, L. 633/1941, con l'eccezione dei reati contemplati dall'art. 171 della stessa legge. Ciò va ad implicare che per i reati penali relativi alla violazione dei diritti d'autore, a partire dall'art. 171-bis in poi, non può essere applicabile la causa di non punibilità per particolare tenuità del fatto prevista dall'art. 132 bis c.p. Quindi, anche se il reato commesso può non sembrare grave, non si potrà beneficiare della non punibilità prevista e, di conseguenza, verrà resa più severa la risposta sanzionatoria nei confronti delle violazioni del diritto d'autore. Questa modifica va a sottolineare la volontà del legislatore di contrastare in modo più rigoroso le violazioni dei diritti d'autore[120].

[120] **GAUDENZI SIROTTI A.,** *Il nuovo diritto d'autore. La tutela della proprietà intellettuale nell'era dell'intelligenza artificiale,* 12 ed., Maggioli Editore, 2023

4. LE NORME E GLI STRUMENTI DI TUTELA AMMINISTRATIVA (REGOLAMENTO AGCOM E LEGGE ANTIPIRATERIA)

La l. 248/2000 ha introdotto nuove norme a tutela del diritto d'autore e con esse anche un nuovo sistema amministrativo relativo allo svolgimento di determinate attività e un sistema sanzionatorio amministrativo. Le novità riguardano principalmente gli artt. 171, 174-bis e 174-ter. L'art. 2, c. 4, L. 248/2000 modifica l'art. 171 LDA con l'aggiunta di un comma il quale introduce una sanzione specifica per la violazione delle disposizioni previste dal terzo e quarto comma dell'art. 68 della legge sul diritto d'autore. Il nuovo comma stabilisce che chi viola tali disposizioni sarà soggetto a due principali conseguenze. Sono, infatti, previste la sospensione dell'attività di fotocopia, xerocopia o qualsiasi altro sistema analogo di riproduzione sarà sospesa per un periodo che va da sei mesi a un anno e una sanzione amministrativa pecuniaria. L'importo della multa varia da due a dieci milioni di lire[121].

All'art. 8 della l. 248/2000 vengono introdotti due nuovi articoli alla l. 633/1941: l'art. 174-bis e l'art. 174-ter. Questi mirano a rafforzare la protezione del diritto d'autore attraverso sanzioni amministrative e misure preventive. L'art. 174-bis prevede delle sanzioni amministrative pecuniarie qualora vi sia la violazione delle disposizioni previste. Queste sanzioni sono pari al doppio del prezzo di mercato dell'opera o del supporto violato, o comunque non inferiore ai 103,00 euro. Se il prezzo non è facilmente determinabile, la sanzione varia da103,00 a 1.032,00 euro. La multa verrà applicata per ogni singola violazione e per ogni esemplare abusivamente duplicato o riprodotto. I proventi verranno destinati, per il 50%, al bilancio dello Stato e poi riassegnati per il potenziamento delle strutture e degli strumenti per la prevenzione e l'accertamento dei reati relativi al diritto d'autore e, per il restante 50%, verranno destinati alla promozione di campagne informative, secondo quanto previsto della l. 400/1988. L'art. 174-ter prevede, invece, la sospensione e la revoca delle attività commerciale. Nel dettaglio, secondo quanto previsto da questo articolo, il Pubblico Ministero deve dare comunicazione al questore qualora avvii un'azione penale per reati non colposi relativi alla violazione del diritto d'autore in un esercizio commerciale o attività soggetta ad autorizzazione. Il questore, dopo aver valutato la situazione può sospendere l'attività per un periodo che va da 15 giorni a 3 mesi. Questa sospensione è aggiuntiva a eventuali misure penali come il sequestro. In caso di condanna, l'attività sarà poi sospesa da 3 mesi ad un anno con possibilità di revoca della licenza in

[121] **LEGGE 248/2000** https://www.parlamento.it/parlam/leggi/00248l.htm

caso di recidiva specifica. Queste disposizioni si possono applicare anche a stabilimenti di sviluppo, stampa, postproduzione, tipografie, masterizzazioni, e centri di emissione o ricezione di programmi televisivi. Le agevolazioni previste per queste attività sono sospese durante l'azione penale, e in caso di condanna, sono revocate per almeno due anni. Sempre l'art. 8, al comma 2, inserisce l'art. 75-bis nel testo unico delle leggi di pubblica sicurezza – TULPS. L'introduzione di questo articoli, approvato con il R.D. 773/1931, aggiunge una nuova disposizione che riguarda le attività legate alla produzione, duplicazione, riproduzione, vendita, noleggio, e cessione di supporti contenenti fonogrammi e videogrammi. L'art. prevede l'obbligo di comunicazione preventiva qualora si intenda svolgere attività a fini di lucro legate alla produzione, duplicazione, riproduzione, vendita, noleggio o cessione di supporti contenenti fonogrammi, videogrammi di opere cinematografiche, audiovisive o sequenze di immagini in movimento. Il questore, poi, una volta ricevuta la comunicazione, rilascia una ricevuta che attesta l'avvenuta iscrizione dell'attività in un apposito registro. Questa iscrizione deve essere rinnovata annualmente. Per la violazione di questa attività è prevista la sanzione amministrativa del pagamento di una somma da 516,00 a 3.096,00 euro[122].

Nel contesto della tutela amministrativa, sicuramente è di notevole importanza, il Regolamento AGCOM che disciplina la tutela del diritto d'autore sulle reti di comunicazione elettronica in Italia. Questo regolamento rappresenta uno strumento normativo essenziale per l'adattamento della legislazione italiana alle esigenze dettate dall'evoluzione digitale. Esso si articola in quattro capi principali. Il primo è dedicato ai principi generali e definisce il contesto normativo e i termini chiave utilizzati. Viene chiarito, poi, l'ambito di applicazione e le finalità del regolamento stesso. In particolare viene precisato che l'obiettivo è tutelare il diritto d'autore senza penalizzare l'innovazione e la libera circolazione delle informazioni. Il secondo capo introduce misure specifiche per lo sviluppo e la tutela delle opere digitali, sottolineando l'importanza di promuovere l'offerta legale e di sensibilizzare il pubblico sul rispetto della proprietà intellettuale. Proprio per questo, viene istituito un Comitato per lo Sviluppo e la Tutela dell'Offerta Legale di Opere Digitali. Questi è un organismo con il principale compito di monitorare il mercato, incentivare l'adozione di codici di condotta e proporre eventuali aggiornamenti al regolamento in risposta ai cambiamenti tecnologici. Il terzo capo del regolamento descrive dettagliatamente le procedure che l'AGCOM può attuare per proteggere il diritto d'autore online. Questo include la possibilità per i soggetti legittimati di presentare istanze per la rimozione di contenuti che violano la normativa sul diritto d'autore,

[122] **LEGGE 248/2000** https://www.parlamento.it/parlam/leggi/00248l.htm

seguendo un procedimento che deve essere rapido ed efficace. La Direzione dell'AGCOM ha un ruolo centrare in questa fase. Di fatti essa può archiviare istanze non conformi o avviare i procedimenti necessari. Il quarto capo, infine, è dedicato alle misure di tutela, e stabilisce le sanzioni concrete che l'AGCOM può intraprendere per far rispettare la legge, comprese la rimozione di contenuti illegali e la disabilitazione dell'accesso ai siti che ospitano opere contraffatte. In questo regolamento è molto importante l'art. 13, il quale disciplina i provvedimenti a tutela del diritto d'autore. L'articolo si sofferma particolarmente sulla procedura che l'organo collegiale dell'Autorità per le Garanzie nelle Comunicazione (AGCOM) deve seguire quando esamina presunte violazioni del diritto d'autore o dei diritti connessi. La procedura descritta dall'articolo evidenzia l'impegno dell'organo nel garantire il rispetto del diritto d'autore attraverso un processo strutturato che include la possibilità di archiviare i casi infondati, emettere ordini di cessazione delle violazioni e applicare sanzioni in caso di non conformità. Nel dettaglio, se l'organo collegiale, dopo aver esaminato i documenti e le prove, non trova sufficienti prove che dimostrino la violazione del diritto d'autore o dei diritti connessi, allora può decidere di archiviare il caso, e di conseguenza, non verrà intrapresa alcuna azione ulteriore nei confronti del presunto trasgressore. Se, invece, l'organo collegiale ritiene che vi sia effettivamente una violazione può essere emessa una diffida o un ordine di rimozione a seconda dei casi. Nel caso in cui si tratti di fornitori di servizi di media lineari, quali emittenti televisive, verrà emessa una diffida, e quindi un avvertimento ufficiale, affinché venga interrotta la trasmissione che viola la legge sul diritto d'autore. Nel caso in cui si tratti di fornitori di servizi di media a richiesta, come piattaforme streaming, allora viene ordinata la rimozione dei contenuti che violano il diritto d'autore. La rimozione deve essere effettuata entro tre giorni dalla notifica dell'ordine. L'ordine collegiale deve adottare questi provvedimenti entro un termine massimo di 35 giorni dalla ricezione delle istanze che hanno dato avvio al procedimento. I provvedimenti adottati vengono comunicati sia a chi ha presentato l'istanza, sia ai soggetti destinatari della notifica di avvio del procedimento. Se i soggetti destinati non ottemperano alle diffide o agli ordini entro il termine stabilito, allora l'AGCOM ha il potere di applicare sanzioni amministrative. Queste sanzioni sono previste dall'art. 1, c. 31, l. 249/1997. Inoltre, l'Autorità informa gli organi di polizia giudiziaria, come previsto dall'art. 182-ter LDA, affinché possano essere intraprese ulteriori azioni legali o penali se necessario[123].

[123] Regolamento AGCOM in materia di tutela del diritto d'autore sulle reti di comunicazioni elettroniche e procedure attuative ai sensi del decreto legislativo 9 aprile 2003, n. 70, in vigore dal 31 marzo 2014

Recentemente, è stata approvata la delibera 95/2 4/CONS che delibera alcune questioni riguardanti il diritto d'autore, licenze d'uso di opere audiovisive su servizi di video on demand e risoluzione di controversie. Questo nuovo regolamento include nuove sanzioni in caso di inadempimento. Rappresenta un importante regolamento adottato dall'Autorità per le Garanzie nelle Comunicazioni (AGCOM) per l'attuazione di vari articoli della l. 633/1941, meglio conosciuta come la legge sul diritto d'autore, come modificata dal D. Lgs 177/2021. Il regolamento è stato approvato durante la riunione del Consiglio dell'Autorità del 17 aprile 2024 e si fonda su una serie di direttive europee e leggi italiane che mirano a disciplinare il mercato unico digitale, con particolare attenzione ai diritti d'autore e ai diritti connessi. La delibera stabilisci le procedure per la risoluzione delle controversie relative agli obblighi di trasparenza e ai meccanismi di adeguamento contrattuale previsti dagli artt. 110-quater e 110-quinquies l. 633/1941. Il documento definisce, poi, i criteri per determinare la rappresentatività degli organismi di gestione collettiva di settore, nonché le misure di pubblicità per informare della possibilità di concedere licenze e la procedura per l'esclusione delle opere del meccanismo di concessione di licenze collettive estese. Il regolamento risulta cruciale per garantire la corretta applicazione delle norme sul diritto d'autore e in un contesto sempre più digitalizzato e interconnesso e contribuisce così a proteggere i diritti degli autori e a regolamentare l'uso delle opere protette nel mercato unico digitale europeo. Il testo si struttura in vari Capi e articoli, ciascuno dei quali affronta specifiche tematiche. Il primo capo si concentra sulle definizioni essenziali e le disposizioni generali che saranno applicate nel contesto del regolamento. L'art. 1 si dedica a chiarire i termini fondamentali utilizzati nel documento, quali *opera, utilizzatore* e *avente causa.* Il secondo capo è centrale nella delibera e si occupa di promuovere la legalità e lo sviluppo dell'offerta digitale. Gli articoli contenuti in questo capo stabiliscono i principi generali e i meccanismi attraverso cui l'AGCOM intende educare gli utenti e facilitare l'accesso legale alle opere digitali. Viene anche istituito un Comitato per lo sviluppo e la tutela dell'offerta legale, composto da rappresentanti di diversi categorie, quali autori, artisti e fornitori di servizi media. Il terzo e il quarto capo delineano le procedure specifiche per l'accertamento e la cessazione delle violazioni dei diritti d'autore. L'AGCOM viene autorizzata a vigilare sull'attuazione delle misure previste e si assicura che le opere digitali siano protette seconde le normative europee e nazionali. Questi capi sono cruciali per garantire che le violazioni siano adeguatamente sanzionate e che il mercato delle opere digitali operi nel rispetto della legge. Nello specifico, il Capo III tratta le procedure per la protezione del diritto d'autore sulle reti di comunicazione elettronica. L'art. 5 disciplina le modalità di intervento e spiega che l'autorità può intervenire su istanza di parte per tutelare il diritto d'autore, in conformità con le procedure

autoregolamentate di *notice and take down.* L'art. 6 disciplina l'istanza all'autorità. Secondo questo articolo, un soggetto legittimato può presentare un'istanza all'Autorità se ritiene che un'opera digitale sia stata resa disponibile online in violazione della legge sul diritto d'autore, richiedendone la rimozione. L'istanza deve essere trasmessa usando un modello disponibile sul sito dell'Autorità e deve essere accompagna da documentazione che comprovi la totalità del diritto. Il procedimento non può essere avviato se è già in corso un procedimento giudiziario per lo stesso oggetto e tra le stesse parti. Il Capo IV, invece, tratta le disposizioni relative alla tutela del diritto d'autore sui servizi di media e stabilisce le norme che i fornitori di servizi di media devono seguire per rispettare il diritto d'autore. L'art. 10 stabilisce che i fornitori di servizi di media audiovisivi e radiofonici devono operare nel rispetto del diritto d'autore e dei principi stabili dagli artt. 3 e 32-bis del Testo Unico, oltre alle norme previste da questo capo. L'art. 11, invece, regolamenta l'istanza all'Autorità. Infatti, qualora si ritenga che la diffusione di un programma violi la Legge sul diritto d'autore, un soggetto legittimato può presentare un'istanza all'Autorità chiedendo di interrompere la diffusione o di rimuovere il programma dal catalogo[124].

