ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Dipartimento di Informatica - Scienza e Ingegneria - DISI
Corso di Laurea in Ingegneria e Scienze Informatiche

Diritto d'autore e tecnologie emergenti: UGC, DRM, blockchain e IA

Tesi di laurea in:
Informatica e Diritto

Relatrice
Prof.ssa Luisa Dall'Acqua

Candidato
Emanuele Bertolero

Terza Sessione di Laurea
Anno Accademico 2024/2025

Introduzione

Nel moderno ed attuale ecosistema digitale, il diritto d'autore si trova nell'incrocio tra innovazione tecnologica e tutela dei diritti fondamentali. La diffusione capillare della rete internet ha aumentato le possibilità di creazione, accesso e circolazione delle opere, ma ha allo stesso tempo ha reso più porosi i confini della protezione, portando ad un ripensamento degli strumenti giuridici tradizionali. Questa tesi si basa su un presupposto semplice: per governare questo cambiamento occorre parlare sia il linguaggio giuridico che quello informatico, ed occorre inoltre farli dialogare in modo coerente.

Se da una parte la digitalizzazione e le licenze aperte hanno ampliato l'orizzonte dell'accesso al sapere e della sua condivisione, dall'altra parte emergono nuove tensioni: tra sfruttamento economico e libertà creativa, tra tutela del software ed interoperabilità, tra responsabilità degli intermediari e partecipazione in prima persona degli utenti. Il risultato è un equilibrio, che richiede regole nitide, misure tecniche commisurate, ed una grande attenzione al progresso dei modelli di diffusione dei contenuti, in costante evoluzione.

Questa tesi persegue tre obiettivi: ricostruire i fondamenti del diritto d'autore ed i loro adattamenti nell'ambiente digitale; affrontare la cerniera tecnico-giuridica del software e delle misure tecnologiche di protezione; esplorare le nuove frontiere come blockchain, NFT e intelligenza artificiale e mostrarne responsabilità e tutele anche grazie a casi di studio.

La prima sezione introduce l'inquadramento più teorico: dalle origini del copyright e le differenze con il diritto d'autore, ai diritti patrimoniali e morali delle opere, fino agli effetti della digitalizzazione, all'Open Access e le principali licenze aperte come GPL o Creative Commons. Ciò forma la base concettuale e normativa per poter procedere all'analisi dell'evoluzione del diritto nel mondo digitale.

La seconda sezione entra proprio nel vivo dell'incontro con l'informatica. Si analizza dunque una nuova opera dell'ingegno: il software. Vengono chiariti anche gli aspetti tecnici come il codice sorgente, compilato ed eseguibile ed i limiti del reverse engineering per l'interoperabilità, oltre che gli aspetti giuridici delle norme che regolano ciò, come la direttiva europea 2009/24/CE e la legge

italiana n°633/1941. Vengono analizzate anche le opere digitali auto-prodotte dagli utenti, i cosiddetti User Generated Contenti e le piattaforme di condivisione (YouTube, TikTok, Instagram, Twitch, SoundCloud). Si chiariscono gli aspetti di responsabilità regolamentati dalle Direttive 2000/31 e 2019/790, concludendo poi con ciò che aiuta tecnicamente il rispetto proprio di tali responsabilità, ovvero le misure tecnologiche di protezione come DRM, watermarking e fingerprinting.

La terza sezione esplora le nuove frontiere. In primis blockchain, smart contract e non-fungible token, come nuove infrastrutture di tracciabilità e gestione dei diritti, con un caso emblematico, quello della Juventus F.C. contro Blockeras s.r.l, che per la prima volta in Italia chiarisce il rapporto tra i token digitali, i marchi e il diritto d'autore. Si passa poi all'intelligenza artificiale generativa, introducendo architetture tecniche e funzionamento, per poi provare ad inquadrarlo giuridicamente con l'AI Act europeo, ancora in proposta, con il suo nuovo approccio risk-based. In chiusura un altro caso italiano, più recente, che mostra le ricadute concrete di questa tecnologia ancora in forte trasformazione.

In breve, l'elaborato si articola in un percorso progressivo, partendo dalle basi ed arrivando confini dell'innovazione, includendo inquadramenti normativi, approfondimenti tecnici, ed analisi di casi reali. La sfida è trovare condizioni di equilibrio affinché la protezione autoriale resti efficace e proporzionata con un mondo digitale in continua evoluzione.

A chi semina conoscenza senza sapere dove crescerà
e continua a farlo lo stesso.

All'affetto dei miei studenti dell'Istituto Tecnico Industriale "Don L.Orione"
ed ai loro contagiosi sorrisi.

Indice

Elenco delle figure

Capitolo 1

Fondamenti dei diritti d'autore

1.1 Evoluzione storica

1.1.1 Dalle origini (privilegi tipografici) al copyright moderno

Il diritto d'autore, per come lo intendiamo oggi, è il risultato di un lungo percorso giuridico e culturale. Ha radici nell'era moderna, in particolare nel periodo in cui la stampa a caratteri mobili rese possibile la riproduzione in serie dei testi, da cui nacque, come diretta conseguenza, l'esigenza di regolamentarne la produzione, e soprattutto, la distribuzione.

I privilegi tipografici a Venezia e Milano

In risposta a tale necessità nacque il primo strumento di protezione adottato in Europa, quello dei *privilegi tipografici*. Questo primitivo, ma efficace strumento di tutela veniva rilasciato esclusivamente dalle autorità civili, come le amministrazioni locali, in favore dei tipografi, che ottenevano dunque, per un periodo di tempo determinato, l'esclusiva sulla riproduzione e la vendita di un'opera. Ciò permetteva loro di recuperare costi e spese sostenute per la stampa e garantirsi quindi un piccolo utile. In sostanza si trattava di una protezione, ma per lo più di tipo economica, concentrata solo sul soggetto che investiva risorse nella stampa. L'autore e l'opera dell'ingegno rimanevano, dunque, privi di una tutela diretta.

Venezia fu tra le prime città europee ad introdurre tale pratica, le prime concessione di privilegi risalgono infatti al 1486. Questo sistema si rivelò molto efficace nello stimolare la crescita dell'industria tipografica locale, che in poco tempo raggiunse infatti alti livelli di produzione, ancora oggi ricordiamo Venezia come uno dei poli editoriali maggiormente importanti in Europa.

In realtà, negli stessi anni anche a Milano si adottò un regime analogo, ad esempio nel 1841, l'editore Andrea de Bosis ottene un privilegio per la pubblicazione dell'opera denominata *Sforziade* di Giovanni Simonetta. Ed ancora, sempre a Milano nel 1843, un altro privilegio fu concesso per la stampa del *Convivium* di Francesco Filelfo. [1, p. 34]

La transizione al moderno diritto d'autore

La svolta vera si ebbe solo dopo circa due secoli dopo, non più nel contesto italiano, bensì in Inghilterra, con l'emenazione dello *Statute of Anne* nel 1710. È proprio questa legge che viene coralmente considerata la nascita del *copyright moderno*, dato che, per la prima volta nella storia, si riconobbe che il diritto spettava anche all'autore dell'opera e non più solo allo stampatore della stessa. Era ora l'autore in primis ad acquisire il potere giuridico esclusivo sulla propria creazione che poteva, successivamente, cedere all'editore.

Lo *Statute of Anne* aveva un doppio vantaggio: garantiva all'autore una protezione contro le copie non autorizzate e favoriva la diffusione della coltura e del sapere, all'epoca considerata essenziale nello sviluppo della comunità e della società. Proprio per questo, l'atto legislativo fu presentato come uno strumento di "encouragement of learning", ovvero di incentivo all'apprendimento. [1, p. 35]

Nello stesso secolo, ma in Francia, la famosa Rivoluzione del 1789 portò ad una nuova concezione della proprietà intellettuale, furono infatti emanate le leggi del 1791 e 1793 che affermarono il modello del *droit d'auteur*, che in aggiunta ai diritti patrimoniali, tutelava anche i diritti morali dell'autore. Per la prima volta veniva riconosciuto un legame personale tra l'autore e la sua creazione, la sua opera. Tale legame sopravviveva anche a seguito di una cessione dei diritti economici, divenendo perciò inscindibile.

Introduzione e nascita dei due modelli contemporanei

Le esperienze legislative narrate sino ad ora, in parte, posero le basi dei due modelli tuttora vigenti, che saranno analizzati più nel dettaglio nel paragrafo successivo, qui di seguito anticipati:

- il *copyright anglosassone*, maggiormente incentrato sull'industria dell'editoria e sulla logica del mercato, che mira principalmente alla tutela della riproduzione e distribuzione;
- il *diritto d'autore continentale*, che invece tutela anche e maggiormente l'aspetto morale e personale della creazione.

Entrambi i modelli, nonostante le loro differenze, possono essere considerati "padri fondatori" della regolamentazione odierna, che oggi giorno però si trova a confrontarsi con nuove sfide poste soprattutto dalla digitalizzazione, dalla forte crescita di prodotti software, e ancor più recentemente, dall'intelligenza artificiale.

1.1.2 Differenze tra diritto d'autore (civil law) vs. copyright (common law)

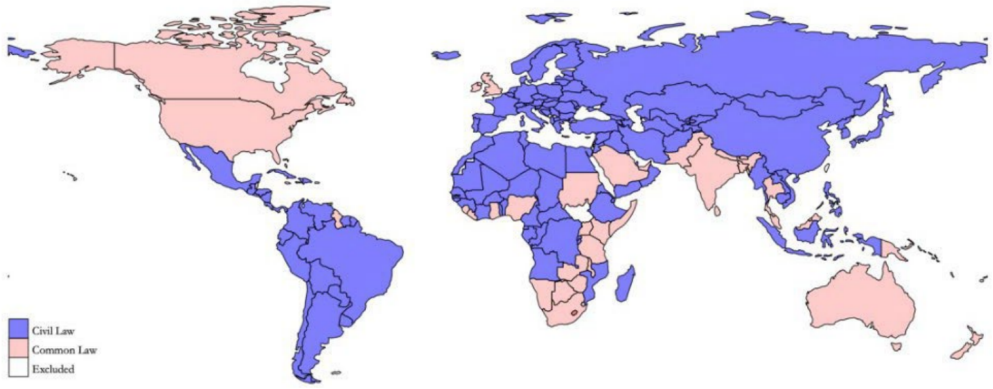


Figura 1.1: Mappa dei paesi Civil law e Common law
Fonte: University of Chicago Law School

• Il diritto d'autore nel modello continentale

Nel diritto d'autore del sistema continentale, che come già accennato nel paragrafo precedente, trova origine nelle leggi francesi e che successivamente è stato recepito da altri paesi europei, tra cui anche l'Italia, l'opera viene intesa come una manifestazione della personalità del suo autore. Dunque l'autore stesso non è solo un produttore di beni, ma bensì è un soggetto che imprime la propria creatività ed identità nell'opera, in maniera del tutto originale. È proprio per questa motivazione che il diritto d'autore mira a tutelare due dimensioni: sia quella patrimoniale ed economica, sia quella personale e morale.

La componente patrimoniale, è comunque fondamentale, perché attribuisce all'autore l'esclusivo potere di sfruttare economicamente l'opera attraverso atti come la distribuzione, la riproduzione e la pubblicizzazione. Questi diritti appena elencati possono essere ceduti a terzi, anche a titolo oneroso, come editori, produttori o altri soggetti interessati. Ciò non vale per la componente morale, che invece ha caratteristiche peculiari: i diritti morali sono imprescrittibili ed inalienabili, dunque restano sempre e comunque in capo all'autore, indipendentemente da eventuali rapporti contrattuali. Essi includono, tra l'altro, il diritto al rispetto dell'integrità dell'opera e alla sua paternità per l'autore.

L'impostazione fin'ora narrata è coerente con l'idea, propria del civil law, che l'opera sia prevalentemente un bene economico e sopratutto non scindibile completamente dal suo autore. [2, p. 28]

• Il copyright nel modello anglosassone

Il sistema del *common law* ha seguito invece una strada diversa. Il copyright, come visto in precedenza, nasce in Inghilterra e si sviluppa in particolare anche negli Stati Uniti d'America. Concettualmente privilegia un'idea più commerciale ed industriale dell'opera, non mira alla protezione della personalità dell'autore, piuttosto protegge l'opera come solo bene economico riproducibile.

Il copyright concentrandosi prevalentemente sul diritto esclusivo di distribuzione e di copia garantisce al titolare la possibilità di sfruttamento economico della stessa, titolare che non sempre coincide con l'autore dell'opera.

Una caratteristica particolare di questo modello è il concetto del *works made for hire*, secondo il quale i diritti delle opere create nel contesto di un rapporto professionale/lavorativo spettano in maniera diretta al committente o datore di lavoro. [3, lett. b] Ciò evidenzia nettamente la diversa impostazione culturale: il baricentro, in questo sistema, si sposta sempre sul soggetto investitore e che organizza la produzione dell'opera, mai sull'autore.

I diritti morali infatti, nel sistema common law, hanno un ruolo completamente marginale se non del tutto assente, inoltre la protezione era subordinata al deposito o alla registrazione, vincoli che negli anni sono stati superati grazie ad accordi internazionali e che hanno condotto ad un'armonizzazione dell'accesso alla tutela, di cui si dirà in seguito.