Le sanzioni previste dalla Delibera 95/24/CONS riguardano le conseguenze per i fornitori di servizi di media che non rispettano le diffide o gli ordini emessi dall'Autorità per la tutela del diritto d'autore. La sanzione è prevista nel caso di inottemperanza alle diffide e agli ordini. Qualora il fornitore di servizi di media non rispetti le diffide o gli ordini emesse dall'Autorità, allora quest'ultima può applicare le sanzioni amministrative previste dall'art. 1, comma 31, l. 249/1997. Inoltre, in caso di mancata ottemperanza, l'Autorità deve informare gli organi di polizia giudiziaria ai sensi dell'art. 182-ter della legge sul diritto d'autore. L'ordine emanato dall'AGCOM deve essere rispettato dalla parte soccombente entro il termine stabilito nel provvedimento e, come già detto, se questo non avviene l'Autorità può infliggere una sanzione amministrativa pecuniaria che varia da diecimila a duecentocinquantamila euro. È fondamentale notare come il regolamento 95/24 non escluda il ricorso alle vie giudiziarie ordinarie in parallelo al procedimento davanti all'AGCOM. Secondo l'art. 14, c. 6, del regolamento, se una parte si rivolge all'Autorità giudiziaria o avvia una procedura di conciliazione, mediazione o negoziazione assistita che coinvolge, anche solo in parte, la stessa controversia, il procedimento dinanzi all'AGCOM può essere sospeso. Tuttavia, questa sospensione è a discrezione della Direzione dell'Autorità, che potrebbe anche decidere di proseguire con il

[124] **AGCOM,** *Delibera 95/24/CONS, Regolamento recante attuazione degli artt. 18-bis, 46-bis, 80, 84, 110-ter, 110-quater, 110-quinquies, 110-sexies, 180-ter della legge 22 aprile 1941, n. 633 come novellata dal decreto legislativo 8 novembre 2021, n. 17, deliberata il 17 aprile 2024.*

procedimento nonostante la pendenza di un giudizio ordinario. Questo approccio consenso all'AGCOM di mantenere una certa flessibilità operativa, garantendo al contempo che le controversie sul diritto d'autore siano affrontate in modo efficiente, sia attraverso procedure amministrative che giudiziarie. Rispetto ai precedenti regolamenti, il nuovo procedimento istituito da AGCOM rappresenta un'estensione significativa dei poteri dell'Autorità nel campo del diritto d'autore. A differenza delle procedure precedenti, come quelle previste dalla Delibera 680/13 per le violazioni di diritti d'autore online, l'avvio di un procedimento davanti all'autorità giudiziaria ordinaria non determina l'archiviazione automatica del procedimento in corso davanti ad AGCOM. Questa differenza potrebbe portare a possibili conflitti tra le decisioni emessa da AGCOM e quelle dell'autorità giudiziaria e crea un quadro complesso in cui le due autorità potrebbero emettere verdetti contrastanti. Altra novità di questo regolamento è l'introduzione di una sanzione amministrativa pecuniaria in caso di mancato rispetto degli ordini di AGCOM. Questo aspetto configura una storia di *diritto privato penal-amministrativo* il quale viene applicato esclusivamente alle ipotesi trattate nel regolamento, e che attribuisce a queste violazioni un disvalore particolare. In parole povere, le condotte che violano il regolamento 95/24/CONS sono trattate con una severità maggiore rispetto ad altre violazioni contrattuali, per le quali la mancata ottemperanza agli obblighi di informazione o di pagamento non comporta sanzioni altrettanto gravi. Questa configurazione, oltre a rafforzare l'Autorità, segna anche una differenziazione nel trattamento delle violazioni del diritto d'autore e pone in rilievo la gravità di queste condotte rispetto ad altre situazioni contrattuali simili. Di conseguenza, AGCOM acquisisce un ruolo di controllo e sanzione molto più incisivo, in grado di intervenire in modo autonomo e parallelo rispetto all'autorità giudiziaria ordinaria e amplifica il suo potere di tutela del diritto d'autore[125].

La pirateria online, come ben sappiamo, è in continua evoluzione e si è sempre più consapevoli del fatto che i pirati digitali siano in grado di utilizzare delle tecniche sempre più sofisticate per evitare il blocco dei loro siti. L'AGCOM, con delibera 189/23/CONS, cerca di rafforzare il quadro normativo per affrontare queste sfide e di introdurre misure più efficaci per la rimozione rapida dei contenuti e la prevenzione della loro diffusione. Questa rappresenta un importante passo avanti nella protezione dei diritti d'autore in Italia e adatta le norme esistenti alle nuove realtà digitali e alle sfide poste dalla pirateria online. La delibera 189/23/CONS modifica al

[125] **AGCOM,** *Delibera 95/24/CONS, Regolamento recante attuazione degli artt. 18-bis, 46-bis, 80, 84, 110-ter, 110-quater, 110-quinquies, 110-sexies, 180-ter della legge 22 aprile 1941, n. 633 come novellata dal decreto legislativo 8 novembre 2021, n. 17, deliberata il 17 aprile 2024.*

regolamento esistente sulla tutela del diritto d'autore nelle reti di comunicazione elettronica, Si concentra sull'aggiornamento delle procedure e delle norme per contrastare la pirateria online, soprattutto alla luce dei recenti sviluppi normativi a livello europeo, come il Digital Services Act (DSA). La delibera fa riferimento a diverse direttive e regolamenti europei, tra cui la Direttiva 2001/29/CE sul diritto d'autore, la Direttiva 2004/48/CE sulla proprietà intellettuale, e il recente regolamento UE 2022/2065 (DSA), che introduce nuove misure contro la diffusione di contenuti illeciti online. La delibera si inserisce nel quadro normativo italiano, tenendo conto della l. n. 633/1941 e del D. Lgs. n. 70/2003, relativo al commercio elettronico. Le misure principali prevedono il blocco dei siti web, gli interventi d'urgenza e la collaborazione internazionale. L'AGCOM può ordinare ai provider di servizi internet di bloccare l'accesso ai siti web che diffondono contenuti illeciti, come film, musica, software e soprattutto eventi sportivi in diretta senza autorizzazione. Poi, sono previste misure cautelari che possono essere adottate in via d'urgenza per fermare violazioni evidenti del diritto d'autore, con un particolare focus su eventi live, dove il danno economico può essere immediato e significativo. Infine, la delibera sottolinea l'importanza della cooperazione con altre autorità regolatorie europee per garantire un'azione coordinata contro la pirateria a livello transfrontaliero[126].

Di fondamentale importanza nel contesto delle sanzioni amministrative della legge sul diritto d'autore è la legge antipirateria (l. n. 93/2023). La legge n. 93 del 14 luglio 2023 – Legge Nuova Antipirateria – rappresenta una significativa innovazione nella lotta contro la pirateria audiovisiva e conferisce nuovi poteri all'Autorità per le Garanzie nelle Comunicazioni per contrastare la diffusione illecita di contenuti tutelati dal diritto d'autore sulle reti di comunicazione elettronica. La legge è stata pubblicata ufficialmente sulla Gazzetta Ufficiale il 24 luglio 2023, dopo essere stata approvata dal Senato il 12 luglio 2023. Il suo obiettivo principale è quello di rafforzare la prevenzione e la repressione delle attività illegali che coinvolgono la distribuzione non autorizzata di opere cinematografiche, audiovisive e altre opere protette. La legge attribuisce all'AGC'M la facoltà di intervenire in maniera incisiva contro la pirateria online. In particolare, l'Autorità può ordinare ai fornitori di servizi di rete, inclusi quelli che forniscono l'accesso a Internet e di disabilitare l'accesso ai contenuti diffusi in violazione del diritto d'autore. Questo avviene attraverso misure tecniche come il blocco della risoluzione DNS dei nomi di dominio e l'instradamento del traffico di rete verso

[126] **DELIBERA N. 189/23/CONS**, *modifiche al regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuate ai sensi del Decreto legislativo 9 aprile 2003, n. 70 di cui alla delibera n. 680/13/CONS.*

indirizzi IP specifici. Un aspetto cruciale della normativa è la capacità dell'AGCOM di prevenire ulteriori tentativi di eludere i blocchi imposti. L'Autorità può infatti ordinare il blocco preventivo di futuri domini, sottodomini o indirizzi IP che, attraverso modifiche, tentino di aggirare i blocchi precedentemente imposti. Nei casi di particolare gravità e urgenza, come la trasmissione di contenutiti in diretta, ad esempio eventi sportivi o prime visioni cinematografiche, l'AGCOM può emettere provvedimenti di disabilitazione d'urgenza senza contraddittorio, su richiesta del titolare dei diritti violati. La legge prevede, infine, delle sanzioni severe per coloro che violano queste disposizioni. Chiunque esegua abusivamente la fissazione, riproduzione, o comunicazione al pubblico di opere tutelate potrà essere sanzionato con una multa che va da 10.000 euro fino al 2% del fatturato realizzato nell'ultimo esercizio chiuso prima della contestazione[127].

La l. n. 93/2023 prevede diverse sanzioni e misure. All'art. 5 prevede le sanzioni per l'inottemperanza agli obblighi, per cui in caso di mancato rispetto degli obblighi prescritti dai provvedimenti di cui all'art. 2 della legge, l'Autorità per le garanzie nelle comunicazioni applica la sanzione previste dall'art 1, comma 31, terzo periodo, l. 249/1997, quindi una multa da 10.000 euro fino al 2% del fatturato realizzato nell'ultimo esercizio chiuso anteriormente alla notifica della contestazione. Sono poi previste, dall'art. 3 della nuova legge antipirateria, delle sanzioni specifiche per pirateria cinematografica, audiovisiva e editoriale. Questo articolo ci riporta agli artt. 171-ter, lettera h-bis, l. 633/1941, 131-bis, c. 4-bis, c.p., 174-ter, l. n. 633/1941. L'art. 171-ter, lettera h-bis, della legge sul diritto d'autore, sanziona chiunque esegua abusivamente la fissazione su supporto digitale, audio, video, o audio-video di un'opera cinematografica, audiovisiva o editoriale, o chi effettua la riproduzione, esecuzione o comunicazione al pubblico della fissazione abusivamente eseguita. L'art. 131-bis, c. 4-bis, c.p., introduce un'eccezione per i delitti previsti nella sezione II del capo II della l. n. 633/1941, ad eccezione dei delitti di cui all'art. 171 della medesima legge. L'art. 174-ter, l. n. 633/1941 estende al primo comma le sanzioni anche alla messa a disposizione di opere o servizi protetti abusivamente, e al secondo comma, aumenta la sanzione pecuniaria per chi mette a disposizione opere o materiali protette in modo abusivo, da 1.032, 00 euro a 5.000 euro.[128]

[127] **LEGGE 14 luglio 2023, n. 93**. *Disposizioni per la prevenzione e la repressione della diffusione illecita di contenuti tutelati dal diritto d'autore mediante le reti di comunicazione elettronica.*

[128] **LEGGE 14 luglio 2023, n. 93**. *Disposizioni per la prevenzione e la repressione della diffusione illecita di contenuti tutelati dal diritto d'autore mediante le reti di comunicazione elettronica.*

IV. CASE STUDY: IL PEZZOTTO

1. RILIEVO E DIFFUSIONE

Accedere illegalmente a partite, film, serie TV e programmi televisivi che normalmente richiederebbero un abbonamento a pagamento ormai è possibile grazie alla diffusione di un dispositivo chiamato *pezzotto.* Molto simile ad un decoder, questo apparecchio viene collegato alla televisione ed è in grado di sfruttare tecnologie avanzate per intercettare e decodificare i segnali criptati dalle emittenti televisive. Questo dispositivo non è completamente gratuito, infatti, permette di guardare contenuti premium, per lo più sportivi, ad un costo che ammonta a circa 10 euro al mese. Il termine *pezzotto* ha due significati distinti: originariamente si riferiva ad un tappeto artigianale della Valtellina. Solo recentemente questo vocabolo è entrato nel linguaggio comune per indicare un sistema illegale per fruire di contenuti televisivi in streaming. Il termine ha origini napoletane: è, infatti, uno slang che indica qualcosa di falsificato o contraffatto. Originariamente, la parola *pezzotto* veniva utilizzata per riferirsi ai CD pirata, ma la sua vera origine si trova nell'uso per descrivere gli scooter *app'zzottati,* ovvero dei ciclomotori a cui venivano modificati in maniera illecita il motore o il telaio[129]. Il pezzotto però non si riferisce solo al decoder pirata, ma all'intero sistema che lo sostiene. Questo sistema prevede che, tramite connessioni internet e decoder modificati, i clienti possano accedere a una vasta gamma di contenuti televisivi, spesso con aggiornamenti tecnici regolari per aggirare le misure di sicurezza implementate dalle emittenti ufficiali. Questo fenomeno ha avuto un impatto notevole, soprattutto in Italia, e si è diffuso rapidamente causando ingenti perdite economiche alle emittenti televisive e ai fornitori di contenuti legali. Le autorità hanno intensificato gli sforzi per contrastare questa pratica illegale, con operazioni di polizia, sequestri di dispositivi e misure legali contro chi li produce, distribuisce e utilizzata. La diffusione dei pezzotti avviene attraverso canali informali, come mercati illegali, gruppi di messaggistica online e, in alcuni casi, persino negozi fisici. La facilità d'accesso e il basso costo hanno, poi, contribuito alla loro popolarità, specialmente tra coloro che cercano di evitare le tariffe degli abbonamenti ufficiali. Nonostante i continui aggiornamenti dei sistemi di protezione, gli sviluppatori del pezzotto riescono comunque a creare versioni aggiornate capaci di aggirare le nuove misure di sicurezza.