Convergenze e punti di contatto

Nonostante le varie differenze sino a questo punto esposte, la globalizzazione dei mercati e il diritto internazionale hanno lentamente incentivato una convergenza progressiva dei due sistemi. La Convenzione di Berna del 1886 ha portato alla protezione in automatico delle opere anche tra vari paesi, senza dunque necessità delle varie formalità ed ha inoltre sancito l'obbligo di riconoscere alcuni dei diritti morali. Ciò ha condotto all'avvicinamento al modello europeo anche i paesi common law. Non è stata la Convenzione di Berna l'unica protagonista di questo avvicinamento, ma anche l'evoluzione tecnologica ha avuto un ruolo al quanto determinante. In particolar modo la digitalizzazione delle opere e la diffusione tramite la rete internet hanno reso un sistema basato su regole diverse poco sostenibile. Le FAQ elaborate da ICOM Italia nel 2021 osservano infatti a tal riguardo che «*i due sistemi svolgono la stessa funzione e tendono sempre più con il tempo ad uniformarsi in relazione all'evolversi delle forme di sfruttamento online delle opere*». [4, p. 10]

Sintesi

Riassumendo, si individuano alcuni tratti caratteristici:

- nel diritto d'autore europeo, l'opera viene protetta come espressione della personalità del suo autore, che ne detiene quindi sempre i diritti morali;

- nel copyright anglosassone, prevale maggiormente l'idea dell'opera come un bene di mercato, attenzionando solo gli aspetti economici e gli investitori.

Nell'era moderna però, grazie a Convenzioni come quella di Berna o alla digitalizzazione i due sistemi, ed i vari paesi, tendono sempre più ad un avvicinamento, quasi fisiologico.

1.1.3 Diritti morali e patrimoniali - Durata della protezione

Diritti morali

I diritti morali tutelano principalmente la personalità artistica e creativa dell'autore, vogliono inoltre garantire che venga rispettato il suo legame con l'opera, anche dopo la sua pubblicazione. La Convenzione di Berna individua due diritti morali fondamentali dei quali ogni autore debba godere:

- il *diritto alla paternità*, che permette all'autore di rivendicare la propria opera di sua creazione;
- il *diritto all'integrità*, che consente invece all'autore di opporsi a qualsiasi modifica dell'opera come deformazioni, mutilazioni o qualsivoglia cambiamento che possa generare pregiudizio alla sua reputazione o al suo onore. [4, p. 10]

Questo nucleo minimo viene poi ampliato dalle varie legislazioni nazionali di civil law che introducono ulteriori prerogative, come:

- il *diritto di pubblicazione*, che concede all'autore la facoltà di rendere nota l'opera o meno;
- il *diritto di ritiro o pentimento*, che garantisce all'autore l'opportunità di ritirare l'opera dal commercio in casi eccezionali.

Tratto comune nei paese europei è considerare questi diritti fortemente inalienabili, imprescrittibili ed irrinunciabili. [4, p. 12]. Questo significa che non possono essere ceduti a soggetti terzi, non terminano nel tempo e non possono

essere rinunciati contrattualmente. In Italia si sancisce espressamente questo regime, permettendo anche agli eredi di operare per far valere i diritti morali a seguito della morte dell'autore.

Diritti patrimoniali

A fianco dei diritti morali troviamo i diritti patrimoniali, che interessano invece l'utilizzazione economica dell'opera. L'unico soggeto che originariamente ha il potere esclusivo di vietare o autorizzare atti di sfruttamente di un'opera è il suo autore, che può farlo sia a titolo oneroso sia gratuito.

Le FAQ ICOM ci aiutano ad individuare le principali facoltà patrimoniali [4, p. 13]:

- il *diritto di riprodurre* l'opera in ogni modo e forma;
- il *diritto di esecuzione* o *di rappresentazione*, che ne permette ad esempio la recitazione in pubblico;
- il *diritto di comunicazione al pubblico* e *di messa a disposizione online*, in particolar modo rilevante nell'era e nel mondo digitale;
- il *diritto di distribuzione*, come il noleggio, il prestito o la vendita;
- il *diritto di adattamento*, come la rielaborazione, la modifica o la traduzione di un'opera.

Questi diritti, diversamente da quelli morali, avendo una natura completamente diversa, sono infatti temporanei, disponibili e soprattutto trasferibili.

Durata temporale della protezione

Per quanto riguarda i diritti patrimoniali, la loro durata è stata individuata a livello internazionale proprio dalla Convenzione di Berna, che prevede una copertura temporale che perdura sino ai cinquant'anni succcessivi alla morte dell'autore dell'opera. Tale termine, trova ulteriore riconoscimento e ampliamento con l'emanazione della Direttiva 2006/116/CE dell'Unione Europea [5] in cui il

termine viene aumentato di ulteriori 20 anni sino a un totale di 70 anni post mortem dell'autore.

Invece i diritti morali hanno una durata diversa, sempre la Convenzione di Berna indica una durata minima che non può essere inferiore a 50 anni dalla morte dell'autore, ma ad esempio in Italia questi diritti vengono considerati perpetui e senza limiti di tempo azionabili dagli eredi.

1.2 Digitalizzazione e beni culturali

1.2.1 Impatti della digitalizzazione sul diritto d'autore

La digitalizzazione è tra i fattori protagonisti che hanno più profondamente pesato sull'evoluzione del diritto d'autore negli ultimi anni. La transazione dai supporti materiali a quelli digitali ha messo in difficoltà sistemi giuridici pensati in un mondo analogico, ma allo stesso tempo, aperto nuove opportunità di condivisione, accesso e fruizione delle opere.

La dematerializzazione

Il primo elemento di cambiamento è stata proprio la dematerializzazione del bene creativo e culturale. Un tempo le opere erano legate ad un supporto di tipo fisico, come ad esempio: libri, dischi o pellicole, mentre oggigiorno possono essere riprodotte in formato digitale e distribuite potenzialmente all'infinito, senza limitazioni "fisiche", ed a costi irrisori, pressoché vicini allo zero. Queste caratteristiche hanno dunque comportato un rimodellamento delle modalità di sfruttamento economico e dei diritti. I vari ordinamenti giuridici si sono dovuti adattare a questo nuovo contesto, dove la copia non è più un'eccezione costosa, ma la quotidiana regola. [6, p. 50-51]

Nuovi canali di diffusione

Il secondo elemento di cambiamento è invece l'espansione delle tecnologia di rete e di collegamento che ha moltiplicato i canali di diffusione delle opere. Grazie ad internet è stata resa possibile una circolazione praticamente globale dei contenuti

digitali e quindi delle opere dematerializzate, che seppur permettano un largo e semplificato accesso alla cultura, d'altro canto accentuano fortemente il rischio di utilizzi non autorizzati e violazioni su larga scala. Da ciò consegue che i classici strumenti di tutela delle opere, fondati su controlli fisici o sistemi di autorizzazione centralizzati, si rivelano ora inadeguati, necessitando quindi di un aggiornamento mirato per poter garantire nuovamente un equilibrio tra la protezione degli autori e le possibilità di accesso da parte degli utenti. [7, p. 16-18]

Nuove tipologie di opere

La digitalizzazione ha portato alla nascita di nuove opere, oltre alle banche dati ed ai programmi per elaboratori oggigiorno troviamo diffuse nuove opere digitali, anche complesse, come i siti web, i videogiochi o le applicazioni cloud. La protezione di queste opere richiede però una combinazione di diversi regimi giuridici tra cui: il diritto d'autore, i marchi, i brevetti, i design. La nostra legge a riguardo non fornisce mai una definizione precisa e non individua mai una specifica disciplina, creando così anche diverse difficoltà agli studiosi della materia che si sono trovati nella scomoda necessità di trovare un regime giuridico applicabile a queste opere dalle caratteristiche al quanto peculiari. Le sfide restano tutt'ora aperte soprattutto in relazione ai vasti contenuti generati da forme di intelligenza artificiale.

Nuove caratteristiche delle opere (digitali)

Un elemento che sicuramente contribuisce a descrivere e comprendere l'impatto della digitalizzazione sul diritto d'autore riguarda le caratteristiche dei media digitali, che li distinguono fortemente dai tradizionali supporti analogici. Già nel 1991 in una pubblicazione su *Communications of the ACM* Pamela Samuelson individua e descrive sei aspetti fondamentali che definiscono la natura delle opere digitali, che qui di seguito sono riassunti [8]:

- la *facilità di replicazione*: i contenuti digitali, espressi sotto forma di bit, sono facilmente replicabili senza perdita di qualità, in modo infinito;

- la *facilità di trasmissione e di uso multiplo*: una volta caricato in rete un file digitale può circolare liberamente senza che il titolare o il suo autore ne abbiano un effettivo controllo e giungere ad un numero indefinito di utenti;
- la *malleabilità dei mezzi digitali*: i media digitali consentono facilmente all'utente di effettuare modifiche, manipolazioni, adattamenti e personalizzazione in modo molto più agevole rispetto alle opere su supporti fisici;
- l'*equivalenza delle opere in formato digitale*: vari tipi di opere di contenuto diverso (testo, audio, video, immagini) coesistono nello stesso ambiente digitale, possono essere dunque memorizzati sugli stessi supporti e diffusi negli stessi canali, c'è quindi un fenomeno di omogeneizzazione;
- la *compattezza*: i contenuti digitali a differenze delle opere stampate o incise occupano pochissimo spazio e sono dunque più facilmente distribuibili;
- la *non linearità nella fruizione*: le opere digitali sono fruibili dall'utente finale in modo libero, non devono più necessariamente seguire, ad esempio, l'indice di un libro ma possono navigarlo cercando parole chiave, saltando dunque da una pagina all'altra senza ordine.

Nuova percezione sociale

L'evoluzione digitale ha sicuramente inciso su aspetti tecnici e giuridici, ma porta anche un cambiamento profondo in quella che è la percezione sociale del diritto d'autore e delle condotte illecite. I comportamenti in rete, che magari portano ad una violazione del copyright, compiuti attraverso uno schermo, spesso vengono percepiti diversamente dal mondo offline. Nella letteratura criminologica infatti è stato evidenziato come il mondo digitale produca una specie di trasformazione percettiva nella persona. Susanna Vezzadini ha provato ad individuare cinque aspetti percettivi che risultano modificati dall'avvento della realtà virtuale: [9]

- la *percezione dell'illegalità del comportamento*;
- la *stima dei rischi derivanti dall'essere scoperto*;

- la *stima dei rischi rispetto alla possibilità di essere denunciato*;
- la *percezione del danno procurato alla vittima*;
- la *valutazione dell'eventualità della sanzione sociale e legale*;

Questa analisi trasferita al campo del diritto d'autore, rende evidente come questi mutamenti portino a pratiche diffuse di condivisione senza consenso di contenuti digitali. Gli utenti si sentono "come giustificati" pensando di *"non recare danno a nessuno"* o che *"sia improbabile che vengano a cercarmi"*, ciò contribuisce a ridimensionare la percezione d'illiceità e all'accettazione di ciò che formalmente comporta una violazione dei diritti d'autore. [7, p. 40]

Sintesi

L'impatto del digitale, quindi, non si esaurisce nella sola questione tecnica ma coinvolge diversi fronti, da quello culturale, economico e sociale. Porta alla ridefinizione dell'idea di "copia", alla comparsa di nuove opere, all'evoluzione di nuovi canali, fino al mutamento della percezione collettiva della legalità nel mondo online. Questa trasformazione richiede quindi un costante aggiornamento dei regolamenti e un forte dialogo tra tecnologi e giuristi.

1.2.2 Riproduzioni digitali e accesso pubblico

La digitalizzazione delle opere culturali è sicuramente un processo anche giuridico, ma innanzitutto tecnico. Resa possibile grazie a strumentazioni moderne e nuove tecniche come: le scansioni 3D, l'acquisizione di immagini ad altissima risoluzione, l'elaborazione dei metadati e la conservazione in archivi digitali cloud. Sul fronte informatico quindi, la riproduzione digitale non è altro che un processo che genera una nuova rappresentazione dell'opera, sostanzialmente un file, che può essere un immagine, un modello 3D o una registrazione audio.

Restrizioni per impedire l'accesso pubblico

Queste rappresentazioni, replicabili infinite volte, favoriscono la diffusione del patrimonio, ma allo stesso tempo aumentano il rischio di un eccessivo controllo

Figura 1.2: Digitalizzazione di un opera artistica tramite rilievo con scanner 3D
Fonte: 3D ArcheoLab

sulle copie da parte di chi detiene gli originali, come le istituzioni culturali. Anche la letteratura accademica ha evidenziato come archivi e musei tendano ad auto-considerare le copie digitali come nuove opere da gestire con logiche proprietarie. [10, p. 7 Par. 3.1] Dal punto di vista tecnico-informatico ciò è effettivamente possibile applicando ai file restrizioni come: filigrane (watermark), abbassamento della risoluzione o DMR. La creazione di queste barriere artificiali permette loro di limitare l'uso delle riproduzioni su delle opere che sarebbero in realtà ormai di pubblico dominio, ostacolando così anche possibili usi leggittimi in ambito didattico o scientifico. Anche la ricerca universitaria in Italia ha investigato su questo conflitto, si evidenzia infatti che l'utilizzo di questi formati chiusi e l'applicazione di restrizioni tecnologiche rischiano di trasformare la digitalizzazione da opportunità ad un nuovo "monopolio digitale", nel quale le opere sono accessibili solo attraverso infrastrutture controllate da pochi. [11, Cap.3 Par.1]

Risposta dell'Unione Europea per contrastare il fenomeno

Per scoraggiare queste pratiche l'Unione Europea nell'articolo 14 della Direttiva (UE) 2019/790 ha stabilito che le riproduzioni delle opere d'arte in pubblico dominio non possono nuovamente essere oggetto di nuovi esclusivi diritti. Da un punto di vista tecnico ciò significa che un modello 3D o una scansione debbano rimanere ad alta risoluzione e senza manipolazioni, devono quindi restare liberamente accessibili. [12, Art. 14] Tuttavia le tecnologie informatiche consentono ancora alle istituzioni di avere un controllo de facto, grazie all'utilizzo di server

proprietari per la messa in rete delle opere digitali, con l'applicazione di restrizioni di accesso alle API, applicate da remoto o la concessione di licenze software per la fruizione di questi contenuti da loro controllate.