[129] **AVERSA A.,** *Cosa vuol dire pezzotto e perché si chiama così. Una parola che deriva dal dialetto napoletano ma che indica anche un tappeto prodotto al nord,* 2024 articolo disponibile su www.unita.it

Il pezzotto presuppone l'utilizzo di tecnologie legali, così come quasi tutta la pirateria online, le quali però vengono utilizzate in maniera illegale. La tecnologia su cui si basano le trasmissioni pirata si chiama IPTV – Internet Protocol Television. L'IPTV è un sistema di trasmissione di programmi televisivi in streaming e quindi, di conseguenza, senza antenna o satellite. Questo sistema utilizza server clandestini per trasmettere canali e contenuti in diretta o on-demand. Il funzionamento è permesso da una serie di informazioni e di dati che si tramutano in immagini e suoni i quali vengono inviati direttamente sui dispositivi personali, quali smartphone, tablet, computer oppure televisioni collegati ad un decoder, come il pezzotto di cui stiamo parlando. Solitamente, infatti, si tratta semplicemente di un box TV al cui interno viene installato il sistema operativo android. Quindi, in parole povere, l'IPTV non è altro che la trasmissione su Internet di ciò che vediamo in televisione. Bisogna però considerare che questa tecnologia non è sempre illegale. Per esempio, è possibile vedere sul nostro dispositivo mobile e sul computer alcuni canali in chiaro come RAI e MEDIASET. È chiaro, però, che se utilizzo l'IPTV per guardare una partita che viene trasmessa su DAZN o SKY, allora starò commettendo un'azione illegale, o meglio un reato. È importante specificare che non è illegale la tecnologia, ma l'uso che i soggetti ne fanno di questa[130].

Come fanno nella pratica i pirati informatici a trasmettere le partite di Serie A su Internet? Tutto ciò è possibile grazie alla messa in piedi di centrali operative da cui verranno trasmessi i dati. Spesso e volentieri, nei telegiornali sono presenti servizi in cui è possibile vedere gli agenti della guardia di finanza che perquisisce delle stanze, simili ad uffici, pieni di cavi, fili, computer e scatole. Questi uffici sono piedi di decoder e box in funzione 24 ore su 24, sintonizzati su un singolo canale. Questi decoder però presentano una peculiarità: sono dotati di regolare abbonamento. I pirati ottengono queste trasmissioni pagando effettivamente un abbonamento, solo che poi li rivendono illegalmente ad un prezzo vantaggioso a migliaia di persone. Il criminale quindi pagherà un abbonamento 100 euro e lo rivenderà a 10 euro, solo che poi lo rivenderà a centinaia e centinaia di persone, ottenendo un surplus notevole. A questo punto comincia il processo di distribuzione ai vari utenti. Per prima cosa, il segnale audio-video dei vari decoder viene inviato ad un apparecchio chiamato *encoder.* Questo apparecchio è in grado di comprimere i dati e di renderli più leggeri. Questa azione è tipica anche di WHATSAPP quando inviamo, ad esempio, delle foto in modo da impiegare meno tempo per passare da un dispositivo ad un altro. L'encoder, soprattutto, è in grado di rendere questi dati compatibili con il sistema IPTV e, di fatti, questa è la funzione più importante per la

[130] **MOCCIA A.,** *Streaming illegale: come funziona l'IPTV e lo scudo "anti-pezzotto" Piracy Shield,,* 2024, articolo disponibile su www.geopop.it

traduzione di dati dalla TV al computer. Questi dati piratati vengono inviati successivamente ad un server e cioè a dei computer dotati di software capaci di salvare questi dati per poi ridistribuirli. Questi server sono spesso collocati all'estero, in Paesi dove la legge è più permissiva. La parte più importante del funzionamento di questi strumenti è data dalla creazione di playlist, le quali contengono dei file di testo: i cosiddetti file M3U. Questi file contengono l'indirizzo delle trasmissioni illegali. Il concetto è molto simile a quello dei siti web e infatti si parla di URL – Uniform Resource Locator, l'indirizzo in cui si trova il file piratato. A conti fatti, queste playlist sono delle liste dei canali illegali che offre il pirata informatico. Una volta create, queste playlist illegali vengono inviate agli utenti, a fronte di un pagamento. Il pezzotto è in grado di leggere questi file di testo e riesce così accedere alla URL di queste trasmissioni[131].

Come fanno le emittenti televisive a bloccare i pirati? Come fanno le forze dell'ordine a risalire ai pirati e a chi possiede il pezzotto? Innanzitutto ci sono le transazioni economiche: l'acquirente del decoder illegale paga un abbonamento mensile al pirata, il quale riceve del denaro senza alcun motivo. E la finanza è in grado di risalire a queste transazioni ingiustificate. In più esiste l'indirizzo IP che è in grado di indicare dove un determinato dispositivo si sta attaccando ad internet. Questo indirizzo varia da dispositivo a dispositivo e da posizioni a posizione. L'indirizzo IP del pezzotto è l'indirizzo a cui vengono inviati i dati, e quindi, di conseguenza, se le forze dell'ordine riescono a rintracciare l'indirizzo IP da cui provengono i dati e a cui vengono inviati, riescono a trovare sia i pirati sia agli utenti che fanno uso di pirateria. Esiste, infine, lo *scudo antipezzotto:* la piattaforma Piracy Shield. L'obiettivo principale è beccare le trasmissioni pirata, ma in che modo? Poniamo che venga trasmessa una partita di serie A da un sito pirata. I detentori della partita e quindi le reti televisive che hanno il diritto di trasmetterla, come DAZN, SKY e AMAZON, scoprono queste trasmissioni pirata e la segnalano al Piracy Shield. A questo punto, la piattaforma avvisa i gestori delle reti internet, i quali bloccano il sito pirata e lo oscurano in trenta minuti. Possono anche essere segnalati tutti gli utenti connessi al sito pirata. La piattaforma è di proprietà dell'AGCOM ed è entrata in vigore dal 1° Febbraio 2024. Alcuni siti famosi di pirateria sono già stati oscurati e sono anche arrivate le prime multe, le quali ammontano fino a 5.000 euro.

I dati legati al fenomeno della pirateria sono sempre più preoccupanti e a dimostrarlo sono le indagini effettuate da FAPAV/IPSOS. I report più recenti risalgono al 2022, i quali dimostrano che

[131] **MOCCIA A.,** *Streaming illegale: come funziona l'IPTV e lo scudo "anti-pezzotto" Piracy Shield,,* 2024, articolo disponibile su www.geopop.it

solo lo scorso anno vi sono stati 30 milioni di atti di pirateria in più rispetto al 2021: vi è stato un incremento del 26% su eventi sportivi live ed è emerso che 4 pirati su 5 sono consapevoli di star commettendo un reato. Nel 2022, la pirateria ha coinvolto il 42% della popolazione adulta, una percentuale abbastanza stabile rispetto agli anni precedenti. Il numero complessivo di atti illeciti, però, è cresciuto e ha raggiunto circa 345 milioni di episodi, con un aumento del 9% rispetto al 2021. Questo incremento è evidente soprattutto nel settore dello sport live, il quale ha registrato un aumento del 26% nella pirateria, facendo emergere una tendenza di crescita costante. Anche i programmi televisivi e le serie TV hanno visto un aumento rispetto all'anno precedente. Con il 35%, i film restano il contenuto più piratato, anche se il trend legato alla pirateria dei film è in diminuzione con un calo del 4%. Questo calo, si pensa, che potrebbe indicare una crescente disponibilità di opzioni legali accessibili e una maggiore consapevolezza dei rischi associati alla pirateria. La modalità più diffusa per accedere ai contenuti piratati è quella digitale, con il 39%. Un aspetto rilevante dell'indagine riguarda il comportamento degli adolescenti. Nel 2022, il 47% dei ragazzi tra i 10 e i 14 anni ha commesso almeno un atto di pirateria audiovisiva. Questa percentuale, nonostante sia ancora abbastanza alta, risulta essere in calo rispetto al 2021. Inoltre, il numero totale di atti di pirateria tra i giovani non ha raggiunto i 25 milioni, un calo significativo rispetto ai 31 milioni del 2018. Sul fronte della deterrenza, l'oscuramento dei siti pirata si è dimostrato un metodo efficace: il 40% dei pirati adulti ha incontrato almeno una volta un sito bloccato e oltre il 49% di questi ha optato per alternative legali. Nel report viene citata anche la legge sul contrasto alla pirateria online, che all'epoca, era ancora in fase di approvazione[132].

Il profilo del pirata media è così costituito: ha un'età inferiore ai 35 anni, ha un'occupazione e possiede un livello di istruzione alto, o quanto meno più alto rispetto alla media della popolazione italiana, e di solito abita al sud e nelle isole. Come abbiamo detto in precedenza, la tipologia preferita dagli utenti per la fruizione di contenuti piratati è la pirateria digitale. Inoltre, le IPTV illecite vengono utilizzate dalla gran parte degli italiani per accedere ai contenuti illeciti, oggetto di pirateria. Di fatti, sono circa 11,8 milioni gli italiani che usufruiscono di queste modalità. La pirateria audiovisiva di film, sport live e serie TV comporta importanti perdite di fatturato per l'economia italiana, pari a quasi due miliardi di euro. Di conseguenza, ciò porta anche ad una perdita di PIL pari a 821 milioni

[132] **FAPAV,** *Indagine FAPAV/IPSOS 2022,* disponibile su: https://fapav.it/indagine-fapav-ipsos-2022/

di euro e una contrazione dei posti di lavoro di circa 11.200 unità. La stima del danno economico potenziale ammonta a circa 767 milioni di euro, ovvero il 14% in più rispetto agli anni precedenti[133].

Il presidente di FAPAV, Federico Bagnoli Rossi, ha commentato i risultati della ricerca condotta da Nando Pagnoncelli, che si riferisce al 2022, e ha messo in luce come il fenomeno della pirateria stia evolvendo nel tempo sfruttando il progresso tecnologico per scopi illeciti. Un esempio recente di questa evoluzione è il dibattito in corso sulla relazione tra il diritto d'autore e l'intelligenza artificiale. I dati presentati dall'indagine FAPAV dovrebbero stimolare ancora di più l'impegno delle istituzioni nel supportare le industrie dei contenuti audiovisivi e multimediali, oltre che a stimolare la collaborazione – tra industrie e istituzioni – per la definizione e l'applicazione di nuovi strumenti preventivi che siano efficaci nel contrastare la pirateria. Inoltre, il presidente di FAPAV ha sottolineato che è essenziale continuare a promuovere attività di sensibilizzazione e campagne educative a sostegno della legalità. Un esempio di tali iniziative è il *Cinema Siete Voi***,** una campagna contro il camcording[134] promossa in collaborazione con ANEC, ANICA e MPA, e rivolta agli spettatori nei cinema, con l'obiettivo di sensibilizzare il pubblico sul problema delle registrazioni illecite dei film. Si ricorda che questa pratica è illecita e costituisce un reato, ai sensi dell'art. 85-bis del Testo Unico, Legge di Pubblica Sicurezza. Un'altra campagna, lanciata durante la Mostra del Cinema di Venezia, è la seconda edizione di *We Are Stories,* una serie di spot che vedono come protagoniste giovani professioniste che raccontano come la loro passione per l'audiovisivo le abbia spinte a realizzare i loro sogni. Bagnoli Rossi ha concluso sottolineando la necessità di lavorare in modo sinergico per promuovere da un lato un'ampia offerta legali di contenuti audiovisivi e dall'altro arginare la pirateria, che continua a rappresentare un serio freno allo sviluppo industriale ed economico del Paese. Anche Nando Pagnoncelli, Presidente di IPSOS Italia, ha espresso la sua opinione sul tema. L'indagine si è concentrata in particolare sulla percezione del danno da parte dei pirati, e i risultati che hanno evidenziato come molti di coloro che piratano non siano pienamente consapevoli del danno che stanno arrecando all'industria audiovisiva, e in particolare, ai lavoratori che ne fanno parte. Pagnoncelli osserva come questo renda ancora più importante continuare le campagne di sensibilizzazione sul tema. Un dato molto importante emerso dalla ricerca è l'efficacia del blocco dei

[133] **REDAZIONE INTERNAPOLI**, *Quattro italiani su dieci usano il pezzotto, i dati sui pirati di partite e film*, 2024 disponibile su: https://internapoli.it/quattro-italiani-su-dieci-usano-il-pezzotto-i-dati-sui-pirati-di-partite-e-film/

[134] Il camcording è una tipologia di pirateria. Con questo termine si intende l'attività svolta da una persona che, entrata in una sala cinematografica recando con sé qualsiasi tipo di dispositivo di registrazione (camcorder, smartphone, cam, registratore audio, ecc.) registra intenzionalmente o riproduce in tutto o in parte il video e/o l'audio del film.

siti web come deterrente per la pirateria, con un crescente numero di utenti che, dopo essere entrati in contatto con siti oscurati, si sono convertiti a fonti legali. La pirateria, ovviamente, rimane un problema significativo per il panorama italiano, ma attraverso l'educazione e le attività di deterrenza è possibile limitarne l'impatto. Questa rappresenta la sfida più grande che l'industria audiovisiva dovrà affrontare nei prossimi anni[135].