Sfida Digitale

Infine, citando il contributo divulgativo pubblicato su *Agenda Digitale*, si sottolinea che la sfida non è solo giuridica, ma anche e soprattutto tecnologia: occorre sviluppare maggiormente ecosistemi in cui le opere digitali siano aperte, interoperabili ed accessibili, come già alcune piattaforme stanno provando a fare, ad esempio *Google Arts & Culture* o *Wiki Loves Monument*.

Figura 1.3: Logo della piattaforma Google Arts & Culture
Fonte: Google LLC

Per concludere, si deve evitare quindi che la digitalizzazione diventi un meccanismo di esclusione anziché di inclusione e condivisione.

1.2.3 Opere orfane e fuori commercio

Opere orfane

Le *opere orfane* sono quelle opere ancora coperte dal diritto d'autore, ma di cui i titolari non possono essere rintracciati o comunque identificabili. Esiste una Direttiva UE, 2012/28 entrata in vigore a fine 2012, che ha appositamente introdotto una disciplina specifica che consente agli archivi, ai musei ed alle biblioteche, dopo una ricerca diligente nelle fonti disponibili, di riprodurre e poi rendere accessibili queste opere.[4, p. 16]

Ciò ha portato alla realizzazione di banche dati informatizzate come l'"Orphan Works Database", gestita dall'EUIPO, che permette un monitoraggio in tempo reale delle opere dichiarate orfane a livello europeo. [4, p. 36]

Figura 1.4: Logo della banca dati Orphan Works Database
Fonte: EUIPO

Opere fuori commercio

Le *opere fuori commercio* sono invece quelle opere non più disponibili sul mercato, però ancora coperte e tutelate dal diritto d'autore, dunque solo quando non siano già trascorsi i 70 anni dalla morte dell'autore. Ad entrare in gioco in questo caso è la Direttiva (UE) 2019/790, che ha l'obiettivo di facilitare la digitalizzazione e la diffusione in rete di tali opere. Se esistono società di gestione collettiva rappresentative, come la SIAE, gli istituti per poter procedere con la messa a disposizione del pubblico debbono negoziare licenze con queste ultime. Solo nel caso in cui tali organismi adeguatamente rappresentativi manchino, allora gli istituti possono procedere con la pubblicazione in rete autonomamente, a fini ovviamente non commerciali. [13, p. 77-79]

Sintesi

Riassumendo, la distinzione tra le opere orfane e fuori commercio, ci dimostra come la digitalizzazione non sia esclusivamente un processo di tipo tecnico, ma anche una delicata operazione che riequilibra la protezione autoriale e l'accesso pubblico, reso possibile in larga scala tramite la potente quanto pericolosa rete internet.

1.3 Accesso libero e licenze aperte

1.3.1 Open Access

Origini e principi

Il movimento per l'Open Access nasce circa due decenni fa, all'inizio del millennio, in un momento caratterizzato dalla cosiddetta *crisi dei prezzi dei periodici*, che

rendeva difficile sempre più il sostenimento di costi per gli abbonamenti alle riviste per bilioteche o università [14, p. 12]. A questa critica situazione sono arrivate le prime risposte con le dichiarazioni internazionali, come:

- la *Budapest Open Access Initiative* (2002);
- la *Bethesda Statement* (2003);
- la *Berlin Declaration* (2003);
- la *Dichiarazione di Messina* (2004) [nazionale, in Italia];

che hanno voluto fissare i principi fondamentali del libero accesso [14, p. 54]. Il presupposto sostenuto è che i risultati della ricerca debbano essere resi accessibili liberamente, privi di barriere giuridiche o economiche e garantire così un'ampia disseminazione a favore dell'avanzamento della cultura e della conoscenza.

La strada Gold OA

Una delle principali modalità è la *Gold Road*, che come impostazione prevede che la pubblicazione avvenga direttamente su riviste ad accesso libero. Queste riviste rendono i contenuti immediatamente e liberamente consultabili online sin dal momento della loro pubblicazione, generalmente finanziandosi tramite contributi provenienti dalle università o enti di ricerca, raramente a carico degli autori delle pubblicazioni. Per i ricercatori il vantaggio consiste nella maggior visibilità e citabilità dei lavori, dato confermato anche da vari studi, che mostrano un incremento delle citazioni per gli articoli Open Access (OA). Tuttavia non mancano anche le criticità: come la comparsa di riviste ibride che mescolano articoli in abbonamento con articoli Open Access. Inoltre si registra il fenomeno degli editori predatori, che tentano di sfruttare questo modello chiedendo dei contributi senza però garantire qualità, violando norme e codici etici editoriali. [14, p. 12]

La strada Green OA

La seconda via è quella della *Green Road*, che consiste nell'auto-archiviazione da parte degli autori in quelli che sono respository istituzionali, conformi agli standard dell'Open Archives Initiative. Questi repository conservano, diffondono e raccolgono le pubblicazioni prodotte nelle università o negli enti di ricerca, garantendo sempre un libero accesso a lungo termine. I repository istituzionali sono oggigiorno considerati essenziali per la comunicazione in ambito scientifico e didattico, dato che garantiscono affidabilità, autenticità e la possibilità di integrazione tramite metadati. Essi inoltre permettono di collegare direttamente le pubblicazioni con i dati della ricerca, garantendo dunque anche una grande trasparenza. [14, p. 76]

Lo strumento giuridico dell'OA: le licenze aperte

Sebbene l'Open Access garantisce la consultazione libera delle opere, l'effettiva possibilità di riutilizzo dipende strettamente dalle condizioni giuridiche che accompagnano la pubblicazione. Infatti molte riviste e repository adottano delle licenze aperte, come le *Creative Commons (CC-BY, CC-BY-SA)*, meglio descritte nel prossimo paragrafo, che consentono agli utenti non solo la lettura, ma anche la ridistribuzione e la rielaborazione dei contenuti, a rispetto ovviamente dei termini stabiliti [14, p. 55] [4, p. 45].

In questo caso, l'Open Access costituisce la cornice culturale, mentre le licenze aperte sono lo strumento giuridico che concretamente rende possibile il riuso e la diffusione.

1.3.2 Creative Commons, GPL e altre licenze

Ambiti di applicazione

Le licenze aperte costituiscono lo strumento giuridico attraverso cui la concezione dell'*open* si attua nella pratica. Esse hanno infatti come obiettivo quello di standardizzare i permessi d'uso, rendendono più trasparente e semplice la gestione

dei diritti, evitando costi e complessità, discusse anche nel paragrafo precedente, tipici delle licenze individuali.

Principalmente si distinguono in tre grandi ambiti d'applicazione:

- *Culturale*: ad esempio, le licenze *Creative Commons* regolano la circolazione di vari tipi di opere, come quelle letterarie, multimediali, artistiche, audiovisive o fotografiche. In questo contesto l'obiettivo principale è quello di rendere la comprensione delle condizioni d'uso immediata, avvalendosi di clausole semplici e pittogrammi intuivi, a regnare è proprio la trasparenza [15, p. 120];

- *Scientifico/accademico*: ad esempio, licenze come *CC-BY* e *Open Data Commons* vengono utilizzate nei portali accademici, nelle piattaforme open data o nei repository istituzionali. Le licenze in questo caso mirano ad una più ampia diffusione dei dati raccolti o dei risultati della ricerca, cercando di favorirne anche una riproducibilità scientifica a fini didattici o di ricerca [14, p. 80-81];

- *Informatico*: in questo ultimo ambito, invece si trovano licenze come, *GNU GPL*, *MIT*, *BSD* e *Apache*, pensate principalmente per regolamentare la distribuzione di software informatico. Esse disciplinano il rapporto tra gli sviluppatori (creatori dell'opera) e gli utilizzatori del codice (fruitori dell'opera), bilanciando la libertà di utilizzo con i giusti vincoli di condivisione ed appropriazione. [16, p. 60].

La tripartizione dimostra come l'ideale "aperto" non sia confinato a un singolo settore, ma rappresenti un paradigma trasversale tra le diverse forme di creatività e di opere frutto d'ingegno, in tutti i campi.

Licenze Creative Commons

Il progetto *Creative Commons* nasce nel 2001, caldeggiato da Lawrence Lessig e da un team di giuristi ed informatici, con il fine comune di offrire agli autori strumenti semplici per comunicare in modo comprensibile le condizioni di

utilizzo delle proprie opere. A queste opere si riconosce il merito di aver creato un vero e proprio "modello di semplificazione", che è stato capace di tradurre concetti giuridici complessi in formule standard e facilmente intuitive.

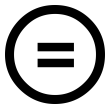
La struttura base si fonda su quattro clausole fondamentali, che possono essere tra loro anche combinate [16, p. 86]:

- 

  BY (*Attribuzione*): è la clausola base, obbligatoria, comune dunque a tutte le licenze CC. Consente a tutti di utilizzare e distribuire l'opera con il solo vincolo che venga attribuita e riconosciuta in modo chiaro la paternità dell'autore originario, includendo perciò il suo nome, il titolo e la fonte dell'opera;

- 

  NC (*Non Commerciale*): permette l'uso dell'opera solo per finalità non commerciali. Significa che l'opera può essere tranquillamente utilizzata, copiata e diffusa liberamente ma solo negli ambiti privati, educativi, culturali o scientifici, non per scopi di lucro o in prodotti venduti sul mercato;

- 

  ND (*Non Opere Derivate*): consente l'utilizzo e la distribuzione esclusivamente in forma originale, senza modifiche, adattamenti, traduzioni o qualsiasi mutazione. Sostanzialmente l'opera può essere riprodotta e condivisa, ma non trasformata in qualcosa di nuovo;

- 

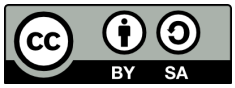
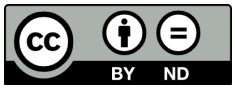
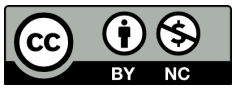
  SA (*Share Alike*): permette la creazione, in questo caso, di opere derivate, imponendo però che vengano a loro volta distribuite con la stessa licenza dell'opera originale. È la clausola che praticamente incarna la logica *copyleft*: garantisce la libertà d'uso, a patto di mantenere e "tramandare" tale libertà concessa.

A queste si aggiunge anche una clausola più particolare, a se stante e non combinabile con le altre:

- 

  CC0 (*Creative Commons Zero*): consente all'autore di rinunciare completamente ai propri diritti patrimoniali e di collocare quindi l'opera nel pubblico dominio.

Dall'incrocio e la combinazione delle clausole si da origine alle varie licenze standard Creative Commons, con livelli variabili di libertà d'uso [16, p. 87]:

Licenza	**Clausole**	**Uso consentito**
	BY	È la licenza più aperta: chiunque può distribuire, copiare e modificare, anche per fini di lucro, purché attribuisca la paternità.
	BY + SA	Consente di utilizzare, ridistribuire ed adattare l'opera, anche per fini commerciali, ma obbligando a rilasciare ogni opera derivata con la medesima licenza dell'originale.
	BY + ND	Permette la ridistribuzione dell'opera, sia a fini economici che non, ma solo in formato originale, senza possibilità di modifica alcuna, come traduzioni o mutazioni.
	BY + NC	Simile alla licenza BY, dunque consente tutte le operazioni di copia, condivisione e creazione di opere derivate, vincolando però solo agli usi non commerciali.
	BY + NC + SA	Come la licenza BY + NC, con l'ulteriore obbligo di mantenere la stessa licenza nelle opere derivate dall'originale.
	BY + NC + ND	È la più restrittiva: le uniche operazioni permesse sono quelle di copia e di redistribuzione, non è possibile effettuare modifiche, creare opere derivate ne tanto meno consente usi commerciali.
	CC0	Rinuncia a tutti i diritti: l'opera entra in pubblico dominio e può essere usata liberamente, senza obblighi di attribuzioni o vincoli vari.

Il successo delle licenze Creative Commons (CC) sta proprio nella loro capacità di rendere facilmente riconoscibili il regime giuridico di un'opera, grazie ad un sistema che combina: un testo legale completo (*legal code*), un riassunto leggibile da tutti (*human readable*) e un codice per i motori di ricerca (*machine readable*). Questo triplice livello comunicativo è stato innovativo e ha reso le CC uno standard di successo su scala globale. [17, p. 21].

Licenze GNU e modello copyleft

Nell'ambito software, la licenza più caratteristica è la GNU General Public License (GPL), nata negli anni ottanta promossa dalla *Free Software Foundation*, evoluta però nel corso dei decenni attraverso varie versioni, dalla prima risalente al 1989 fino alla terza, la più recente, del 2001, ciascuna delle quali ha chiarito ed aggiornato diversi aspetti in risposta ai continui progressi tecnologici e giuridici. La GPL si basa su quattro libertà principali, che mirano a garantire all'utente la possibilità di [16, p. 60]:

1. eseguire il software per qualsiasi finalità o scopo;
2. studiare il funzionamento del programma e modificarlo;
3. distribuirne delle copie;
4. mutarlo, migliorarlo e condividerne le migliorie.

Il principio fondamentale della GPL è il *copyleft*, che ribalta la tradizionale logica del copyright: chi vuole ridistribuire un'opera deve mantenere le medesime condizioni di libertà, impedendo in questo modo, che il codice originariamente libero venga "chiuso" e assorbito in software proprietari [18, p. 41-43].

Contrariamente, altre licenze software adottano un approccio più permissivo, come la *MIT* o la *BSD*, che consentono agli utilizzatori un'ampia libertà di riuso anche in codici proprietari. La differenza dunque è che la GPL garantisce sempre la libertà del codice, anche dopo rielaborazione, invece le licenze permissive rischiano che il software venga inglobato in progetti chiusi [16, p. 96-97].

Conclusione

Creative Commons e GNU GPL si focalizzano su ambiti diversi ma rispondono sempre e comunque ad una stessa logica: semplificare e garantire il riuso delle opere. In entrambi i casi il diritto d'autore non viene mai abbandonato, bensì reinterpretato come mezzo di abilitazione collettiva, piuttosto che di restrizione. Ciò costituisce un passaggio fondamentale nel percorso che condurrà, nel capitolo successivo, a dettagliare ed approfondire ulteriormente il legame tra l'informatica e il diritto d'autore.

Capitolo 2

Informatica e diritto d'autore

2.1 Il software come opera dell'ingegno

2.1.1 Tutela giuridica del codice: definizioni, origini e differenze secondo le Direttive 91/250/CEE e 2009/24/CE

Il software: nuova categoria di opere dell'ingegno

Il software ha gradualmente assunto, dagli anni settanta, un ruolo importante non solo nell'industria dell'informatica, ma anche nel mondo del diritto della proprietà intellettuale. La sua è infatti una natura ibrida: è allo stesso tempo linguaggio tecnico ma anche creazione intellettuale. Ciò ha posto sin da subito la questione della sua tutela giuridica. In Europa, si trovano le prime risposte normative con le Direttive 91/250/CEE e 2009/24/CE, che hanno qualificato il programma informatico come opera dell'ingegno protetta, al pari delle opere letterarie, dal diritto d'autore [16, p. 31-32]. Questa scelta è dovuta proprio dal fatto che il software, pur avendo una dimensione funzionale, è di fondo costituito da codice scritto in linguaggio sorgente, che è possibile assimilare ad un testo, quindi passibile di protezione autoriale più che brevettuale. In Italia, questi principi sono stati recepiti nella Legge sul diritto d'autore, la n°633 del 22 aprile 1941, tramite il d.lgs. 518/1992, che ha introdotto la disciplina specifica dei programmi per elaboratore

nella LDA (artt. 64-bis–64-quater), poi aggiornata in coerenza con la direttiva 2009/24/CE.

Origine della tutela

Il diritto d'autore nasce in un'epoca sicuramente "non digitale", come visto anche nel capitolo precedente, con il copyright inglese e il droit d'auteur francese, che ricordiamo essere stati concepiti in origine per le opere letterarie ed artistiche. La tutela del software, che nasce in un periodo in cui la rivoluzione digitale era ancora in fase di sviluppo, è frutto in realtà di un adattamento a ciò: il codice sorgente viene visto come "testo" e quindi protetto dal copyright. Questa impostazione differisce dal modello statunitense, dove si è discusso a lungo di una possibile "brevettabilità" degli algoritmi, discussioni che hanno poi riconosciuto del limiti, in quanto il brevetto tutela invenzioni tecniche e non idee espresse con linguaggi formali.

Differenza tra diritto d'autore e brevetto nel software

Volendo confrontare i due tipi di tutele, la differenza principale sta proprio nell'oggetto della protezione:

- il *diritto d'autore*: tutela la forma creativa ed espressiva del codice, il "modo" in cui è scritto, non l'idea sottostante;
- il *brevetto*: protegge un'invenzione tecnica, capace di produrre un "effetto tecnico" innovativo ed originale.

Nel software questo confine è un po' problematico: un algoritmo, di per sè, è una sequenza logico-matematica, comparabile ad una formula, e come tale non è brevettabile [18, p. 114-115]. Per rientrare nell'ambito brevettuale dovrebbe essere integrato in una soluzione tecnica più grande, come ad esempio un sistema di compressione dati o un metodo crittografico con applicazione industriale. La scelta in Europa, illustrata brevemente in precedenza, di privilegiare il copyright, ha garantito una protezione più uniforme e meno restrittiva, evitando la diffusione di brevetti di "pura logica", che nel tempo avrebbero sicuramente ostacolato l'innovazione e l'interoperabilità.

DIRITTO D'AUTORE	BREVETTI
Tutela dei programmi per elaboratore (software) realizzati da una persona fisica	Tutela del software quando incorporato in un'invenzione realizzata da una persona fisica
Requisiti per la tutela: carattere di originalità e novità	Requisiti per la brevettabilità: novità, originalità, applicazione industriale e carattere tecnico
Nessuna formalità richiesta per ottenere tutela	Necessaria una procedura di registrazione presso uffici autorizzati
Tutela per tutta la vita dell'autore e fino a 70 anni dopo la sua morte	L'invenzione sarà tutelata per 20 anni dalla data di registrazione

Figura 2.1: Tabella comparativa tra diritto d'autore e brevetto
Fonte: Studio Legale Stefanelli

Verso il funzionamento tecnico

Comprendere la logica di questa tutela giuridica richiede un approfondimento tecnico del software: il diritto d'autore protegge il codice, detto sorgente, e l'organizzazione del programma, non il risultato delle sue elaborazioni. È quindi necessario fare distinzione tra codice sorgente, compilato ed eseguibile, aspetti illustrati nel prossimo paragrafo, per comprendere meglio come il diritto interagisca con i diversi livelli del software.

2.1.2 Aspetti tecnici del codice: sorgente, compilato, eseguibile

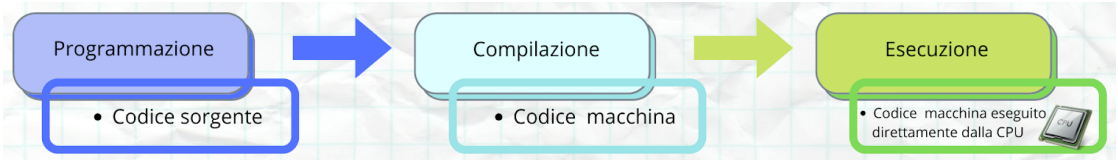


Figura 2.2: Passaggio da codice sorgente a programma eseguibile
Fonte: AulaB

- **Codice sorgente: il linguaggio dell'autore**

Alla base di ogni software informatico vi è il cosiddetto *codice sorgente*, cioè un'insieme di istruzioni informatiche, scritte dallo sviluppatore, in un linguaggio di programmazione ad alto livello, ovvero facilmente comprensibile all'essere umano, come: C, C++, C#, Java, Python, JavaScript, PHP, Dart, Kotlin e tanti altri. Questo codice è, sostanzialmente, un testo caratterizzato da una propria semantica e sintassi specifica, che descrive all'elaboratore cosa fare, istruzione dopo istruzione. Un buon codice sorgente, oltre che essere funzionale, esprime anche originalità e stile, può essere considerato un prodotto "artistico" della programmazione. Proprio qui interviene il diritto d'autore che riconosce protezione al sorgente come opera letteraria. Nello specifico la Direttiva 2009/24/CE equipara il codice sorgente a un testo, riconoscendo i diritti morali e patrimoniali [19]. La creatività infatti risiede nella scrittura del sorgente e non tanto nell'esecuzione del programma [16, p. 8]. Da un punto di vista più pratico pubblicare il codice sorgente ne garantirebbe trasparenza e possibilità di verifica, mentre mantenerlo segreto aiuterebbe a limitarne la modificabilità e lo studio da parte di terzi, come avviene infatti nel software proprietario.

- **Compilazione: dal testo al linguaggio macchina**

Un computer non è capace di interpretare direttamente le istruzioni scritte dall'uomo, seppur in linguaggio di programmazione. Per funzionare infatti necessità di un linguaggio diverso, composto da istruzioni binarie. Per questo motivo il codice sorgente, descritto in precedenza, deve essere processato da un apposito programma, detto *compilatore*, che lo traduce in *codice oggetto* e successivamente *codice macchina*. Il processo della compilazione è dunque tecnicamente fondamentale: prende in ingresso il file con il sorgente e produce, in uscita, come risultato un file binario eseguibile dal computer. Da precisare però che questa trasformazione non è meramente meccanica, comporta in realtà varie ottimizzazioni, traduzioni semantiche e sintattiche ed operazioni di linking con librerie esterne, ovvero l'inclusione di codice di terze parti. Riassumendo in altre parole il testo scritto dall'autore, il programmatore in questo caso, viene trasformato in linguaggio comprensibile dal processore. Sul piano giuridico

le operazioni di compilazione non danno origine ad una nuova opera, ma sostanzialmente ad una forma derivata del medesimo software. Sempre la Direttiva 2009/24/CE chiarisce infatti che la tutela copre sia il sorgente sia le forme derivate come il compilato [19, Art. 1(2)]. Ciò significa che anche i codici binari, pur non essendo leggibili dall'uomo, godono della stessa tutela e impediscono quindi ad altri la duplicazione o la distribuzione non autorizzate.

- **Codice eseguibile: il livello dell'utente**

Il prodotto finale della compilazione è il *codice eseguibile*, che viene normalmente distribuito agli utenti finali sotto forma di file binari: come file *.exe* per software Windows, file *.apk* per applicativi mobile Android o file *.ipa* per applicativi mobile iOS. L'eseguibile è la traduzione finale costituita da sequenze di bit, interpretabili unicamente dall'hardware. Da un punto di vista tecnico è ciò che permette all'utente di vedere il programma in azione in modo semplice: cliccando sulla relativa icona il sistema operativo carica in memoria le istruzioni e il processore le esegue in tempo reale. Tuttavia dal file eseguibile non è possibile risalire immediatamente al funzionamento interno del software, se non per mezzo di tecniche avanzate e complesse come il reverse engineering, approfondite nel prossimo paragrafo e comunque regolamentate [18, p. 29]. Sul piano giuridico gli effetti di questa distanza tra l'eseguibile e il sorgente sono abbastanza significativi. La distribuzione del solo file eseguibile impedisce all'utente di conoscere le logiche di funzionamento del programma, lasciandolo "in balia" della licenza, è quindi il sorgente la condizione di libertà, dato che solo in possesso di esso è possibile studiare e modificare il software. Nei modelli proprietari queste caratteristiche vengono propriamente sfruttate come mezzo di controllo e di chiusura.

2.1.3 Reverse engineering e interoperabilità: quadro tecnico e normativo (Direttiva 2009/24/CE e L. 633/1941)

Alla luce della netta distinzione tra codice sorgente, compilato ed eseguibile, e considerato che l'utente spesso dispone soltanto dell'eseguibile, diventa centrale

domandarsi in che misura sia lecito e possibile risalire dalla forma binaria alle logiche originarie del programma, per garantirne magari l'interoperabilità: questo è precisamente l'ambito del *reverse engineering*.

Significato tecnico del reverse engineering

Il *reverse engineering* applicato al software è quella tecnica che permette di risalire dal codice eseguibile, di norma distribuito pubblicamente agli utenti, ad una rappresentazione più comprensibile del programma, con l'obiettivo di capirne il funzionamento interno e la struttura. Da un punto di vista tecnico non è mai possibile ricostruire precisamente e perfettamente il codice sorgente originale, grazie al RE si riesce però ad avere una rappresentazione approssimativa o semplificata, utile a capire come il software elabora i dati, quali moduli utilizza o in che modo interagisce con gli altri programmi.

Il reverse engineering può essere attuato mediante due approcci, che talvolta vengono tra loro integrati:

- l' *analisi statica*: che si concentra sul codice decompilato o binario, e che consente di estrarre informazioni strutturali e cardinali del software, come dipendenze tra moduli, chiamate a funzioni o grafi di controllo, ovvero mappe dei possibili percorsi che il codice può seguire. Il suo vantaggio principale è fornire una visione nel complesso della struttura del programma;

- l' *analisi dinamica*: che osserva in modo diretto l'esecuzione del programma, monitorando l'interazione tra i moduli e il flusso dei dati in tempo reale. Dà garanzia sull'effettività dei comportamenti rilevati anche se in modo parziale e limitato.

Entrambi gli approcci, con i loro vantaggi e limiti, vengono spesso utilizzati, sia singolarmente, che complementarmente per ottenere ricostruzioni più accurate possibili del funzionamento interno di un software. [20, p. 60].