Per affrontare il problema della pirateria e il conseguente problema legata all'acquisto dei pezzotti sono state effettuate diverse campagne di sensibilizzazione. Alcune sono state anticipate nei paragrafi precedenti, quali il *Cinema Siete Voi* e *We Are Stories.* Le campagne di sensibilizzazione contro l'uso del pezzotto e la pirateria digitale sono cruciali per combattere questo fenomeno che danneggia gravemente l'industria audiovisiva e sportiva, sottraendo risorse vitali e mettendo a rischio migliaia di posti di lavoro. Queste campagne mirano a educare il pubblico sui rischi legali, economici e sociali associati all'uso di decoder illegali e alla fruizione di contenuti piratati, e cercano di modificare atteggiamenti e comportamenti. Una delle principali campagne di sensibilizzazione è #STOPIRACY – LA PIRATERIA UCCIDE IL CALCIO. Lanciata dalla Lega Serie A sotto la guida di Luigi De Siervo, questa campagna si propone di sensibilizzare il pubblico sui danni che la pirateria causa al calcio italiano. L'accento è posto sull'impatto economico diretto che il furto di contenuti audiovisivi ha sui club sportivi, che si traduce in una riduzione delle risorse disponibili per ingaggiare nuovi talenti e mantenere un livello competitivo internazionale. *Vedere illegalmente una gara di calcio significa privare la Serie A di risorse essenziali per sopravvivere*: questo è il messaggio chiave della campagna, che ha l'obiettivo di sottolineare come ogni atto di pirateria sia un colpo diretto al cuore della passione per il calcio e al futuro dello sport stesso[136].

L'ideatore della campagna, Luigi De Siervo, fiorentino classe 1969, ha avuto una carriera di successo che lo ha portato a ricoprire ruoli di grande responsabilità. Ha iniziato la sua carriera alla multinazionale Toy's "R" Us, passando poi per la RAI, dove ha trascorso 17 anni come Direttore Commerciale e successivamente come Amministratore Delegato di Rai Com, fino a diventare uno dei massimi esperti di diritti televisivi sportivi come Presidente e AD di Infront Italia. Da febbraio 2019, De Siervo è al vertice del calcio italiano, e ha contribuito significativamente a rendere il calcio nazionale un prodotto sempre più attraente per il mercato internazionale. Grazie alla sua visione

[135] **FAPAV,** *Indagine FAPAV/IPSOS 2022* disponibile su: https://fapav.it/indagine-fapav-ipsos-2022/

[136] **LEGA SERIE A,** *Campagna contro la pirateria audiovisiva. La pirateria uccide il calcio - #STOPIRACY*, promossa in occasione della prima e seconda giornata della Serie A TIM 2022/2023.

strategica, il *marchio Italia* è tornato a essere desiderato nei mercati globali. De Siervo è stato uno dei primi a prendere una posizione pubblica contro la pirateria e fare della lotta contro questo crimine una delle sue priorità. Cinque anni fa, con la campagna di sensibilizzazione "#STOPIRACY – LA PIRATERIA UCCIDE IL CALCIO", è riuscito a focalizzare l'attenzione delle istituzioni e dell'opinione pubblica su una questione cruciale per la sopravvivenza del calcio e dell'intero settore audiovisivo italiano. Il nostro Paese, tristemente noto per essere uno dei principali mercati di consumo di contenuti calcistici illegali, ha sofferto pesantemente a causa della pirateria digitale, che ha contribuito alla perdita di competitività del calcio italiano. De Siervo ha sottolineato l'importanza di combattere questa piaga, gestita dalla criminalità organizzata, che priva i club di risorse essenziali, e danneggia il sistema calcistico italiano. Il fenomeno della pirateria, che ha preso piede a livello globale, ha trovato terreno fertile in Italia, soprattutto durante il periodo del lockdown, quando si è registrato un boom delle IPTV illegali. La pirateria ha inflitto danni significativi al calcio italiano, privando la Serie A delle risorse necessarie per ingaggiare nuovi talenti e mantenere la competitività internazionale dei club. I danni economici sono enormi: si stima che la pirateria costi al sistema calcistico oltre 300 milioni di euro all'anno. Queste risorse finiscono nelle casse della criminalità organizzata e indebolisce l'intera industria. Il Governo riconosce la gravità del problema e ha approvato una legge innovativa contro la pirateria online. questa legge, sostenuta dal settore audiovisivo e sportivo, prevede misure concrete per contrastare la diffusione illegale di contenuti protetti dal diritto d'autore. Uno degli aspetti più innovativi è l'introduzione della piattaforma digitale Piracy Shield, la quale consente di bloccare tempestivamente i segnali illegali entro trenta minuti dalla segnalazione. Questo strumento, messo a disposizione dell'AGCOM dalla Lega Seria A, rappresenta un passo avanti nella lotta alla pirateria. La piattaforma Piracy Shield, attiva da quasi due mesi dopo una lunga fase di test, ha già ottenuto risultati significativi e ha bloccato più di diecimila siti illegali. Il processo è semplice: i titolari dei diritti segnalano le violazioni, che vengono validate in piattaforma, e l'Autorità ordina agli ISP di bloccare gli indirizzi illegali entro trenta minuti. I dati raccolti vengono poi messi a disposizione dell'AGCOM per ulteriori verifiche e coinvolge anche fornitori di servizi VPN e DNS alternativi. Grazie alla prontezza di intervento degli ISP, il tempo medio di blocco dei segnali è sceso a circa tre minuti. Questa piattaforma è stata presa come modello di riferimento da diversi Paesi esteri e ha dimostrato la sua efficacia a livello internazionale. Nonostante questi successi, De Siervo sottolinea che la strada da percorrere è ancora lunga. È essenziale continuare a combattere la pirateria a tutti i livelli, compresa la sanzione degli utenti finali, i quali rischiano multe fino a 5.000 euro. È necessario un cambiamento culturale per far capire che

vedere le partite in modo illecito non è solo un atto che costituisce reato, ma anche un comportamento dannoso per il calcio e per l'intero sistema economico del Paese. Il prossimo passo sarà punire chi continua a infrangere la legge, per proteggere il calcio italiano e garantire la sua competitività a livello internazionale[137].

Un'altra campagna di sensibilizzazione contro la pirateria digitale è promossa da Bobo Vieri e rappresenta un'iniziativa significativa per combattere l'uso del pezzotto e la pirateria nel settore audiovisivo e sportivo. Christian "Bobo" Vieri è un ex calciatore e noto personaggio pubblico, ed è stato scelto come volto della campagna grazie alla sua grande popolarità e alla sua credibilità, soprattutto tra gli appassionati di calcio. La campagna, lanciata dalla Lega Serie A, si proponeva di sensibilizzare il pubblico, in particolare i tifosi di calcio, sui gravi danni che la pirateria infligge al mondo sportivo. Il messaggio centrale era che l'uso di dispositivi illegali, come il pezzotto, non è solo un atto di furto, ma danneggia direttamente il calcio italiano, le squadre, i giocatori, e tutti coloro che lavorano nel settore. Bobo Vieri, con il suo stile diretto e coinvolgente, ha veicolato il messaggio che *rubare il calcio è come fare un autogol alla propria passione.* Ha evidenziato come l'acquisto di abbonamenti illegali e il rifiuto di utilizzare sistemi illegali siano fondamentali per sostenere il calcio e mantenerlo competitivo a livello internazionale. La campagna si è rivolta principalmente ai tifosi di calcio, una fascia demografica che spesso utilizzata il pezzotto per accedere illegalmente alle partite. Utilizzando un volto amato e rispettato come quello di Vieri, la campagna ha cercato di parlare direttamente a chi si identifica con i valori del calcio e del fair play. La campagna è stata diffusa attraverso diversi canali, tra cui spot televisivi, social media, e apparizioni pubbliche di Bobo Vieri. I video della campagna sono stati particolarmente efficaci, mostrando Vieri in situazioni quotidiane mentre discuteva dei pericoli e delle implicazioni morali della pirateria digitale. Grazie alla notorietà di Vieri, la campagna ha raggiunto un vasto pubblico e ha aumentato la consapevolezza sul tema della pirateria. La sua partecipazione ha reso il messaggio più accessibile e convincente per molti tifosi, che potrebbero altrimenti ignorare avvisi più formali. L'obiettivo a lungo termine della campagna era ridurre significativamente l'uso del pezzotto e altri dispositivi illegali, promuovendo invece la fruizione di contenuti attraverso canali legali. La speranza era che, attraverso l'educazione il cambiamento culturale, si potesse arginare la pirateria e garantire un futuro sostenibile per il calcio italiano. La campagna di Bobo Vieri ha dunque giocato un ruolo chiave nel contrastare la pirateria,

[137] **ODDINO M.** *La nostra battaglia ai pirati,* Sportclub, articolo disponibile su www.sportclubonline.it/rubriche/sport/2120-la-nostra-battaglia-ai-pirati

utilizzando la sua attrattività per cambiare la percezione pubblica e promuovere un comportamento più responsabile e legale tra i tifosi di calcio[138].

2. IL CONTRASTO AL PEZZOTTO TRAMITE SISTEMI TECNICI

Il pezzotto è un decoder illegale che consente di accedere ai programmi trasmessi dalle piattaforme televisive a pagamento come Sky, Netflix, o Dazn senza sottoscrivere un abbonamento legittimo. Questi dispositivi sfruttano il sistema IPTV, che permette di trasmettere i segnali dei canali televisivi attraverso una rete informatica. In pratica, il segnale dei canali a pagamento viene intercettato e ritrasmesso su internet: consente così agli utenti di visualizzarlo sul proprio decoder illegale. Questo sistema è alimentato da reti criminali organizzate che forniscono i servizi illegali a basso costo, sottraendo risorse significative ai fornitori legittimi di contenuti. Tuttavia, è possibile contrastare queste pratiche illegale mediante diversi mezzi[139].

Il contrasto al pezzotto rimane tutt'oggi una sfida particolarmente complessa e dinamica che coinvolge autorità, aziende e provider di servizi. Questi dispositivi rappresentano una minaccia significativa per l'industria audiovisiva e sportiva, poiché consentono la visione di eventi in diretta, film, serie TV e altri contenuti protetti dal diritto d'autore, sottraendo risorse vitali ai legittimi detentori dei diritti e alimentando circuiti criminali. Una delle soluzioni più innovative per combattere la diffusione del pezzotto è l'utilizzo di piattaforme digitali come Piracy Shield. Questa tecnologia, implementata dalla Lega Serie A in collaborazione con AGCOM, permette di identificare e bloccare rapidamente i flussi illegali di contenuti. Il funzionamento della piattaforma si basa su una stretta collaborazione tra i titolari dei diritti, le autorità di regolamentazione e i provider di servizi Internet (ISP). Quando un contenuto illegale viene rilevato, la piattaforma segnala il flusso illecito e ne ordina il blocco entro un lasso di tempo molto breve, spesso nell'arco di pochi minuti. Questo approccio non solo interrompe l'accesso illegale ai contenuti, ma dissuade anche i pirati, riducendo l'attrattiva del pezzotto. In teoria, a partire dal 31 gennaio 2024, l'Italia si preparerà ad intensificare la lotta contro la pirateria digitale tramite l'attivazione della piattaforma Piracy Shield. Per comprendere meglio il

[138] **DIPARTIMENTO PER L'INFORMAZIONE E L'EDITORIA,** *Campagna contro la pirateria digitale con Bobo Vieri*, 2023.

[139] **GABBANELLI C.,** *Pezzotto: cos'è, come funziona e quali sono i rischi*, Lexplain, 2024, articolo disponibile su: https://www.lexplain.it/pezzotto/

funzionamento della piattaforma, si può prendere in considerazione una partita di calcio. Quando i detentori dei diritti individuano uno streaming abusivo, utilizzano Piracy Shield per denunciare l'infrazione, e caricano gli indirizzi IP o i domini che trasmettono illegalmente la partita. Da quel momento, gli operatori di rete hanno un tempo massimo di 30 minuti per oscurare l'accesso a quei flussi illeciti. Questo meccanismo di risposta rapida è stato sviluppato per colpire duramente la pirateria e per ridurre drasticamente il tempo in cui i contenuti illegali restano accessibili. Con il supporto di Piracy Shield si vuole scoraggiare l'uso di piattaforme illegali e proteggere l'industria audiovisiva italiana, in modo da garantire che i contenuti vengano consumati solo attraverso canali legali.[140]

Piracy Shield è una piattaforma avanzata per contrastare la pirateria digitale, in particolare per quanto riguarda i contenuti sportivi. Realizzata dalla startup innovativa SP TECH, in collaborazione con lo studio Previti, e ospitata sul cloud MICROSOFT AZURE, Piracy Shield opera come una sorta di *guardiano* automatizzato, capace di rilevare e oscurare rapidamente i siti che trasmettono contenuti illegalmente. Nel dettaglio, il funzionamento della piattaforma prevede quattro passaggi: la segnalazione dei contenuti illegali, la creazione e gestione del ticket, l'oscuramento automatico, e infine, la creazione di una white list e i controlli[141].