Interoperabilità

Il reverse engineering è spesso adottato con l'obiettivo di risolvere problemi di *interoperabilità*, ovvero la capacità di sistemi informatici diversi di funzionare

insieme e di comunicare tra loro. Tipico esempio è l'implementazione di protocolli senza aver accesso al codice sorgente o più banalmente l'apertura di un file prodotto da un noto software con un'applicazione concorrente. L'assenza dell'interoperabilità genera il fenomeno del *blocco da fornitore*, ovvero la dipendenza imposta da un unico produttore software, che osteggia l'innovazione e la concorrenza. È proprio per questo che la normativa europea ha cercato di bilanciare due esigenze ben distinte e tra loro contrapposte: da un lato, la tutela del software come opera d'ingegno, dell'altro, non impedire l'integrazione tecnologica talvolta necessaria alla crescita digitale. Il software viene quindi protetto come opera, ma le idee ed i principi, anche a base delle interfacce, restano fuori dalla tutela per impedire monopoli su elementi tecnici e indispensabili. [21, p. 142-143]

Divieti ed eccezioni

In linea di massima, la decompilazione e il reverse engineering non sono consentiti, in quanto rappresentano una riproduzione e trasformazione di un'opera non autorizzata. Tuttavia la direttiva di riferimento, la 2009/24/CE, contempla un'eccezione, in particolar modo nell'articolo 6. Viene infatti consentita la decompilazione solo nella misura necessaria per l'ottenimento di informazioni indispensabili all'interoperabilità di un software autonomamente creato. L'eccezione è soggetta condizioni specifiche: [19, Art. 6]

1. le informazioni non devono già essere disponibili tramite altri canali o altri modi;

2. le attività debbono limitarsi alle sole parti del software necessarie alla sua interoperabilità;

3. tutte le informazioni ottenute non possono poi essere sfruttate per sviluppare un programma simile o concorrente, tanto meno per violare i diritti dell'autore originario.

Anche l'articolo 5 aggiunge delle eccezioni, permette infatti all'utente di studiare ed osservare il programma durante l'utilizzo, ed addirittura di decompilarlo, quando ciò è strettamente necessario per correggere degli errori che ne compromettono il corretto funzionamento [19, Art. 5]. La corrispondente disciplina italiana si

rinviene sempre nella legge 633/1941: in particolare, l'art. 64-ter definisce i diritti esclusivi sul software, mentre l'art. 64-quater consente l'osservazione/studio del programma e la decompilazione nella misura strettamente necessaria all'interoperabilità [22].

2.1.4 Casi pratici

SAS Institute v. World Programming Ltd

Nella definizione dei limiti del diritto d'autore applicato al software rappresenta un passaggio importante il caso *SAS Institute*. La società in questione, produttrice di un linguaggio di programmazione proprietario, chiamato SAS System, aveva accusato una sua concorrente di mercato, l'azienda World Programming Ltd. (WPL). L'accusa contestava la creazione di un software compatibile da parte della WPL capace di esegurie programmi scritti in linguaggio SAS, riproducendo così strutture e funzionalità pressochè identiche al programma proprietario originale.

La Corte di Giustizia UE con la sentenza del 2 maggio 2012 nella causa C-406/10, chiamata a valutare la portata della tutela, ha dunque stabilito che: i linguaggi di programmazione, i formati file e le funzionalità di un programma non sono protetti dal diritto d'autore poiché non rappresentano forme di espressione, ma idee e principi. [23] La decisione ha finalmente chiarito che non equivale a una violazione l'imitazione delle funzionalità di un programma informatico, purché non si tratti di riproduzione del codice vero e proprio. È stato quindi escluso che la realizzazione di un software, capace di interpretare dei file creati con altri programmi preesistenti, configuri una contraffazione: proteggere integralmente le interfacce ostacolerebbe di l'interoperabilità e il naturale progresso dell'innovazione tecnologica. [24]

Questo caso ha dunque indicato il giusto confine tra l'illecita copia del codice e la lecita riproduzione delle funzioni, rimarcando la necessità di garantire una libertà tecnica senza vincoli eccessivi.

Top System SA v. Belgian State

Circa dopo un decennio dal precedente caso SAS la Corte di Giustizia è tornata ad esprimersi su una tematica simile, esprimendosi sui limiti della decompilazione e l'uso legittimo del software. Questa vicenda trova luogo in Belgio, dove sotto accusa è finita la Pubblica Amministrazione che aveva modificato, senza autorizzazione del titolare, un programma fornito dalla software house *Top System SA*. L'azienda sosteneva che l'intervento costituisse una violazione dei diritti d'autore, mentre la Pubblica Amministrazione dichiarava di aver proceduto in tal senso per dover risolvere dei malfunzionamenti informatici, detti bug, che impedivano il corretto uso del programma.

La Corte di Giustizia UE con la sentenza del 6 ottobre 2021 nella causa C-13/20, chiamata a valutare la portata della tutela, ha stabilito che l'utente legittimo può decompilare e modificare un programma nella misura necessaria a risolvere errori che ne compromettono il funzionamento [25]. Anche questa decisione è in linea con l'impianto europeo di equilibrio tra libertà d'uso e protezione del diritto d'autore. La Corte ha inoltre voluto valorizzare il principio di autonomia funzionale dell'utente legittimo: chi dispone di una copia del programma deve poter garantirne il coretto funzionamento, pure mediante tecniche di decompilazione, analisi e correzione. [21, p. 151]

Questo secondo caso ha quindi consolidato come, la tutela, non debba essere ostacolo alla manutenzione, alla sicurezza, all'analisi ed all'interoperabilità dei software.

Riflessioni conclusive

Alle luce delle direttive e dei casi discussi, la giurisprudenza europea mostra una linea coerente:

- *proteggere l'espressione creativa* dei software nel codice sorgente;
- *escludere dalla protezione le idee e i principi* come linguaggi, formati ed interfacce, favorendo la concorrenza e l'interoperabilità dei programmi;

- *consentire la decompilazione* dei software, nei limiti previsti in favore dell'interoperabilità e della correzione errori.

Questo approccio vuole garantire un equilibrio tra la tutela e l'innovazione tecnologica. I casi SAS e Top System rappresentano infatti passaggi fondamentali nella costituzione di un diritto d'autore che si adatti alle esigenze del mondo dell'informatica, dei software e del progresso.

2.2 Opere digitali e piattaforme online

2.2.1 Introduzione alle opere digitali

Natura informatica e dipendenza tecnologica

Nel contesto odierno, le opere digitali rappresentano una categoria di contenuti creativi, la cui esistenza e disponibilità sono strettamente connesse alla tecnologia che le genera e le rende fruibili. In termini più informatici, ogni opera digitale è rappresentata da una sequenza di bit, ovvero una sequenza binaria di dati 0 e 1, che necessita, fisiologicamente, di un sistema software ed hardware per essere interpretata e resa tangibile. Nell'era digitale le opere dell'ingegno non si identificano più quindi con il supporto fisico, ma con l'informazione che viene codificata e resa trasmissibile tramite infrastrutture tecnologiche informatiche.

Differentemente dalle opere analogiche con una propria autonomia materiale, quelle digitali sono fortemente dipendenti dai formati, i protocolli e le piattaforme su cui vengono create e diffuse:

- Il *formato*: che determina come l'informazione è organizzata, esempi di formati possono essere:
  - Immagini raster: *JPG* , *PNG* , *GIF*
  - Immagini vettoriali: *SVG* , *EPS* , *AI*
  - Container video: *MP4* , *MOV* , *AVI* , *MKV*
  - Codec video: *H.264 / AVC*, *H.265 / HEVC*, *VP9*, *AV1*

  - Audio compressi (lossy): *MP3*
  - Audio senza perdita (lossless): *WAV*, *FLAC*
  - Documenti e testi: *PDF*, *DOC*, *TXT*
  - Formati compositi o multimediali: *HTML*, *XML*, *ZIP*

- Il *protocollo di comunicazione*: che regola le modalità per la comunicazione e la trasmissione, esempi di protocolli possono essere: *HTTP*, *HTTPS*, *TCP/IP*;

- La *piattaforma*: che costituisce l'ambiente di elaborazione e distribuzione, è il contesto tecnico e giuridico nel quale l'opera ha un valore economico ed assume un significato.

Ne consegue che in questo contesto l'opera ha una forma non solo espressiva ma anche tecnologica, la creazione stessa non può prescindere dall'infrastruttura tecnologica che la ospita.

La creazione di un'opera digitale

Figura 2.3: Passaggio da contenuto creativo a opera digitale diffusa
Fonte: auto-prodotta

L'esistenza di un'opera digitale e la sua creazione si articolano principalmente in tre fasi:

1. *Codifica*: è la conversione di un contenuto creativo come un testo, un suono o un immagine in formato digitale. Avviene mediante software o algoritmi che traducono l'informazione in una sequenza binaria.

2. *Memorizzazione*: una volta codificata, l'opera è memorizzata su un supporto di tipo elettronico, come: un hard-disk, un server o un cloud. La memorizzazione digitale è tecnicamente una forma di riproduzione secondo l'art. 13 della L. 633/1941.

3. *Trasmissione*: è l'ultima fase, rende l'opera accessibile ai destinatari più remoti, solitamente tramite una rete, come Internet. Sul piano giuridico in questo caso la "comunicazione al pubblico" è disciplinata dall'art. 16 della L. 633/1941.

Verso la distribuzione e i contenuti generati dagli utenti

L'analisi condotta fin'ora rappresenta la base dell'ecosistema digitale contemporaneo, la trasmissione e la fruizione oggi giorno utilizzano modalità più avanzate come i content delivery network, tecnologia approfondita insieme allo streaming nel paragrafo successivo, con le loro implicazioni tecniche e giuridiche. Parallelamente, la diffusione sui social e le piattaforme collaborative ha portato gli utenti a non essere solo fruitori di opere digitali, ma loro stessi i creatori e distributori, generando il fenomeno dell'user generated content, anch'esso approfondito nei prossimi paragrafi insieme ai processi di upload, encoding e riconoscimento automatico dei contenuti.

Concludendo, l'opera digitale si delinea come qualcosa di tecnicamente e giuridicamente complesso, il cui ciclo di esistenza, dalla codifica alla fruizione in larga scala, è interamente mediato da sistemi informatici e reti digitali.

2.2.2 Streaming: funzionamento e tutela

Introduzione tecnica

Lo *streaming* è una tecnologia che consente la trasmissione e l'accesso a dati multimediali e contenuti digitali in tempo reale, senza più la necessità di scaricare file integrali sui dispositivi. Differentemente dal *download*, dove l'opera digitale deve esser appunto scaricata completamente prima della fruizione, lo streaming permette di iniziare la riproduzione anche se i dati non sono completamente trasferiti, ma ancora in trasmissione attraverso la rete.

Questo processo descritto sinora da un punto di vista informatico richiede una comunicazione continua tra due soggetti:

- il *client* che richiede il contenuto e ne accede in tempo reale: riceve i dati attraverso la rete;
- il *server* che offre l'opera multimediale a richiesta: invia i dati attraverso la rete.

Il contenuto è solitamente un flusso multimediale, audio o video, che viene tecnicamente suddiviso in pacchetti dati digitali, inviati in sequenza e riassemblati dal lettore multimediale del client.

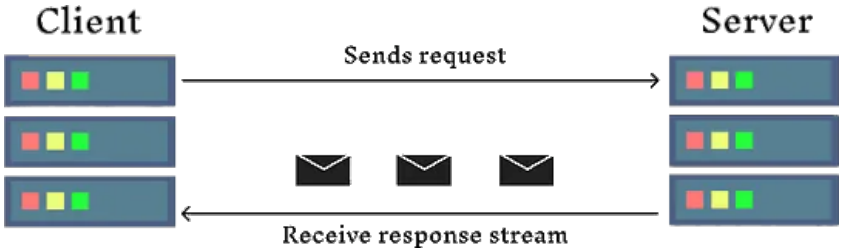


Figura 2.4: Streaming dati tra client e server
Fonte: Medium.com

Questa modalità di accesso ai contenuti offre importanti vantaggi in termini di rapidità ed accessibilità, e ovviamente complementari svantaggi come la maggiore complessità gestionale. La trasmissione in streaming deve assolutamente garantire continuità e sincronizzazione, evitando dunque qualsiasi tipo di interruzioni, anche minime, dovute dalla congestione della rete o l'instabilità della connessione [26, p. 9-10].

Lo streaming dunque, oltre ad essere un innovativo metodo di diffusione dei contenuti, è un insieme di processi coordinati che permette la fruizione immediata delle opere d'ingegno nell'attuale contesto digitale.

Buffering, protocolli e tipologie

Uno degli elementi tecnici fondamentale per avere i vantaggi propri dello streaming, come accessibilità ed immediatezza dei contenuti in tempo reale, è il sistema di

buffering. Come accennato nel paragrafo precedente la riproduzione in streaming dei contenuti deve essere garantita anche in presenza di ritardi o perdite di pacchetti, il buffering permette ciò grazie ad un accumulo temporaneo di dati in memoria locale, chiamato *buffer*. Durante questa fase, il lettore multimediale del client crea una sorta di "riserva" di contenuto, che viene fruito mentre i nuovi dati continuano ad arrivare dal server.

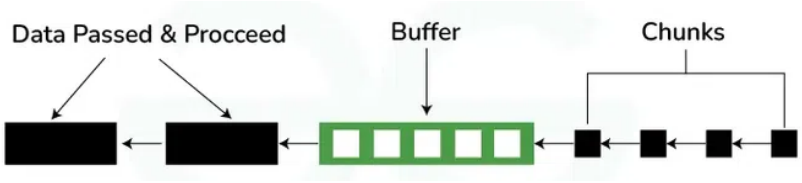


Figura 2.5: Sistema di buffering in un flusso streaming
Fonte: GeeksforGeeks

Questo processo comporta quindi la creazione di copie temporanee dell'opera, di rilevanza giuridica effimera, data la piccolissima quantità di dati memorizzati per un tempo minimo pressoché nullo, che garantiscono però un'esperienza fluida all'utente.

La trasmissione di questi flussi si basa sull'impiego di diversi protocolli di reti specializzati, con compiti specifici [26, p. 13]:

- *RTP (Real-time Transport Protocol)*: che garantisce il trasporto in tempo reale dei pacchetti che compongono il contenuto multimediale;
- *RTCP (Real-time Control Protocol)*: che garantisce la qualità del servizio grazie al monitoraggio e la sincronizzazione dei flussi;
- *RTSP (Real-time Streaming Protocol)*: che gestisce la comunicazione tra il client e il server e consente le funzionalità di play, pausa e stop.

Sul fronte operativo, lo streaming può essere diviso in due tipologie [26, p. 10]:

- *Live* streaming: quando la trasmissione è in tempo reale, utilizzato per trasmettere contenuti come eventi sportivi o dirette varie;
- *On-demand* streaming: quando è l'utente ad accedere al contenuto pre-registrato e sempre disponibile, come film, serie tv o podcast.

In entrambi i caso lo schema tecnico è il medesimo, cambiano invece le logiche di distribuzione e sincronizzazione.

Profili giuridici e tutela del diritto d'autore

Lo streaming, sotto il profilo giuridico, si trova tra due diritti esclusivi che vengono riconosciuti all'autore: la *riproduzione* e la *comunicazione al pubblico*. La visione o l'ascolto di contenuti multimediali in streaming non comportano il salvataggio in locale dell'opera, però il sistema genera copie temporanee nel buffer, necessarie alla trasmissione del flusso.

La direttiva InfoSoc 2001/29/CE al comma 1 dell'articolo 5 specifica che tali atti rientrano nella protezione del diritto d'autore a meno che non siano transitori, privi di valore e parte di un procedimento tecnico, come nel caso del sistema buffering [27, Art. 5]. Inoltre la Corte di Giustizia dell'Unione Europea nella sentenza Infopaq (C-5/08) ha ulteriormente chiarito che questa memorizzazione di frammenti di un'opera, può essere un atto di riproduzione ai fini di tutela se non rispetta tali condizioni. Spostandoci invece nel sistema italiano, la legge di riferimento è la n°633 del 22 aprile 1941 che riconosce all'autore, il diritto, in esclusiva di riprodurre e comunicare al pubblico la propria opera [22, Art. 13, 16]. Tuttavia l'avvento della rete internet, dello streaming e delle piattaforma di distribuzione ha moltiplicato questi atti in forme automatizzate e non delimitabili.

La giurisprudenza, più recentemente, ha evidenziato come la trasmissione in streaming, dunque senza download permanente, possa configurare una violazione del diritto d'autore se avviene senza l'autorizzazione del titolare dei suoi diritti. Diversamente non si parla di violazione quando le riproduzioni tecniche temporanee sono necessarie appunto al funzionamento dei servizi di streaming, considerate dunque lecite, purché rispettino sempre la transitorietà e l'accessorietà [28, p. 240-241].

2.2.3 User Generated Content e distribuzione: aspetti tecnici e normativi (Direttive 2000/31 e 2019/79 e L. 633/1941)

Introduzione tecnica

La distinzione tra creatore e fruitore di contenuti, con l'avvento della digitalizzazione, si è lentamente assottigliata. La coltura online è fortemente partecipata da utenti che producono e diffondono contenuti, che prendono dunque il nome di *User Generated Content*, abbreviato *UGC*. La definizione classica descrive infatti gli UGC come contenuti multimediali creati proprio dagli utenti, e grazie alla semplificazione delle tecnologie, da loro messi poi a disposizione in rete. Il digitale permette oggigiorno di combinare facilmente qualsiasi contenuto, come testi, immagini, suoni e video, generando opere derivate, remixate o addirittura rielaborate con strumenti di editing e piattaforme di diffusione. [29]

La produzione degli UGC nasce come attività non professionale e del tutto spontanea, le finalità non sono prevalentemente di tipo economico, ma di espressione personale. Anche secondo Ofcom questi contenuti sono espressione di un apporto creativo, privi di lucro e frutto di un'attività non principale [30, p. 529]. Si tratta quindi di una forma di creatività diffusa e resa attuabile dalle infrastrutture del Web 2.0, con annesse piattaforme che ne amplificano la diffusione.

Piattaforme digitali

La diffusione degli UGC avviene attraverso le piattaforme digitali che fungono quindi da intermediari tecnici tra gli utenti creatori e gli utenti fruitori. Le infrastrutture informatiche messe a disposizione da questi ambienti si occupano dell'encoding, del caricamento e della distribuzione dei contenuti, svolgono di conseguenza un ruolo centrale nella gestione e controllo dei diritti d'autore.

Di piattaforme ne esistono diverse, differenziate in base al tipo di contenuto che permettono di creare e diffondere, come:

- 
  YouTube : principale piattaforma per la condivisione video, importante riferimento per la produzione e monetizzazione dei contenuti;
- 
  TikTok : basata su clip video molto brevi e applicativi di editing integrati che favoriscano e incentivano la creatività spontanea;
- 
  Instagram : inizialmente improntata sulla sola fotografia, oggi ampliata con video, storia e reel, offre anche funzioni di interazione diretta;
- 
  Twitch : prevalentemente dedicata allo streaming in tempo reale di videogiochi o contenuti di intrattenimento ludico ricreativo;
- 
  SoundCloud : orientata alla distribuzione di contenuti musicali autoprodotti.

Queste piattaforme oltre ad essere degli spazi di pubblicazione offrono anche sistemi di filtraggio e monitoraggio automatizzato dei contenuti condivisi. Implementano software avanzati in grado di individuare opere sotto protezione, di gestire i reclami e stabilire le modalità di utilizzo.

Bilanciamento giuridico tra creatività e diritto d'autore

La produzione e condivisione di contenuti e la grande partecipazione attiva da parte degli utenti, ha portato la necessità di trovare un equilibrio tra la libertà creativa e la tutela del diritto. Pratiche tipiche come remix, parodie e riuso trasformato sono grandi forme di espressione digitale, ma pongono questioni di legittimità in quanto vengono spesso utilizzate opere preesistenti tutelate da protezione. Applicando rigorosamente le norme tradizionali, esplorate fin'ora, si rischia di reprimere la creatività diffusa, anche nei casi in cui i contenuti non incidono sullo sfruttamento economico, ma hanno solo fini espressivi e creativi. Il pensiero attuale ha evidenziato la necessità di introdurre questo bilanciamento normativo, che allo stesso tempo riconosca il valore degli UGC e tuteli gli interessi economici dei titolari dei diritti. [30, p. 521]

Nel quadro europeo la Direttiva Europea 2000/31 sul commercio elettronico aveva infatti inizialmente stabilito, con l'articolo 14, un'esenzione di responsabilità per i fornitori dei servizi di hosting imponendogli di rimuovere tempestivamente

eventuali contenuti illeciti, caricati dagli utenti, quando venivano a conoscenza della loro presenza [31, Art. 14]. Importante sottolineare che la direttiva risale a circa due decenni fa, con la comparsa degli UGC e le innovative piattaforme digitali, questo modello è presto divenuto inadeguato: le piattaforme non sono più dei semplici intermediari passivi, ma sono ora "host attivi" nella selezione, classificazione e monetizzazione dei contenuti multimediali caricati dagli utenti [30, p. 550]. Ad aggiornare ed evolvere la situazione normativa è stata la Direttiva Europea 2019/790 con l'articolo 17, stabilendo che i prestatori dei servizi di condivisione, come le piattaforme, sono direttamente responsabili per gli atti di comunicazione al grande pubblico effettuati dagli utenti, salvo che adottino misure efficaci per prevenire diffusioni non autorizzate o siano autorizzati dai titolari dei diritti [12, Art. 17].

In Italia, l'art. 14 della direttiva 2000/31 è stato recepito dal d.lgs. 70/2003; più di recente, la direttiva 2019/790 invece è stata attuata con il d.lgs. 177/2021, che ha adeguato la legge n°633 del 1941, legge sul diritto d'autore, al nuovo regime dei servizi di condivisione di contenuti online.

Al termine di questo percorso giuridico si è quindi trovato un equilibrio che favorisce una circolazione degli UGC assicurando allo stesso tempo la giusta remunerazione ai titolari dei diritti e la tutela della creatività digitale.

2.3 Misure tecnologiche di protezione

2.3.1 DRM: definizione, funzionamento e impatti

Definizione e principi generali

Il vocabolo *Digital Rights Management*, abbreviato DRM, compare parallelamente allo sviluppo del web, che ha portato alla nascita dei primi mercati di contenuti digitali, intorno alla metà degli anni novanta. Questa sigla indica tutti i sistemi tecnologici che sostituiscono o affiancano i tradizionali strumenti normativi di controllo dei diritti d'autore. Il DRM comprende tutte quelle procedure sia hardware che software in grado di descrivere, proteggere, identificare e monitorare l'uso dei contenuti digitali, dalla creazione, alla diffusione fino alla fruizione da

parte degli utenti [32, p. 5]. Il DRM lavora come un'infrastruttura automatizzata, a differenza dei classici e più semplici sistemi di protezione delle copie. Queste nuove tecnologie non si limitano a vietare la duplicazione delle opere digitali, ma determinano perfino come, dove e per quale lasso di tempo il contenuto potrà essere fruito, traducendo in codice informatico le clausole del diritto [32, p. 2]. In questo senso il DRM può essere visto come una vera e propria "informatizzazione del contratto", in cui la volontà negoziale è sostituita dal software stesso e da come viene impostato. Il suo scopo principale, dunque, è garantire ai titolari dei diritti il controllo sulle modalità di accesso all'opera digitale e preservare la sua integrità economica, impedendo che l'utente finale ne possa diventare il proprietario. Il fruitore non acquista più l'opera bensì il diritto all'uso temporaneo.

Funzionamento tecnico

Un sistema DRM è generalmente articolato in tre componenti:

- Il modulo di *cifratura* dei contenuti: garantisce che i file, come musica, film o e-book, siano distribuiti in forma crittografata e possano essere decifrati solo dagli autorizzati;
- Il sistema di *autenticazione e licenza*: gestisce le chiavi di decriptazione verificando l'identità dell'utente;
- Il *controllo d'uso*: definisce le condizioni di fruizione dei contenuti e le fa rispettare.

Negli ecosistemi digitali moderni, in particolar modo nei servizi di streaming video, queste funzionalità sono integrate in sistemi complessi basati su *Trusted Execution Environments* (TEE), componenti dedicati che provvedono alle operazioni complesse di cifratura e gestione delle chiavi, garantendo massima sicurezza. Oggigiorno i sistemi software DRM maggiormente utilizzati sono tanti, come: *Apple FairPlay*, *Microsoft PlayReady* e *Google Widevine*, diffusi in larga scala su miliardi di dispositivi [33, p. 1].

Il loro funzionamento si articola in diverse fasi:

Figura 2.6: Loghi dei principali sistemi DRM
Fonte: axinom.com

1. *Distribuzione del contenuto cifrato*: attraverso dei canali sicuri, resi tali da protocolli come *HTTPS* o *MPEG-DASH*;

2. *Richiesta di licenza*: indirizzata al server DRM da parte dell'applicazione in uso all'utente;

3. *Emissione della chiave*: necessaria per decriptare il contenuto e strettamente legata al dispositivo e all'identità dell'utente;

4. *Esecuzione controllata*: nel rispetto delle condizioni contrattuali e con verifica costante e periodica della riproduzione.

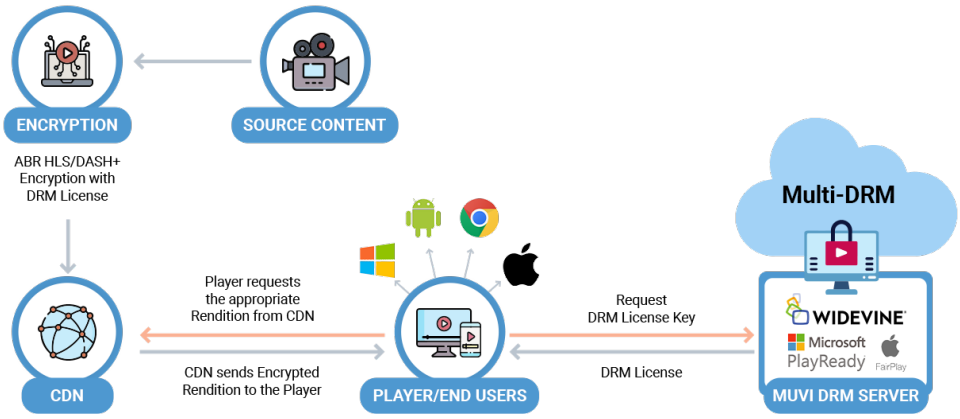


Figura 2.7: Diagramma del funzionamento di un sistema DRM
Fonte: muvi.com

In questo iter il punto di controllo è il dispositivo dell'utente stesso, il contenuto che viene riprodotto non viene mai realmente reso accessibile liberamente. In questo modello di sicurezza l'utente legittimo viene comunque considerato un

potenziale nemico, il rischio di violazione può infatti provenire dal fruitore che tenta di by-passare le protezioni del DRM. Recenti analisi hanno infatti portato alla luce problemi legati ad attacchi *side-channel*, vulnerabilità nella gestione delle chiavi crittografiche e mancanza di contromisure efficaci contro la crittografia quantistica [33, p. 7].