Il primo passaggio è la segnalazione dei contenuti illegali. In questa fase, i detentori dei diritti, quali ad esempio Sky o Dazn, possono caricare sulla piattaforma gli indirizzi IP o i Fully Qualified Domain Name (FQDN) dei siti pirata che trasmettono contenuti senza autorizzazione. Il FQDN è un nome di dominio completo e preciso che identifica chiaramente una risorsa online. Insieme agli indirizzi o ai domini, i detentori dei diritti devono fornire prove forensi che attestino la violazione, in modo da garantire che le segnalazioni siano basate su evidenze concrete. Una volta caricati i dati, si passa alla seconda fase in cui Piracy Shield genera un ticket che include la segnalazione nella lista dei siti da oscurare. Questo processo avviene in pochi minuti e, se necessario, chi effettua la segnalazione ha un breve lasso di tempo per correggere eventuali errori prima che il ticket venga finalizzato. Il terzo passaggio riguarda l'oscuramento automatico, in cui gli operatori di telecomunicazioni e di rete, collegati a Piracy Shield tramite una VPN (Virtual Private Network), hanno trenta minuti di tempo per oscurare i siti segnalati. Il sistema può operare anche in automatico:

[140] **ANGIUS R. e ZORLONI L.,** *Piracy Shield, come funziona la piattaforma nazionale per oscurare lo streaming illegale*. *Wired Italia*, 2023 articolo disponibile su: https://www.wired.it/article/piracy-shield-piattaforma-agcom-pezzotto-streaming-illegale/

[141] Ibidem

ad esempio, l'Associazione Italiana Internet Provider (AIIP) ha sviluppato un'interfaccia che verifica ogni 1-2 minuti l'aggiornamento della lista dei siti da oscurare, eseguendo le richieste in tempo reale. Piracy Shield, infine, contiene anche una white list, ossia una lista di risorse che non devono essere oscurate, in modo da garantire che i blocchi siano mirati solo ai contenuti illegali. Sebbene il sistema preveda anche una funzione di sblocco e una per la segnalazione di errori, queste operazioni sono regolamentate in modo diverso e richiedono ulteriori procedure, sui cui l'AGCOM sta ancora lavorando. Piracy Shield non solo rappresenta un avanzamento tecnologico nel contrasto alla pirateria, ma è anche un potenziale sostituto delle vie legali tradizionali. Gli operatori dei contenuti possono, infatti, ricorrere alla piattaforma per ottenere la rimozione rapida dei contenuti illegali, senza dover necessariamente passare per i tribunali. Tuttavia, questo processo di accreditamento richiede che le segnalazioni siano corredate da una descrizione dettagliata del motivo per cui si richiede l'oscuramento. La piattaforma è perfettamente in grado di agire con grande velocità e precisione, ma la sua automatizzazione solleva anche alcune preoccupazioni riguardo alla possibilità di errori e alla mancanza di controllo umano diretto nel processo di oscuramento. Nonostante ciò, Piracy Shield rappresenta una risposta concreta e tecnologicamente avanzata alla crescente minaccia della pirateria digitale, soprattutto in un contesto in cui lo streaming illegali è in forme aumento, come dimostrato dall'incremento del 26% dei contenuti sportivi piratati tra il 2021 e il 2022[142].

Piracy Shield, concepito come uno strumento innovativo per contrastare la pirateria digitale, soprattutto nello streaming illegali di eventi sportivi, ha incontrato notevoli difficoltà nella sua implementazione, mettendo in luce diversi limiti che ne compromettono l'efficacia. Come già detto, il Piracy Shield è stato introdotto in risposta alla crescente diffusione di contenuti piratati, in particolare nel contesto sportivo, dove la trasmissione illegale di partite di calcio e altri eventi ha raggiunto proporzioni significative. Istituito con L. 93/2023, il Piracy Shield rappresenta una delle misure più concrete adottate dall'Autorità Garante delle Comunicazioni (AGCOM) per tutelare il diritto d'autore in modo tempestivo, senza dover ricorrere a lunghi procedimenti legali. Nonostante le buone intenzioni e la necessità di uno strumento del genere, il Piracy Shield ha mostrato seri problemi fin dai primi momenti della sua operatività. Uno dei principali limiti risiede nella mancanza di un controllo umano diretto nel processo di oscuramento dei siti, che avviene in modo quasi totalmente automatizzato. Questa automatizzazione ha sollevato parecchie preoccupazioni riguardo

[142] **ANGIUS R. e ZORLONI L.,** *Piracy Shield, come funziona la piattaforma nazionale per oscurare lo streaming illegale*. *Wired Italia*, 2023 articolo disponibile su: https://www.wired.it/article/piracy-shield-piattaforma-agcom-pezzotto-streaming-illegale/

alla possibilità di errori: siti legittimi potrebbero essere oscurati per errore, e il processo di sblocco è complicato e non sempre tempestivo. Inoltre, l'efficacia del sistema è stata messa in discussione. Nonostante l'obbligo per gli operatori di oscurare i siti entro 30 minuti, i pirati digitali hanno spesso dimostrato una capacità straordinaria di adattarsi e riorganizzarsi rapidamente, creando nuovi domini o indirizzi IP per eludere i blocchi. Un'altra critica riguarda il fatto che Piracy Shield, pur essendo uno strumento necessario, non è stato sviluppato in modo ottimale. La piattaforma sembra soffrire di una mancanza di test approfonditi prima del lancio ufficiale, il che ha portato a una serie di malfunzionamenti e difficoltà operative. Questo problema si aggrava se si considera che Piracy Shield ha il compito delicato di proteggere i diritti d'autore in un contesto dove la velocità d'intervento è cruciale, specialmente durante eventi sportivi in diretta[143].

Uno dei principali problemi di Piracy Shield è la sua limitata efficacia geografica. Le misure di oscuramento dei siti incriminati funzionano solo per chi si connette dall'Italia. Questo significa che si utilizza una VPN può facilmente aggirare i blocchi imposti, rendendo l'intero sistema inefficace per chi sa come nascondere la propria posizione. Un'altra grave criticità riguarda il rischio di oscuramento di siti legittimi, che non hanno nulla a che fare con la pirateria. Questo problema deriva dal fatto che molti indirizzi IP possono essere condivisi tra più siti web. Un esempio evidente è quello dei servizi come Cloudflare, che fungono da Content Delivery Network (CDN) per migliaia di siti. Se un sito pirata condivide l'IP con siti legittimi, tutti possono essere bloccati senza distinzione. Questo problema era stato anticipato dall'opposizione durante la fase di discussione della legge, con la proposta di creare una white list di siti da proteggere, ma questa fase è comunque ancora in fase di completamento. I problemi tecnici del Piracy Shield sono stati ulteriormente aggravati da errori operativi. Durante un'audizione alla Camera, il presidente di AGCOM ha riconosciuto che ci sono stati problemi, come l'oscuramento di indirizzi IP legati a Cloudflare, che ha reso irraggiungibili migliaia di siti web legittimi. Inoltre, è emerso che la lista degli interventi di oscuramento non è trasparente e non c'è un obbligo legali di pubblicazione. Ciò rende difficile per i siti colpiti ingiustamente ottenere una notifica tempestiva e presentare ricorso. Le problematiche del Piracy Shield non si limitano ai suoi malfunzionamenti operativi. Un leak del codice sorgente della piattaforma su GitHub ha rilevato falle significative nel design e nell'implementazione del sistema. Questo leak suggerisce che la piattaforma è stata sviluppata in modo approssimativo e potenzialmente vulnerabile. Oltre, ai problemi tecnici, sono stati esposti anche i nomi delle persone che hanno

[143] **PASTORELLA G.** *Piracy Shield, tutte le falle dell'antipirateria di Stato*, Agenda Digitale, 2024

lavorato al codice, violando così la legge sulla privacy. Di fronte a questi gravi problemi, diverse voci, tra cui l'Unione Nazionale Consumatori, hanno chiesto la sospensione della piattaforma. Questo permetterebbe di correggere le criticità e di tutelare meglio gli utenti, che al momento rischiano di subire danni ingiusti. Una delle priorità dovrebbe essere migliorare la trasparenza del sistema, in modo che chi subisce un blocco ingiusto possa essere informato tempestivamente e avere un tempo ragionevole per presentare ricorso. In conclusione, Piracy Shield rappresenta un passo avanti importante nella lotta alla pirateria digitale, ma la sua implementazione è stata finora segnata da notevoli difficoltà. La necessità di proteggere i contenuti digitali, soprattutto in un settore redditizio come quello sportivo, è evidente, ma per raggiungere gli obiettivi prefissati sarà necessario rafforzare e migliorare questo strumento, affrontando i limiti tecnici e procedurali emersi nelle prime fasi di utilizzo. La speranza è che, con ulteriori sviluppi e miglioramenti, la piattaforma Piracy Shield possa effettivamente diventare l'arma efficace contro la pirateria, senza compromettere i diritti dei legittimi titolari dei contenuti ne quelli degli utenti che navigano online. Per evitare che continui a causare danni collaterali significativi, è necessario un ripensamento e un miglioramento delle sue modalità operative[144].

Oltre alla piattaforma Piracy Shield esistono diversi strumenti tecnici sul mercato per contrastare le violazioni del diritto d'autore, e in particolare del pezzotto, ciascuno con caratteristiche specifiche e un ambito di applicazione che varia a seconda dell'uso che ne viene fatto. Questi strumenti sono principalmente utilizzati all'interno di organizzazioni private e pubbliche, dove si cerca di limitare l'accesso a contenuti illegali o non autorizzati su Internet. Tuttavia, la loro efficacia diminuisce quando vengono applicati nel contesto delle reti residenziali di banda larga, in parte perché gli utenti domestici possono facilmente aggirarli. Tra questi strumenti possiamo citare la tecnologia Deep Packet Inspection (DPI), il blocco delle IPTV a livello di DNS, l'identificazione e l'oscuramento degli IP, il tracciamento dei flussi video e watermarking e, infine, la collaborazione internazionale e le azioni legali.

La Deep Packet Inspection (DPI) è una tecnologia avanzata di filtraggio dei dati in transito su reti a commutazione di pacchetto, come Internet, che consente di esaminare non solo l'intestazione dei pacchetti, ma anche il loro contenuto, noto come payload. Questa capacità permette di identificare contenuti specifici all'interno dei pacchetti dati e di agire in base a criteri prestabiliti dall'operatore o

[144] **PASTORELLA G.,** *Piracy Shield, tutte le falle dell'antipirateria di Stato*, Agenda Digitale, 2024

dai fornitori di servizi Internet (ISP). La DPI viene utilizzata per una varietà di scopi, tra cui l'identificazione di anomalie nei protocolli di rete, la rilevazione di intrusioni, la prevenzione della propagazione di virus e l'ottimizzazione del traffico di rete. Inoltre, può essere impiegata per raccogliere dati statistici sull'utilizzo della rete, fornendo agli ISP informazioni dettagliate sul comportamento degli utenti. Una delle principali differenze tra la Deep Packet Inspection e altre forme di Packet Inspection è la sua capacità di analizzare non solo le informazioni di intestazione, come gli indirizzi IP e i numeri di porta, ma anche i dati contenuti nei pacchetti stessi. Questo significa che la DPI può identificare e intervenire su flussi di pacchetti che condividono caratteristiche simili, rendendola uno strumento potente per il controllo del traffico di rete. Grazie a queste caratteristiche, la DPI è ampiamente utilizzata dagli ISP e dagli operatori di telecomunicazioni (TLC) per ottimizzare e dare priorità al traffico sulla propria rete. Ad esempio, può essere utilizzata per ridurre la larghezza di banda destinata ad applicazioni P2P, limitando così il traffico associato a pratiche di file sharing non autorizzato. Inoltre, la DPI viene adottata anche da organizzazioni governative per fini di intelligence, permettendo un controllo e un monitoraggio approfondito delle comunicazioni digitali. In ambito aziendale, la DPI può essere integrata in firewall evoluti per contrastare tentativi di traffico P2P offuscato, così facendo l'integrità della rete sarà protetta e si potrà prevenire la fuoriuscita di dati sensibili. Tuttavia, la Deep Packet Inspection presenta alcuni limiti significativi. Uno dei principali è la violazione della privacy degli utenti, poiché l'analisi dettagliata dei dati di rete implica un livello di sorveglianza che può essere considerato invasivo. Inoltre, la DPI è una tecnologia complessa e costosa da implementare e richiede infrastrutture avanzate e competenze tecniche elevate per essere gestita efficacemente. Un altro problema riguarda il suo potenziale conflitto con i principi della neutralità della rete, i quali prevedono un trattamento equo di tutto il traffico di Internet, senza discriminazioni basate sul contenuto o sul tipo di applicazione. L'uso su vasta scala della DPI potrebbe, inoltre, contrastare con i principi di libertà democratica, poiché potrebbe essere impiegata per monitorare e controllare in modo invasivo le comunicazioni online, limitando così la libertà di espressione e il libero accesso alle informazioni. Queste preoccupazioni sollevano importanti questioni etiche e legali sull'impiego della Deep Packet Inspection in contesti sia pubblici che privati[145].

Il blocco a livello di Domain Name System (DNS) è una strategia sempre più utilizzata nella lotta contro la pirateria digitale, in particolare contro i servizi illegali di IPTV. Questo metodo sfrutta

[145] **AGCOM,** *Indagine Conoscitiva. Il diritto d'autore sulle reti di comunicazione elettronica.*

il ruolo centrale che i server DNS giocano nell'ecosistema di Internet. Il Domain Name System (DNS) è il sistema che traduce i nomi di dominio leggibile (www.esempio.com) in indirizzi IP numerici (220.0.3.1) che i computer utilizzano per identificare le risorse su Internet. Quando un utente inserisce un indirizzo web nel browser, il server DNS si occupa di trovare l'indirizzo IP associato a quel dominio, permettendo la connessione al sito richiesto. Nel contesto del blocco DNS, gli ISP configurano i loro server DNS per impedire la risoluzione dei nomi di dominio associati a servizi di IPTV pirata o a siti che facilitano la distribuzione illegale di contenuti protetti dal diritto d'autore. Quando un utente tenta di accedere a uno di questi domini bloccati, il server DNS dell'ISP restituisce un errore o reindirizza l'utente a una pagina di avviso, informandolo che il sito è stato bloccato per violazioni del diritto d'autore. Il blocco DNS è particolarmente efficace contro siti noti che forniscono contenuti piratati. Poiché la maggior parte degli utenti si affida ai server DNS forniti dal proprio ISP, un blocco a questo livello può impedire l'accesso alla maggioranza dei visitatori. Per gli ISP, implementare un blocco DNS è relativamente semplice e non richiede modifiche sostanziali all'infrastruttura di rete. Questo rende il blocco DNS una soluzione economica e immediata per contrastare la pirateria. Il blocco DNS può essere rapidamente aggiornato per includere nuovi domini man mano che emergono, rendendo possibile una risposta dinamica alle evoluzioni del mercato della pirateria. Uno dei principali limiti del blocco DNS è che può essere facilmente aggirato. Gli utenti con un minimo di conoscenza tecnica possono configurare il proprio dispositivo per utilizzare server DNS alternativi, come quelli forniti da Google, che non applicano blocchi imposti dagli ISP. Inoltre, esistono strumenti e servizi che permettono di bypassare il blocco DNS, come VPN e i proxy. Per ovviare ai limiti del blocco DNS, questa tecnica viene spesso combinata con altre misure antipirateria, quali ad esempio le Deep Packet Inspection. Come abbiamo già detto, la DPI consente di esaminare il contenuto dei pacchetti di dati in transito. Questo permette di individuare e bloccare le trasmissioni illegali anche se queste utilizzano tecniche di offuscamento o bypassano il DNS. La combinazione di DPI e blocco DNS può migliorare l'efficacia delle misure antipirateria[146].