Implicazioni giuridiche e sociali

Sul fronte del diritto il DRM si trova in un incrocio tra regolazione tecnologica, contrattualistica e tutela amatoriale. Il potere tecnologico in mano ai gestori delle piattaforme, si trasforma di fatto in potere contrattuale, portando ad un rapporto sbilanciato tra fornitore e utente [32, p. 75]. Il fruitore accetta delle condizioni di licenza predisposte e non modificabili, si trova perciò obbligato, a dover rispettare i termini, da una struttura tecnica paragonabile ad un "giudice automatico" inflessibile. Ciò incide profondamente sull'equilibrio nel diritto d'autore tra interessi privati e pubblici. Le misure tecnologiche di protezione sono previste e regolamentate dagli articoli 6 e 7 dalla direttiva 2001/29/CE. Queste misure tutelano i titolari delle opere digitali, ma rischiano di limitare eccessivamente le eccezioni concesse come uso didattico, copia privata, parodia o conservazione del patrimonio.

Altra problematica è legata all'interoperabilità e tutela del consumatore, il DRM se applicato senza opportuni controlli pubblici può ridurre l'accessibilità, per esempio, potrebbe limitare l'uso di un contenuto digitale dipendentemente da: un periodo di tempo, un determinato dispositivo, l'inserimento di una password di accesso o la necessità di una costante connessione ad internet [34, p. 128]. La pratica ci mostra quindi che l'autonomia tecnica del DRM supera spesso la regolamentazione del legislatore, sostituendo la legge con l'algoritmo.

Conclusioni sul DRM

Il DRM è il punto di incontro, e di tensione, tra innovazione tecnologica e accesso alla conoscenza ed ai contenuti digitali. In termini informativi è un sofisticato ed avanzato sistema di sicurezza basato su cifratura, autenticazione e controllo, nei termini giuridici invece è una "codificazione" privata del diritto che rischia di

alterare un equilibrio tra pubblico e privato [32, p. 193]. Queste tecnologie digitali consentono inoltre di predeterminare, in anticipo, i termini ed i modi in cui un contenuto potrà essere fruito, un potere che può trasformare il diritto d'autore, da strumento di tutela in meccanismo di controllo eccessivo se non bilanciato da principi di interoperabilità e rispetto delle eccezioni.

2.3.2 Watermarking e fingerprinting: tecniche ed esempi

Introduzione: ruolo di watermarking e fingerprinting

Nell'ampio sistema di tutela digitale, watermarking e fingerprinting ricoprono un ruolo complementare rispetto ai DRM trattati finora, spostano infatti l'attenzione dal mero controllo all'accesso dei contenuti alla possibilità di tracciare, identificare e provare la paternità e le condizioni d'uso durante il ciclo di vita dell'opera digitale. Le due tecniche hanno scopi differenti:

- il *watermarking*: consiste nell'*incorporare* nel contenuto digitale un contrassegno interno capace di sopravvivere a trasformazioni e riutilizzi, in modo da essere sempre identificabile;
- il *fingerprinting*: consiste nell'*estrarre* del contenuto digitale un'impronta che ne riconosce l'identità senza però modificare il file originale.

Sui piani giuridico e tecnologico le due tecniche formano, insieme alla crittografia, i tre pilastri dei sistemi di gestione dei diritti digitali, su questa "triade" poggia l'intera architettura di questi sistemi. [32, p. 17].

Tecniche di watermarking

Il watermark digitale, da un punto di vista concettuale, è un'informazione inserita dentro il contenuto digitale qualsiasi esso sia, come un immagine, una traccia audio, un video o un documento. Lo scopo è quello di attestarne la provenienza, garantirne l'integrità e permetterne la tracciabilità.

Da un punto di vista applicativo invece, la marca applicata deve essere discreta, in modo da non deteriorare la qualità originale del file, allo stesso tempo però sufficientemente resistente alla varie trasformazioni o conversioni dei file,

garantendo una rivelabilità. Tecnicamente queste esigenze si riassumono in quattro proprietà fondamentali: *sicurezza*, *impercettibilità*, *individuabilità*, *robustezza*.

Da un punto di vista operativo si distinguono diverse tipologie di marcature:

- i *watermark visibili*: pensati essere altamente percettibili e per avere quindi un effetto immediatamente dissuasivo, l'utente finale inequivocabilmente riesce ad attribuire l'autore e la provenienza del contenuto al file stesso;
- i *watermark invisibili*: destinati invece ad una rilevazione da parte di software ed algoritmi specifici e non direttamente dall'essere umano ad occhio nudo.

Figura 2.8: File con watermark visibile (a sinistra) ed invisibile (a destra)
Fonte: sealpath.com

L'idea principale, al di là delle specifiche implementazioni, è che l'inserimento della marcatura avvenga in porzioni di segnale, selezionate perchè poco percettibile all'occhio o all'orecchio umano. La sfida tecnica è inserire la marca dove la sensibilità percettiva è presente, ma in modo minore, e la stabilità a compressioni, ridimensionamenti o ricampionamenti sufficientemente garantita per permetterne una buona estrazione e verifica. [35, p. 10-12]

Nel contesto audio l'inserimento si basa su modelli psico-acustici dell'udito che permettono di porre l'informazione sotto le soglie di mascheramento temporale e frequenziale, in modo da renderla trasparente all'ascoltatore, ma percettibile dal rivelatore. Questo approccio è considerato un vero e proprio modello comunicativo, in cui l'embedder invia un messaggio su di un canale affetto da rumori e il detector deve recuperarlo, con un tasso d'errore accettabile. [35, p. 38-39]

Tecniche di fingerprinting

Il fingerprinting, diversamente dal watermarking, non va a modificare il contenuto, il suo compito è invece quello di generare una firma, che può successivamente esser confrontata con dei database di riferimento per individuare eventuali corrispondenze con opere registrate.

Su scala industriale ne è un esempio il famoso *YouTube Content ID*, sistema di fingerprinting che automaticamente, al momento del caricamento di contenuti sulla piattaforma, ne analizza audio e video. L'estrazione dell'impronta digitale permette poi il confronto un database di file direttamente forniti dai titolari dei diritti d'autore. Un eventuale corrispondenza rilevata genera una rivendicazione, le conseguenze sono regolamentate e gestite dalle policy del titolare e possono portare a una delle seguenti ripercussioni [36]:

- il *blocco* del video, che non sarà quindi visibile sulla piattaforma;
- la *monetizzazione* del video, grazie ad annunci pubblicitari con conseguente condivisione dei guadagni;
- il *tracciamento* statistico delle visualizzazioni.

Da un punto di vista informatico, il valore, in generale del fingerprinting è proprio nella sua abilità nel riconoscere contenuti protetti anche quando hanno subito compressioni, tagli, ricampionamento o conversione. Il sistema, per farlo, si affida a delle soglie di similarità, che non devono essere ne troppo stringenti, ne troppo permissive, altrimenti aumenta il tasso di errore, che è comunque, inevitabilmente, sempre presente anche se in piccole percentuali.

Limiti

Facilità di rimozione o alterazione. I watermark sono progettati per resistere a trasformazioni ragionevoli, ma non godono di assoluta invulnerabilità. Operazioni come: compressione con perdita, filtraggi, ricampionamenti, ridimensionamenti, rotazione o trasformazioni analogico/digitali come stampa e scansione, possono

portare ad indebolire o cancellare la marca. Questi interventi sono catalogati differenziando tra [35, p. 32-34]:

- *attacchi alla robustezza*: che mirano a rendere inutile oppure a rimuovere il marchio;
- *attacchi di presentazione*: che modificano la marca in modo che l'algoritmo di verifica non sia utilizzabile;
- *attacchi di interpretazione*: che alterano la paternità, inserendo un altro marchio.

Oltre che gli attacchi di tipo *legale* che cercano di sfruttare ambiguità normative e tattiche processuali per mettere in dubbio la paternità e il valore del watermark, riducendo la tutela al diritto d'autore.

False detection. Altro caso limite sopratutto nei sistemi di fingerprinting dove la decisione, come già visto, è affidata a delle soglie. Abbassarle può portare alla generazione di falsi positivi per via di corrispondenze spurie, mentre alzarle aumenta i falsi negativi, non riconoscendo opere protette e dunque non tutelando opportunamente gli autori. A portare verso l'errore nel riconoscimento ci sono anche le piccole e normali distorsioni, introdotte dalla quotidiana fruizione come piccoli tagli o ricodifiche dei file.

Capitolo 3

Nuove frontiere e casi di studio

3.1 Blockchain, Smart Contracts e NFT

3.1.1 La blockchain come registro distribuito e immutabile per la protezione delle opere

Architettura essenziale e proprietà

Figura 3.1: Concatenazione dei blocchi nella Blockchain
Fonte: BibLus

Una *blockchain* è un registro distribuito in cui le varie operazioni sono raccolte in blocchi. Ogni blocco è caratterizzato da un proprio header che contiene: l'hash del blocco precedente e la radice Merkle delle transazioni del corrente blocco. Grazie a questa struttura i blocchi sono tra loro concatenati crittograficamente, la modifica di un solo bit andrebbe a cambiare la radice Merkle e conseguentemente

l'hash del blocco, andando così a rompere la catena. Ad ogni operazione la catena viene replicata su più nodi in rete ed aggiornate solo tramite un meccanismo di consenso [37, p. 13-15]. Tutto ciò si riassume in tre proprietà caratteristiche di questa architettura:

- *Integrità*: l'uso di hash e Merkle rende facilmente rilevabile una qualsiasi alterazione dei dati;
- *Immutabilità*: il meccanismo di consenso rende computazionalmente proibitivo, praticamente impossibile, riscrivere la storia della catena alterandola;
- *Tracciabilità*: ogni operazione è riconducibile al suo autore ed è verificabile, nulla avviene in anonimato.

Ciò rende questa tecnologia perfetta per le opere digitali dato che, ancorando l'hash di un opera, si riesce ad ottenere data certa, prova di anteriorità e prova di integrità, opponibili a terzi, dell'opera stessa. Se il file originale dell'opera cambiasse infatti l'hash non combacerebbe più, il sistema funge da vero e proprio "notaio digitale".

Permissionless vs permissioned: cosa cambia

È necessario chiarire che non tutte le blockchain sono uguali, si distinguono in base a chi è autorizzato a partecipare al processo di validazione e scrittura dei blocchi, si dividono così in due grandi categorie [38, p. 15-18]:

- blockchain *pubbliche (permissionless)*: si basano su ambienti dove i partecipanti non si conoscono, il sistema utilizza meccanismi di consenso ad alta intensità computazionale, risulta infatti un sistema energivoro e meno efficente ma con massima trasparenza e decentralizzazione, non esiste un'autorità unica centrale;
- blockchain *private o consortili (permissioned)*: limitano invece la partecipazione al processo di validazione ai soli nodi approvati, agevolando la rapidità e un minor costo energetico, riducendo però la resistenza alle

modifiche, dipendendo quindi maggiormente dalla fiducia riposta nei gestori del consorzio o della rete privata.

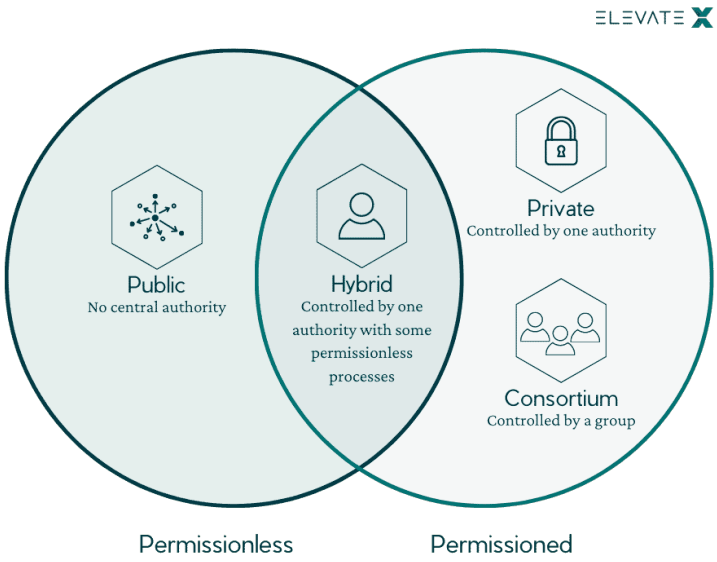


Figura 3.2: Suddivisione permissionless e permissioned
Fonte: ElevateX

Riconoscimento giuridico in Italia

Nel diritto italiano la definizione di tecnologie basate su registri distribuiti viene introdotta dall'articolo 8-ter del Decreto Legge 135/2018 [39, Art. 8-ter]. Viene finalmente riconosciuto che la memorizzazione di un file informatico su un sistema di blockchain produce effetti di validazione temporale elettronica, di cui all'articolo 41 del regolamento eIADS. Questo rende quindi l'ancoraggio su blockchain un mezzo di prova di data certa ed anteriorità certa [38, p. 68]. Fatto salvo che l'opera in sé ed i diritti d'autore su di essa rimangono disciplinati, come ampiamente approfondito nei primi capitoli, dalla Legge 633/1941.