Un metodo complementare consiste nell'identificazione e l'oscuramento degli indirizzi IP dei server che ospitano i servizi IPTV illegali. Questi sono metodi cruciali nella lotta contro la pirateria, in quanto vengono utilizzati per identificare e impedire l'accesso ai server che forniscono contenuti illegali. Questo approccio richiede un monitoraggio costante e l'aggiornamento regolare delle liste di indirizzi IP associati a queste attività, poiché i pirati cambiano frequentemente server e

[146] **HERZOG E. e HOFMANN C.,** *No ai blocchi di rete e all'isolamento digitale,* Economieswisse Dossier Politica, 2018.

indirizzi IP per eludere i controlli. In Canada, ad esempio, un'operazione di blocco degli IP ha dimostrato la sua efficacia nel ridurre la disponibilità di contenuti pirata, con l'implementazione di blocchi IP durante eventi live come le partite della NHL. In questo caso, le autorità utilizzano tecnologie avanzate per identificare e confrontare i contenuti trasmessi illegalmente con quelli legittimi, bloccando di conseguenza gli IP incriminati. Tuttavia, l'implementazione su larga scala di questo metodo può portare a sfide significative, come la necessità di bilanciare l'efficacia del blocco con il rischio di *overblocking,* ovvero il blocco accidentale di indirizzi IP legittimi[147]. Un altro esempio viene dal Regno Unito, dove SKY ha adottato un approccio proattivo, bloccando migliaia di domini associati a servizi IPTV illegali. Questo blocco è stato possibile grazie all'uso di ingiunzioni dinamiche, che permettono di adattare il blocco in tempo reale a seconda delle necessità. La strategia include anche il monitoraggio delle nuove tecniche utilizzate dai pirati, come l'uso di algoritmi per la generazione di nuovi domini, che richiedono un aggiornamento continua delle tecniche di blocco. In sintesi, il blocco degli IP rappresenta una strategia efficace, ma complessa, che richiede risorse significative per essere mantenuta nel tempo e per garantire che venga applicata in modo mirato ed efficace[148].

Un altro strumento utile a combattere la pirateria è il watermarking. Il watermarking rappresenta una delle tecnologie più sofisticate per tracciare e identificare le origini di flussi video pirata. Questo sistema funziona integrando all'interno del video un marchio digitale, un modello di bit non visibili che non possono essere rimossi senza compromettere la qualità del video. Questi bit sono collegati all'identità dello spettatore, e consentono di risalire a chi ha distribuito illegalmente il contenuto dopo che è stato decrittografato. Esistono vari metodi di watermarking, tra cui modifica di bitstream, watermarking lato client e watermarking con variante A/B. La modifica di bitstream è un metodo che edita alcune parti del bitstream del video, conservando la qualità dell'immagine e rendendo possibile l'identificazione dello spettatore e della sessione. È un metodo robusto, ma richiede un elevato carico di elaborazione e introduce latenza. Ciò lo rende inadatto per i contenuti live. Il watermarking lato client consiste nell'applicare la filigrana al flusso video direttamente nel dispositivo del cliente, tramite una sovrapposizione grafica invisibile o visibile. Questo metodo è utile per estrarre rapidamente la filigrana e può essere implementato su dispositivi più datati e set-top box. Tuttavia, poiché la filigrana viene aggiunta solo una volta che il video raggiunge il dispositivo del cliente, lo streaming necessita di una protezione aggiuntiva. Invece, il watermarking con variante A/B

[147] **MAXWELL A.,** *Canadian ISPs blocked pirate IPTV & logged customer IP Adresses*, 2023.
[148] Ibidem

viene principalmente utilizzato in ambito OTT (Over The Top), questo metodo crea due flussi video identici ma con diverse filigrane. I flussi vengono poi uniti o interlacciati nel dispositivo client o attraverso l'elaborazione Edge CDN (Content Delivery Network) per generare un identificatore univoco. È un metodo efficace e conveniente, ma non ideale per contesti in cui è necessaria un'estrazione rapida della filigrana. L'elemento chiave per l'efficacia del watermarking è l'utilizzo di un sistema di monitoraggio continuo, che permette di identificare e contrastare rapidamente i pirati. Questo può essere gestito internamente o essere affidato a servizi di monitoraggio esterni. Aziende come AKAMAI collaborano con fornitori di servizi di watermarking per garantire l'integrazione di queste soluzioni all'interno di una strategia antipirateria globale[149].

Infine, per combattere efficacemente la pirateria digitale, e in particolare quella legata ai servizi IPTV illegali, è fondamentale la cooperazione internazionale. Molti server si trovano in Paesi con legislazioni meno rigide, e rendono necessaria una stretta collaborazione tra le autorità italiane e organismi internazionali come Europol e Eurojust. In questo contesto, operazioni su larga scala, come l'operazione *Eclissi,* hanno coinvolto diversi Paesi europei per oscurare piattaforme IPTV illegali e sequestrare i server coinvolti[150]. Le autorità italiane, in collaborazione con partner internazionali, sono riuscite a smantellare reti criminali transnazionali, e hanno sequestrato beni e strumenti utilizzati per la trasmissione di contenuti piratati. Queste operazioni spesso portano a procedimenti legali contro i responsabili, inclusi il sequestro di apparecchiature e l'irrogazione di pesanti sanzioni economiche, che possono scoraggiare ulteriori attività illecite. La chiusura dei server e l'oscuramento dei siti web sono accompagnati da azioni legali, che possono includere il sequestro di ingenti somme di denaro e di risorse digitali, nonché l'individuazione e la sanzione degli utenti finali che fruiscono di questi servizi illegali. Questi sforzi congiunti sono cruciali per proteggere i diritti degli operatori legittimi e garantire un mercato digitale equo[151].

Il contrasto al pezzotto, quindi, richiede un approccio integrato che combini tecnologie avanzate, azioni legali e sensibilizzazione del pubblico. Mentre le piattaforme di blocco automatico, il DPI, il blocco DNS, e l'oscuramento degli IP rappresentano soluzioni tecniche efficaci, la collaborazione internazionale e le campagne di sensibilizzazioni sono cruciali per ridurre l'attrattiva

[149] **AKAMAI**, *Protezione dei dati OTT*. Report disponibile su: https://www.akamai.com/site/it/documents/white-paper/protecting-the-bank-of-ott-whitepaper.pdf

[150] **CARRÀ M.,** *Tv pirata, è partita la caccia europea: coinvolti 5 milioni di italiani,* 2019 articolo disponile su money.it

[151] **GIUFFRE' A.,** *Pirateria, operazione internazionale: sequestrati oltre 5500 siti, sanzionati gli utenti* 2020 *https://tg24.sky.it/cronaca/2020/11/11/operazione-internazionale-pirateria*

della pirateria e promuovere l'utilizzo di contenuti legali. La natura evolutiva della pirateria digitale richiede un continuo aggiornamento delle tecnologie e delle strategie di contrasto per proteggere l'industria audiovisiva e sportiva italiana.

3. IL CONTRASTO AL PEZZOTTO TRAMITE IL DIRITTO PENALE

Il pezzotto è, quindi, un termine gergale che si riferisce alla visione illegale di contenuti audiovisivi, come partite di calcio, film e serie TV, attraverso dispositivi o servizi non autorizzati che permettono di aggirare i diritti d'autore e le licenze ufficiali. Questo fenomeno, che ha preso piede in Italia e in molti altri Paesi, costituisce un grave violazione del diritto d'autore e può avere significative conseguenze legali. In Italia, il contrasto al pezzotto viene affrontato attraverso una serie di normative penali che mirano a tutelare i diritti d'autore e a reprimere le attività illecite connesse alla pirateria digitale. Le principali disposizioni sono contenute nel Codice penale e nella Legge sul Diritto d'Autore (L. n. 633/1941).

Come già anticipato nei capitoli precedenti, l'art. 171-bis l. n. 633/1941 punisce chiunque, senza averne diritti e a scopo di lucro, duplica, distribuisce o comunica al pubblico opere protette dal diritto d'autore. Le sanzioni possono includere pene detentive fino a 3 anni e multe consistenti. L'uso del pezzotto rientra in queste fattispecie, in quanto comporta la fruizione di contenuti protetti senza autorizzazione. Il diritto penale italiano affronta il contrasto alla pirateria e alla violazione del diritto d'autore attraverso una serie di disposizioni che mirano a tutelare non solo i diritti economici dei creatori, ma anche l'integrità del mercato legale dei contenuti. Nello specifico, la norma che sanziona penalmente il cosiddetto pezzotto e altre condotte simile, è articolata in diverse fattispecie che coprono una vasta gamma di comportamenti illeciti. Il reato è configurato da una serie di condotte alternative, tutte considerate lesive del diritto d'autore. Tra queste, la duplicazione di programmi per elaboratore, l'importazione, la distribuzione, la vendita, e la detenzione a scopo commerciale o imprenditoriale di programmi contenuti in supporti non contrassegnati dalla SIAE. Inoltre, la legge punisce anche la concessione in locazione di tali programmi e la riproduzione o trasferimento su altri supporti di contenuti di una banca dati senza autorizzazione. Altre condotte rilevanti includono la comunicazione o presentazione in pubblico di contenuti protetti, nonché l'estrazione e il reimpiego di banche dati in violazione delle disposizioni vigenti. Tutte queste attività, se realizzate senza il consenso dei titolari dei diritti d'autore, integrano il reato di violazione delle norme sul diritto

d'autore. L'elemento soggettivo richiesto per la configurazione di questo reato è il dolo specifico. Ciò significa che l'autore del reato deve agire con la consapevolezza e la volontà di trarre un profitto dall'attività illecita. Non è sufficiente la mera commissione dell'atto illecito; è necessario che questo sia compiuto con l'intenzione specifica di ottenere un vantaggio economico o patrimoniale. Il momento di consumazione del reato coincide con la realizzazione di una delle condotte tipizzate. La prescrizione del reato è fissata in sei anni, salvo eventuali interruzioni che possono prolungare questo termine. Gli atti interruttivi della prescrizione, come previsto dall'art. 161 c.p., possono estendere ulteriormente la durata della prescrizione. Le sanzioni per chi commette questi reati sono particolarmente severe. La pena può variare da sei mesi a tre anni di reclusione, accompagnata da una multa che può andare da 2.500 a oltre 25.000 euro. Nei casi di maggiore gravità, la reclusione minima è di due anni, con una multa che non può essere inferiore a 30.000 euro. Questo inasprimento delle pene riflette la volontà del legislatore di contrastare in modo efficace la pirateria e proteggere i diritti d'autore. La procedibilità per questi reati è d'ufficio, il che significa che le autorità possono procedere senza necessità di una querela da parte della vittima. Questo approccio è stato adottato per garantire una tutela più ampia ed efficace contro la pirateria, vista la difficoltà per i singoli titolari di diritti d'autore di monitorare e segnalare tutte le violazioni[152].

Una delle normative utili a contrastare l'utilizzo del pezzotto è l'art. 640-ter c.p., il quale disciplina il reato di frode informatica. L'art. 640 c.p., cita testuali parole: *Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro. La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o taluna delle*

[152] **Art. 171 bis Legge 22/04/1941, n.633** – *Protezione del diritto d'autore*.

circostanze previste dall'articolo 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età, e numero 7[153].

L'art. 640-ter c.p. riprende elementi tipici del reato di truffa, con la differenza principale che il comportamento fraudolento non è rivolto direttamente contro una persona, ma contro un sistema informatico o telematico. In altre parole, il bene giuridico protetto è non solo il patrimonio, ma anche il corretto funzionamento dei sistemi informatici e la libertà di autodeterminazione del soggetto passivo. La fattispecie di reato si configura quando un individuo, attraverso l'alterazione o un intervento senza diritto su un sistema informatico o telematico, provoca un ingiusto profitto a proprio vantaggio o a vantaggio di terzi, con un conseguente danno per altri. L'intervento può avvenire in diverse modalità, come la manipolazione dei dati, delle informazioni, o dei programmi contenuti nel sistema. L'elemento soggettivo richiesto per la configurazione del reato è il dolo generico. Ciò significa che l'agente deve avere la consapevolezza e la volontà di alterare il funzionamento di un sistema informatico o di intervenire senza diritto su di esso, con l'intenzione di procurarsi un ingiusto profitto a danno altrui. Il reato si consuma nel momento in cui l'agente realizzata l'ingiusto profitto. Questo momento è cruciale per la determinazione della configurazione del reato e per il calcolo della prescrizione. Le sanzioni variano in base alla gravità del reato. Nelle ipotesi meno gravi, è prevista, al comma 1, la reclusione da 6 mesi a 3 anni e una multa da 51 a 1.032 euro. Nelle ipotesi aggravate, al comma 2, è prevista la reclusione da 1 a 5 anni. Nelle ipotesi più gravi, al comma 3, è prevista la reclusione da 2 a 6 anni e una multa da 600 a 3.000 euro. La procedibilità avviene a querela di parte. Qualora, invece, ricorrano circostanze aggravanti, come quelle previsti dai commi 2 e 3, la procedibilità sarà d'ufficio[154].

L'art. 615-ter c.p., che disciplina l'accesso abusivo ad un sistema informatico o telematico, rappresenta, anch'esso, uno strumento importante per il contrasto al pezzotto. L'articolo recita le seguenti parole: "*Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore*

[153] **PADOVANI T.,** *Diritto penale,* 12 ed., Giuffrè Francis Lefebvre, 2019
[154] Ibidem

del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio (art. 615-ter, Codice penale)[155].

La normativa penale in materia di accesso e mantenimento abusivo in sistemi informatici o telematici ha come obiettivo principale la protezione del diritto alla riservatezza del titolare legittimo di tali sistemi. In particolare, essa si prefigge di tutelare i sistemi informatici e telematici da accessi non autorizzati e da mantenimenti contrari alla volontà del legittimo titolare. Il reato previsto dalla legge si articola in due principali condotte illecite: introduzione abusiva in un sistema informatico o telematico protetto da misure di sicurezza e mantenimento nel sistema informatico o telematico contro la volontà espressa o tacita del legittimo titolare del sistema. La prima comporta l'accesso non autorizzato a un sistema informatico che ha implementato misure di protezione. La seconda invece si riferisce alla permanenza nel sistema, nonostante il titolare del sistema abbia espresso o implicitamente indicato il desiderio di non consentire l'accesso. Il delitto in questione richiede il dolo generico, ovvero la coscienza e volontà di introdursi nel sistema informatico o telematico in modo abusivo, oppure di mantenervisi contro la volontà del legittimo titolare. Poiché si tratta di un reato di pericolo, il momento di consumazione del reato coincide con l'effettivo accesso al sistema informatico o telematico, o con il momento in cui il soggetto permane abusivamente nel sistema. Le sanzioni previste per questo tipo di reato variano a seconda della gravità e delle circostanze specifiche. Al comma 1, la pena prevista è la reclusione fino a 3 anni. Al comma 2, in circostante aggravate, la pena può arrivare da 1 a 5 anni di reclusione. E infine, in casi di maggiore gravità previsti dal comma 3, le pene possono variare da 1 a 5 anni di reclusione per la condotta di cui al comma 1, da 3 a 8 anni di reclusione per la condotta di cui al comma 2. Le modalità di procedibilità differiscono a seconda della gravità del reato. Il comma 1, ci dice che il reato può essere perseguito solo a querela di parte, ovvero su richiesta della persona offesa. I commi 2 e 3, invece indicano che la procedibilità è

[155] **PADOVANI T.,** *Diritto penale,* 12 ed., Giuffrè Francis Lefebvre, 2019

d'ufficio; quindi, il reato può essere perseguito anche senza querela della parte offesa. La competenza per i reati previsti è attribuita al Tribunale monocratico, che giudica in prima istanza. Anche i termini di prescrizione variano a seconda della gravità del reato: per i reati citati dai commi 1 e 2, il termine di prescrizione è di 6 anni, per i reati presenti al comma 3, il termine di prescrizione è di 8 anni. È importante comunque notare che questi termini possono essere prorogati per effetto di atti interruttivi ai sensi dell'art. 161 del Codice penale. In sintesi, il sistema normativo si propone di tutelare l'integrità e la riservatezza dei sistemi informatici e telematici attraverso un sistema di norme che definiscono le condotte illecite, stabiliscono le sanzioni e regolano le modalità di procedibilità e i termini di prescrizione, assicurando così una protezione adeguata contro gli accessi non autorizzati e le permanenze abusive[156].

Chi utilizza il pezzotto o altra forma di pirateria online può anche essere accusato di ricettazione, ai sensi dell'art. 648 c.p. La normativa recita il seguente testo: *Fuori dei casi di concorso nel reato [110], chi, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare, è punito con la reclusione da due ad otto anni e con la multa da 516 euro a 10.329 euro. La pena è aumentata quando il fatto riguarda denaro o cose provenienti da delitti di rapina aggravata ai sensi dell'articolo 628, terzo comma, di estorsione aggravata ai sensi dell'articolo 629, secondo comma, ovvero di furto aggravato ai sensi dell'articolo 625, primo comma, n. 7-bis) [379, 648-ter, 649, 709, 712]. La pena è della reclusione sino a sei anni e della multa sino a 516 euro, se il fatto è di particolare tenuità [62n. 4, 133]. Le disposizioni di questo articolo si applicano anche quando [648-bis] l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile [85] o non è punibile [46, 379, 649] ovvero quando manchi una condizione di procedibilità [336–346 c.p.p.] riferita a tale delitto.*

La ricettazione è un reato previsto dall'art. 648 del Codice penale italiano. Rappresenta una delle fattispecie attraverso cui il legislatore ha cercato di tutelare in maniera incisiva sia il patrimonio delle persone sia il corretto funzionamento della giustizia. La ricettazione, infatti, si inserisce in un contesto più ampio di criminalità, in quanto presuppone sempre l'esistenza di un reato precedente dal quale derivi un bene illecito. Questo la rende particolarmente significativa perché colpisce chi, pur non avendo partecipato direttamente al crimine originario, contribuisce a mantenere vivo il ciclo della criminalità, appropriandosi, acquistando o gestendo i proventi di quel reato. Il principale obiettivo

[156] **PADOVANI T.,** *Diritto penale,* 12 ed., Giuffrè Francis Lefebvre, 2019

della norma è quello di proteggere il patrimonio delle persone, ma non solo: la ricettazione mira anche a salvaguardare l'integrità dell'amministrazione della giustizia. Questo secondo aspetto è cruciale, perché punire chi ricetta beni di provenienza illecita significa evitare che i frutti di un reato restino nascosti, impedendo alla giustizia di recuperare tali bene e di perseguire efficacemente i responsabili del reato principale. In questo senso, la ricettazione non è solo una questione di beni materiali, ma coinvolge direttamente il funzionamento della giustizia. La ricettazione è un reato che può essere commesso da chiunque, con l'eccezione dell'autore del reato originario e della vittima. Ciò significa che, per essere considerato un ricettatore, una persona deve essere estranea ai fatti che hanno generato il bene illecito. L'esclusione dell'autore del reato principale e della vittima dalla possibilità di essere accusati di ricettazione è coerente con la logica della norma. Di fatti, il ricettatore è colui che si approfitta del crimine già avvenuta e ne perpetua gli effetti attraverso il possesso o la gestione dei beni derivanti dal reato. Il reato si realizzata attraverso una serie di condotte specifiche, che la legge individua in modo chiaro e trasparente: l'acquisto, la ricezione, l'occultamento dei beni di provenienza illecita, o anche l'intromissione nella gestione di tali bene. Quello che accomuna tutte queste condotte è l'intenzione del soggetto di ottenere un profitto. Questa finalità lucrativa è ciò che distingue la ricettazione da altre figure di reato che possono, in apparenza, sembrare simili. È proprio il dolo specifico, e quindi la volontà di trarre un vantaggio economica, che qualifica la condotta come ricettazione. L'illecito si consuma nel momento in cui il soggetto attivo compie una delle condotte indicate. Non è necessario che il profitto si realizzi effettivamente, ma basta che l'azione sia finalizzata a tale scopo. Le sanzioni previste per la ricettazione sono piuttosto severe, a testimonianza della gravità con cui il legislatore considera questo reato. Si parla di una reclusione che può variare da due a otto anni, accompagnata da una multa che va da 516 a 10.329 euro. In presenza di circostanze aggravanti, la pena può essere ulteriormente aumentata, mentre nei casi meno gravi, si prevede una reclusione fino a sei anni e una multa ridotta. Il reato di ricettazione è procedibile d'ufficio, il che significa che le autorità possono avviare l'azione penale indipendentemente da una denuncia da parte della vittima. Questo aspetto evidenza l'interesse pubblico a perseguire la ricettazione, considerata una minaccia non solo per i singoli individui, ma per l'intera società. La competenza per giudicare questo reato spetta al Tribunale monocratico, il quale si occupa delle cause in primo grado. Infine, i termini di prescrizione per il reato di ricettazione sono fissati in otto anni, ridotti a sei per i casi meno gravi. Tuttavia, questi termini possono essere interrotti da specifici atti processuali, come previsto dall'art. 161 c.p., il che può allungare il tempo entro in cui il reato può essere perseguito. In sintesi, la ricettazione è un reato complesso e multiforme che colpisce non solo chi compie direttamente atti

di criminalità, ma anche chi, indirettamente, partecipa al ciclo del crimine sfruttandone i proventi. La sua rilevanza va oltre la semplice appropriazione di beni, incidendo profondamente sulla tutela del patrimonio e sull'efficacia dell'amministrazione della giustizia. Di conseguenza, chi viene trovato in possesso di un pezzotto può essere perseguito penalmente per ricettazione se si dimostra che sapeva della natura illegale del dispositivo e lo utilizzava intenzionalmente per ottenere un vantaggio economico[157].

Il fenomeno del pezzotto è, quindi, un esempio emblematico di come la criminalità digitale possa impattare gravemente su diversi settori economici e sulla tutela dei diritti d'autore. In ambito penale, l'uso di questi dispositivi rientra nella violazione delle normative sulla proprietà intellettuale, quali ad esempio la contraffazione, ai sensi dell'art. 473 c.p., con possibili configurazioni di reati come la ricettazione, la frode informatica, e le violazioni del diritto d'autore previste dalla l. 633/41. La guardia di finanza ha intensificato le operazioni per contrastare la diffusione e l'uso del pezzotto, considerato un danno per le emittenti televisive e anche una pratica che alimenta i circuiti di criminalità organizzata. La GDF, insieme alle autorità giudiziarie, sta utilizzando strumenti investigativi avanzati per monitorare le reti IPTV illegali, rintracciare i distributori e sequestrare i dispositivi incriminati. Un esempio significativo è stato un blitz coordinato dalla Guardia di Finanza di Ancona, che ha portato all'arresto di 15 persone coinvolte in un vasto sistema di IPTV illegali. Questo intervento ha permesso di smantellare un'intera rete che gestiva l'accesso illecito a contenuti audiovisivi e ha dimostrato l'efficacia dell'azione penale contro tali crimini[158].

Dal punto di vista legale, la normativa italiana è piuttosto chiara: chi utilizza o distribuisce dispositivi come il pezzotto può essere accusato di vari reati. In particolare, l'art. 171-octies della legge sul diritto d'autore prevede sanzioni sia pecuniarie che detentive. Tuttavia, non è escluso che possano essere contestati anche reati come l'associazione a delinquere (art. 416 c.p.), se si dimostra l'esistenza di un'organizzazione criminale volta a diffondere questi dispositivi. Gli utenti finali, spesso ignari delle conseguenze legali, rischiano anch'essi pesanti sanzioni. Oltre alle multe, che possono raggiungere i 25.000 euro, c'è la possibilità di essere perseguiti penalmente con pene detentive fino a tre anni. Questo crea un precedente importante, volto a scoraggiare l'uso del pezzetto e a proteggere i diritti dei legittimi titolari dei contenuti.

---

[157] **PADOVANI T.,** *Diritto penale,* 12 ed., Giuffrè Francis Lefebvre, 2019

[158] **CARUSO D.,** (2024). *Pezzotto, arrestate 15 persone: le azioni della Guardia di Finanza*, 2024, articolo disponibile su PianetaCellulare.it. https://www.pianetacellulare.it/articoli/pezzotto-arrestate-15-persone-le-azioni-della-guardia-di-finanza.php

CONCLUSIONE

La pirateria online è una delle problematiche più insidiose e diffuse del nostro tempo, un fenomeno che ha saputo adattarsi e crescere di pari passo con le innovazioni tecnologiche e i cambiamenti nei comportamenti dei consumatori. Come evidenziato nel corso di questa analisi, la pirateria non solo minaccia l'integrità economica delle industrie creative, ma ha anche profonde implicazioni sociali, culturali e legali. Nonostante gli sforzi congiunti a livello globale per arginare il fenomeno, attraverso leggi più severe, l'adozione di tecnologie avanzate come i sistemi DRM e l'implementazione di campagne educative, la pirateria continua a rappresentare una minaccia persistente. Le cause profonde della pirateria, radicate nella disparità di accesso ai contenuti, nei costi elevati dei prodotti digitali e nella percezione che l'informazione e la cultura debbano essere accessibili a tutti, non possono essere affrontate esclusivamente con misure punitive. È necessario un approccio più equilibrato e inclusivo, che comprenda non solo l'enforcement delle leggi, ma anche la promozione di soluzioni legali accessibili e attrattive per i consumatori. I successi ottenuti da alcune piattaforme di streaming legale, che hanno saputo offrire un'alternativa valida alla pirateria, dimostrano che la chiave per contrastare efficacemente questo fenomeno risiede nella capacità di rispondere alle esigenze e alle aspettative degli utenti.

Tuttavia, la lotta contro la pirateria è tutt'altro che vinta. Le tecnologie avanzano e con esse emergono nuove forme di pirateria, sempre più sofisticate e difficili da rilevare. Il crescente utilizzo di reti private virtuali (VPN), di software per il mascheramento dell'identità e di piattaforme decentralizzate come i Torrent, rende il compito delle autorità di contrasto sempre più arduo. Inoltre, l'integrazione della pirateria con altre forme di criminalità informatica, come il cybercrime, amplifica ulteriormente le sfide da affrontare. In questo contesto, è essenziale che tutti gli attori coinvolti – governi, aziende, organizzazioni internazionali e consumatori – lavorino insieme per sviluppare strategie efficaci e sostenibili. La cooperazione internazionale, la condivisione delle informazioni e lo sviluppo di nuove tecnologie di protezione sono passi fondamentali per ridurre l'impatto della pirateria. Al contempo, è cruciale continuare a educare il pubblico sulle conseguenze della pirateria e promuovere una cultura del rispetto per il diritto d'autore e il lavoro creativo.

In conclusione, la pirateria online rappresenta una sfida complessa e multifattoriale che richiede un approccio olistico e concertato. Solo attraverso una combinazione di misure legali, tecniche, educative e culturali sarà possibile contenere e, auspicabilmente, ridurre l'incidenza di

questo fenomeno, proteggendo al contempo il diritto degli autori e dei creatori di vedere riconosciuto il valore del loro lavoro. L'evoluzione della pirateria online e le strategie per il suo contrasto continueranno a essere temi di grande rilevanza per il futuro, riflettendo le tensioni tra innovazione tecnologica, diritti di proprietà intellettuale e accesso all'informazione in un mondo sempre più interconnesso.

SITOGRAFIA E BIBLIOGRAFIA

AGENZIA DELLE DOGANE, *L'impatto economico della contraffazione e della pirateria*, 2010

AGCOM, *Indagine Conoscitiva. Il diritto d'autore sulle reti di comunicazione elettronica.*

AGULAR L. e **MARTENS B.**, *Digital Music Consumption on the Internet: Evidence from Clickstream Data*, JRC Technical Reports, Institute for Prospective Technological Studies Digital Economy Working Paper 2013/04, Joint Research Centre, European Commission, 2013

AKAMAI, *Protezione dei dati OTT*.

ALIPRANDI S., *Capire il copyright. Percorso guidato nel diritto d'autore*, Ledizioni, 2012

ANDRIULO L., *Conseguenze penali e violazione diritto d'autore*, 2023

ANGIUS R. e **ZORLONI L.**, *Piracy Shield, come funziona la piattaforma nazionale per oscurare lo streaming illegale*, Wired Italia, 2023

ANTONIELLI A., *Cyber Crime: cos'è, come affrontarlo e difendersi in azienda*, Politecnico di Milano, 2024 https://blog.osservatori.net/it_it/cybercrime-definizione-italia

AUTERI P., *Il contenuto del diritto d'autore,* in AA.VV., *Il Diritto industriale,* 7 ed., Giappichelli, 2023, p. 625 ss.

AUTERI P., *Diritto d'autore,* in AA.VV., *Il Diritto industriale,* 7 ed., Giappichelli, 2023, p. 649 ss.

AVERSA A., *Cosa vuol dire pezzotto e perché si chiama così. Una parola che deriva dal dialetto napoletano ma che indica anche un tappeto prodotto al nord*, 2024

BACCI M., *Plagio Musicale e Contraffazione di Opera Musicale*, IPRights, 2020

BARILLARO A., *Cosa significa masterizzare e come si fa*, 2023

BENEGGI M., *Legalpop, cos'è la pirateria informatica, quali sanzioni ha*, 2021

BSA, *Seizing Opportunity Through License Compliance, Global Software Survey*, 2016

CAPRIO G., *Il peso della pirateria nel mondo del libro*, 2024

CARUSO D., *Pezzotto, arrestate 15 persone: le azioni della Guardia di Finanza*, 2024

CASO R., *Digital Right Management, Il commercio delle informazioni digitali tra contratto e diritto d'autore*, Ristampa digitale, Trento, 2006

CARRÀ M., *Tv pirata, è partita la caccia europea: coinvolti 5 milioni di italiani*, 2019

CROSS M., *Social Media Security. Leveraging Social Networking While Mitigating Risk*, 2013

CUNEGATTI B., *Manuale del diritto d'autore*, Editrice Bibliografica, 2020

D'AMMASSA G., *Dizionario dei termini di diritto di autore*, 2023

D'AMMASSA G., *Le difese e le sanzioni civili*, 2014

D'AMMASSA G., *Le difese e le sanzioni penali*, 2014

DANAHER B., **DHANASOBHON S.**, **SMITH D. M.** e **TELANG R.**, *Converting Pirates Without Cannibalizing Purchasers: The Impact of Digital Distribution on Physical Sales and Internet Piracy*, 2010.

DARA V., *La pirateria registra ancora centinaia di miliardi di visite e genera danni ingenti per l'industria dei media*, 2022

DIPARTIMENTO PER L'INFORMAZIONE E L'EDITORIA, *Campagna contro la pirateria digitale con Bobo Vieri*, 2023

DIRETTIVA 2004/48/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 29 aprile 2004 sul rispetto dei diritti di proprietà intellettuale

FAPAV, *Indagine FAPAV/IPSOS 2022*

FIMI, FPM – *Contro la pirateria musicale e multimediale*, 2024

FLOR R., *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di internet. Un'indagine comparata in prospettiva europea ed internazionale*, CEDAM, 2010

FLORIO A., *I sistemi di Digital Rights Management (DRM)*, 2009 https://www.dirittodellinformatica.it/diritto-autore/copyright-focus/i-sistemi-di-digital-rights-management-drm.html/

FRONTIER ECONOMICS, *The Economic Impacts of Counterfeiting and Piracy – Report prepared for BASCAP and INTA*, 2017

GABBANELLI C., *Pezzotto: cos'è, come funziona e quali sono i rischi*, Lexplain, 2024

GARCIA C. A., *Violazione del diritto d'autore: cosa si rischia*, 2023

GARTNERG2 e **THE BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD LAW SCHOOL**, *Five scenarios for Digital Media in a Post-Napster World*, Research Publication No. 2003-07, 2003 https://cyber.harvard.edu/wg_home/uploads/286/2003-07.pdf

GAUDENZI SIROTTI A., *Il nuovo diritto d'autore. La tutela della proprietà intellettuale nell'era dell'intelligenza artificiale*, 12 ed., Maggioli Editore, 2024

GIUFFRE' A., *Pirateria, operazione internazionale: sequestrati oltre 5500 siti, sanzionati gli utenti*, 2020 https://tg24.sky.it/cronaca/2020/11/11/operazione-internazionale-pirateria

GRECO P. e **VERCELLONE P.**, *I diritti sulle opere dell'ingegno*, in VASSALLI, *Trattato di diritto commerciale*, UTET, Torino, 1974

HERZOG E. e **HOFMANN C.**, *No ai blocchi di rete e all'isolamento digitale*, *Economieswisse Dossier Politica*, 2018

IDC, *The Dangerous World of Counterfeit and Pirated Software*, White Paper, 2013

IFPI, *Global Music Report*, 2016 https://ifpicr.cz/ifpi-global-music-report-2016

JARACH G. e **POJAGHI A.**, *Manuale del diritto d'autore*, Ugo Mursia Editore, 2019

JENNINGS K. e **BOSSLER A. M.**, In: Holt, T., Bossler, A. (eds) *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, Palgrave Macmillan, Cham, 2020.

JINDAL M., *How Much Does Piracy Cost the Music Industry? – 8 Effects*, Bytescare blogs, 2024, https://bytescare.com/blog/how-much-does-piracy-cost-the-music-industry

KARAGANIS J. e **RENKEMA L.**, *Copy culture in the US and Germany*, The American Assembly, 2013 https://www.researchgate.net/publication/263565520_Copy_Culture_in_the_US_and_Germany

KESDEN G., *Content Scrambling System (CSS): Introduction*, 2000.

LAVAGNINI S., *Il diritto d'autore nel mercato unico digitale*, Giappichelli, 2022

LAI M., *eMule: origini e ritorno alla ribalta dello storico software p2p*, Everyeye Tech, 2020 https://tech.everyeye.it/articoli/speciale-emule-origini-ritorno-ribalta-storico-software-p2p-50124.html

LEGA SERIE A, *Campagna contro la pirateria audiovisiva. La pirateria uccide il calcio - #STOPIRACY*, promossa in occasione della prima e seconda giornata della Serie A TIM 2022/2023.

LUCCHI N., *The Unfair play of DRM Technologies: Rereading the rules of the Game from the Consumer's Perspective*, Papers. Paper 50, New York University School of Law, 2007

MANDAL S., *How an e-book is pirated, its implications for the stakeholders, and the extent of the problem*, 2023.

MAXWELL A., *Canadian ISPs blocked pirate IPTV & logged customer IP Adresses*, 2023.

MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE, DIPARTIMENTO PER L'INNOVAZIONE E LE TECNOLOGIE, *Relazione Informativa Digital Rights Management*, 2004. https://www.interlex.it/testi/pdf/drmfull.pdf

MOCCIA A., *Streaming illegale: come funziona l'IPTV e lo scudo "anti-pezzotto" Piracy Shield*, 2024.

MONTAGNANI M. L. e BORGHI M., *Proprietà digitale. Diritti d'autore, nuove tecnologie e digital rights management*, EGEA, 2006.

MUSO, *The Publishing Piracy Report*, 2021.

NEU M., *Understanding Music Piracy and its impact on the Industry*, Reprtoir, 2023.

ODDINO M., *La nostra battaglia ai pirati*, Sportclub, disponibile su www.sportclubonline.it/rubriche/sport/2120-la-nostra-battaglia-ai-pirati.

OSSERVATORIO CYBERSECURITY & DATA PROTECTION, *Cos'è la cybersecurity e perché è importante in azienda*, Politecnico di Milano.

OSSERVATORIO CYBERSECURITY E DATA PROTECTION POLITECNICO DI MILANO, *Cybersecurity, data protection e gestione del rischio cyber: i principali trend*.

OXERA, *Competing with 'free'? The damages of music piracy*, 2011.

PADOVANI T., *Diritto penale,* 12 ed., Giuffrè Francis Lefebvre, 2019

PASTORELLA G., *Piracy Shield, tutte le falle dell'antipirateria di Stato*, Agenda Digitale, 2024.

PIROSA G., *Piratebay: storia e sviluppi del sito di Torrent più famoso*, digital-pr.it, 2024. https://www.digital-pr.it/piratebay-storia-e-sviluppi-del-sito-di-torrent-piu-famoso/

PRICE D., *Sizing the piracy universe*, NetNames, 2013.

REDAZIONE INTERNAPOLI, *Quattro italiani su dieci usano il pezzotto, i dati sui pirati di partite e film*, 2024.

RIAA, *About Piracy*, 2022.

ROSENBLATT B., TRIPPE B. e MOONEY S., *Digital Rights Management. Business and Technology*, John Wiley & Sons, 1 ed., 2001.

SENA G., FRASSI A. E. P., D'AMMASSA G., GIUDICI S., MINOTTI D., MORRI F., *Diritto d'autore e diritti connessi nella società dell'informazione,* IPSOA, 2003

SHINDER LITTLEJOHN D. E., CROSS M., *Scene of the Cybercrime*, 2 ed., 2008. https://www.sciencedirect.com/science/article/abs/pii/B9781597492768000029

SIGNORELLI A. D., *Cosa resta di Napster, 20 anni dopo*, Wired Italia, 2019. https://www.wired.it/attualita/tech/2019/06/01/napster-20-anni-dopo-storia-sean-parker/

SMITH M. D. e JONSSON J. E., *What the Online Piracy Data Tells Us About Copyright Policymaking*, Hudson Institute, 2023. https://www.hudson.org/intellectual-property/what-online-piracy-data-tells-us-about-copyright-policymaking

SPEDICATO G., *I Digital Rights Management System tra produzione e diffusione di opere dell'ingegno. Quale nuovo aspetto per il diritto d'autore?*, in *Ciberspazio e diritto*, vol. 5, n. 3, 2004, pp. 273-302.

SPEDICATO G., *Le misure tecnologiche di protezione del diritto d'autore*, Gedit, Bologna, pp. 171-244, 2006.

STANIMIROVIC U., *A publisher Guide to DRM. What is DRM, How does it works, and when do publisher need it*, Video Technology, 2023.

TEAM D., *Pros & Cons of Physical vs Digital Music Distribution*, Daisie Blog, 2024. https://blog.daisie.com/pros-cons-of-physical-vs-digital-music-distribution/

TERRACINA D., *La tutela penale del diritto d'autore e dei diritti connessi*, Giappichelli, Torino, 2006.

THE USENIX ASSOCIATION, *Proceedings of the 10th USENIX Security Symposium*, 2001. https://web.archive.org/web/20201031040253/https://www.usenix.org/legacy/publications/library/proceedings/sec01/craver.pdf

TRIPALDI G., *Digital Rights Management: come affrontare la salvaguardia del Diritto d'autore nell'era digitale*, 2002.

UBERTAZZI L. C., *Diritto d'autore*. Estratto da *Commentario breve alle leggi su proprietà intellettuale e concorrenza*, 4 ed., CEDAM, 2007.

UBERTAZZI L. C. e AMMENDOLA M., *Il diritto d'autore*, UTET Università, 1993.

UBERTAZZI L. C., *I diritti d'autore e connessi. Scritti*, 2 ed., Giuffrè Editore, 2003.

VALERIO E. e ALGARDI Z., *Il diritto d'autore. Commento teorico-pratico alla nuova legge italiana 22 aprile 1941, n. 633*, Milano, Giuffrè Editori, 1943.

WHITMAN K. et al., *Psychological reactance to anti-piracy Messages explained by gender and attitudes*, *Journal of Business Ethics*, 2024. DOI: 10.1007/s10551-023-05597-5.