Limiti: la privacy

Questa tecnologia oltre ai tanti benefici fin'ora presentati ha anche importanti limiti. Emergono infatti delle criticità quando l'ancoraggio contiene dei dati

personali, o metadati riconducibili a persone. In questi casi nascono quesiti su chi è il titolare del trattamento o su come poter esercitare i diritti dell'interessato, come quelli di rettifica o cancellazione, dal momento che il tutto si trova in un registro immutabile e potenzialmente distribuito anche fuori dall'Unione Europea. La dottrina propone diverse soluzioni [40, p. 149]:

- per le *blockchain permissioned*: modelli di contitolarità tra i vari membri del consorzio con annesso riparto di responsabilità, secondo quanto previsto dall'articolo 26 del GDPR;
- per le *blockchain permissionless*: divieti tecnici d'inserimento di particolari tipologie di dati o attuazione di tecniche di anonimizzazione.

Conclusioni e sviluppi

In sintesi la blockchain si configura come un registro immodificabile, distribuito e trasparente, capace di garantire tracciabilità e certezza di ogni operazione digitale. Tuttavia, la mera registrazione dei dati in blocchi concatenati non è sufficiente a gestire opportunamente i diritti connessi alle opere. L'esigenza quindi di automatizzare anche l'esecuzione di regole giuridiche, oltre che la prova porta alla nascita degli smart contract, naturale evoluzione delle blockchain che permettono la programmazione di rapporti giuridici auto-esecutivi con tutti i privilegi delle blockchain stesse.

3.1.2 Funzionamento tecnico e giuridico degli Smart Contracts

Nozione e struttura di uno Smart Contract

Nel 1994 il crittografo Nick Szabo per la prima volta introduce il termine *smart contract*, nato per definire un programma in grado di eseguire autonomamente clausole contrattuali prestabilite al verificarsi di specifiche condizioni. Solamente con l'arrivo della blockchain, e di piattaforme decentralizzate come *Ethereum*, tale concetto è divenuto applicabile nel concreto. Ethereum permette infatti la creazione di contratti auto-esecutivi che lavorano in modo decentralizzato e

trasparente [38, p. 20-22]. Uno smart contract sul fronte tecnico non è altro che un insieme di istruzioni informatiche scritte in un linguaggio specifico per questo tipo di software, come il linguaggio *Solidity*, e registrate sulla blockchain. Vengono dunque ereditate tutte le proprietà delle blockchain, il codice del contratto una volta pubblicato non può quindi essere più modificato e viene eseguito automaticamente dai nodi della rete. Le varie operazioni avvengono in modo deterministico ed immutabile, garantendo la verificabilità del risultato.

La struttura minima di uno smart contract prevede:

- *variabili di stato*: che in modo permanente memorizzano i dati del contratto;
- *funzioni*: che descrivono le azioni da eseguire;
- *eventi*: che registrano operazioni sulla blockchain;
- *indirizzo*: che identifica in modo univoco il contratto sulla rete.

Piattaforma Ethereum e il linguaggio Solidity

Ethereum rappresenta l'evoluzione di una già nota e famosa piattaforma decentralizzata, Bitcoin, introducendo però la possibilità di programmare logiche contrattuali anche più complesse. Ogni contratto viene eseguito in un ambiente distribuito, chiamato *Ethereum Virtual Machine* detto *EVM*, che processa le istruzioni in cambio di un pagamento di un costo empirico, chiamato *GAS*, che rappresenta sostanzialmente quanto costa alla rete eseguire un certo pezzo di codice, così da limitare abusi e spreco di risorse computazionali [38, p. 23].

Solidity è il linguaggio principale utilizzato per la creazione degli smart contract, soprattutto su Ethereum. Rientra tra i linguaggi ad alto livello, dunque vicini all'utente, con una sintassi simile al famosissimo JavaScript. Attraverso Solidity è possibile quindi, anche da chi abbia conoscenze di sviluppo base, descrivere e definire in modo chiaro e semplice le strutture dati e le funzioni che regolano la logica del contratto. Il codice, una volta scritto, viene compilato in un formato leggibile dalla Ethereum Virtual

Machine, per poi entrare in rete tramite una transazione e fare parte integrante della blockchain, ottenendo anche un indirizzo che identifica quindi univocamente il contratto.

```
contract SimplePayment {
    address payable owner;
    constructor() { owner = payable(msg.sender); }
    function pay() public payable {}
    function withdraw() public { owner.transfer(address(this).balance); }
}
```

Figura 3.3: Codice di esempio in Solidity

Nel frammento di codice si dimostra lo logica auto-esecutiva, in questo esempio facilmente leggibile, si nota come il trasferimento avviene automaticamente e senza possibilità di alterare le condizioni.

Riflessioni giuridiche

Sul fronte giuridico la questione riguarda la riconoscibilità degli smart contract come contratti ai sensi dell'articolo 1321 del codice civile, ossia come un accordo finalizzato a costituire e regolare rapporti giuridici patrimoniali. Lo smart contract può assumere un ruolo duplice:

- come *strumento di esecuzione automatica* di un contratto in precedenza già perfezionato;
- come *modalità di formazione del consenso* in cui direttamente nel codice informatico viene incorporata la volontà delle parti.

Nel contesto del diritto d'autore gli smart contract potrebbero essere impiegati più come nella seconda modalità, ad esempio, come strumenti di gestione automatizzata dei diritti. Un contratto scritto in Solidity potrebbe regolare in maniera automatica le licenze d'uso di un'opera digitale, regolando: le condizioni di accesso, la durata temporale, la suddivisione automatica dei compensi e l'invio di royalties all'autore ogni qual volta l'opera venga riprodotta.

Il legislatore italiano già riconosce tra l'altro la rilevanza di questa tecnologia, come già accennato, all'articolo 8-ter del D.L. 135/2018. La norma definisce questi programmi informatici capaci di vincolare automaticamente due o più parti, riconosce inoltre il valore probatorio alla validazione temporale, equiparandola alla marca temporale elettronica.

Conclusioni e sviluppi

Gli smart contract rappresentano un punto di incontro tra automazione tecnologica e autonomia giuridica, questi contratti che si "auto-eseguono" richiedono un equilibrio tra efficienza algoritmica e controllo umano. Piattaforme come Ethereum o linguaggi come Solidity forniscono ad oggi una buona infrastruttura per questa trasformazione, ma la loro integrazione nel sistema giuridico è ancora in corso. Proprio su questa base tecnologica si innesta la successiva evoluzione, quella del *Non-Fungible Token* (*NFT*) che sfruttano gli smart contract per gestire, rappresentare e scambiare opere digitali uniche, collegando in modo ancor più diretto, il diritto d'autore con il dominio tecnico della blockchain.

3.1.3 NFT e Crypto Art

Definizione e funzionamento tecnico

Gli *NFT*, acronimo di *Non-Fungible Token*, sono dei certificati digitali registrati su blockchain, rappresentano perciò un oggetto del tutto unico e non intercambiabile. Differentemente, ad esempio, dalle ormai famosissime cripto-valute, che sono fungibili e tra loro identiche, gli NFT godono di un'identità digitale esclusiva. Ognuno è infatti distinto da un suo identificatore e da vari metadati aggiuntivi utili a descriverne le caratteristiche, la provenienza o l'autore.

Il token è strutturato in modo tale da non contenere direttamente l'opera digitale, ma un link o un hash, generato da appositi algoritmi come SHA-256, che rimanda al file conservato fuori dalla catena, in un server esterno dedicato. Questo riesce a garantire la tracciabilità e verificabilità dell'opera e al contempo preservarne l'integrità [41, p. 25]. Anche se l'opera si trova fuori dalla blockchain

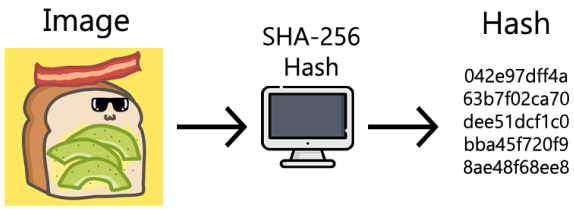


Figura 3.4: Generazione di un hash di un'opera digitale
Fonte: Medium

una sua eventuale modifica o variazione comporterebbe un aggiornamento del suo hash, rendendo quindi immediatamente individuabile l'alterazione.

Ogni transazione relativa al token viene registrata pubblicamente nella blockchain, andando a creare una sorta di catena di provenienza, che permette a chiunque di attestare la storia di proprietà dell'opera digitale [42, p. 7]. L'NFT ha dunque un grandissimo valore, derivato non solo dal file rappresentato, ma anche dal suo certificato di unicità che lo rende una sorta di titolo di proprietà digitale.

NFT e mercato dell'arte digitale

Famoso è il fenomeno della Crypto Art, che ha avuto vita grazie all'utilizzo degli NTF anche nel campo artistico, un'innovativa forma di produzione e circolazione artistica, in cui l'opera digitale e il suo certificato coincidono, nel registro blockchain. Questo fenomeno ha raggiunto un'ampia notorietà a livello mondiale, quando nel 2021 l'opera digitale *Everydays: The First 5000 Days* è stata venduta all'asta per circa 70 milioni di dollari, facendo entrare la blockchain nel mercato tradizionale dell'arte [41, p. 24].

Oggigiorno qualsiasi artista può facilmente mostrare o mercificare le loro opere digitali senza l'ausilio di intermediari, garantendo autenticità e controllo. Per farlo, chiunque, può avvalersi di piattaforme specializzate basate su blockchain, che funzionano come delle vere e proprie gallerie virtuali, le più famose sono: SuperRare, Foundation o OpenSea.

La digitalizzazione ha aumentato l'indipendenza dagli intermediari tradizionali e trasformato le piattaforme ed i social in spazi di scambio economico e visibilità

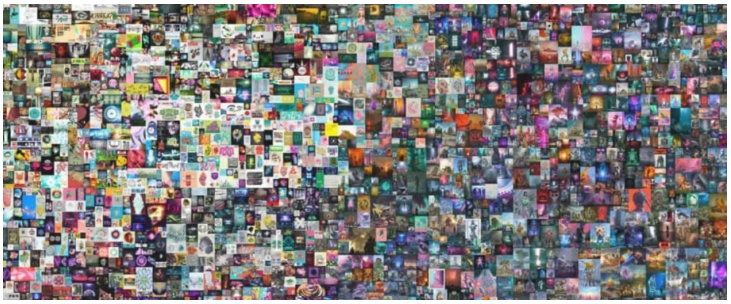


Figura 3.5: Opera *Everydays: The Last 5000 Days*
Fonte: Repubblica.it

[42, p. 1]. Tuttavia la facilità di creazione di questi token e l'assenza di una mediazione hanno favorito invece la crescita di fenomeni speculativi. In questo ambiente il valore dell'opera è dato più dalla rarità artificiale o dalla montatura nel mercato che dai classici criteri artistici. Attuale è il dibattito tra chi individua negli NFT una democratizzazione del mercato artistico e chi invece una mercificazione della creatività digitale.

Profili giuridici e diritto d'autore

L'avvento di questi token ho necessariamente portato ad una riflessione radicale sul diritto d'autore sulle categorie classiche di copia, opera e titolarità. La "tokenizzazione" di un opera cambia la concezione materiale della creatività ad una dimensione più informatica. La tutela non riguarda più l'oggetto fisico, come un quadro o una tela artistica, ma la rappresentazione digitale dell'opera, certificata dal token.

Il primo aspetto riguarda la differenza tra la proprietà del token e la titolarità dei diritti d'autore sull'opera associata. L'acquirente di un token NFT, salvo diversi patti, non diventa titolare dei diritti economici sull'opera associata, ma acquisisce solo la titolarità del token che si limita ad attestare l'autenticità dell'opera e non conferisce di certo il diritto a riprodurla o distribuirla. Sostanzialmente il token è la rappresentazione crittografica della copia dell'opera, non il suo diritto, agisce come certificato digitale, ma da solo non è sufficiente a trasferirne automaticamente i diritti patrimoniali. [42, p. 9]

Il secondo profilo rilevante riguarda la possibilità di utilizzare i token per disciplinare licenze d'uso e royalty automatiche [41, p. 29]. Gli autori possono indicare la percentuale di compenso spettante a ogni rivendita o quando revocare la licenza in caso di violazioni. Questo modello crea una forma di DRM decentralizzato, in cui la norma si auto-esegue senza necessità di intermediari.

In ultimo gli NFT ridefiniscono in parte le nozioni di originalità e creatività artistica, specialmente quando le opere sono generate o elaborate da intelligenze artificiali, l'autore umano si riduce a semplice curatore del processo creativo e non ne è più il protagonista.

Conclusioni

Gli NFT rappresentano a pieno il punto d'incontro tra mercato digitale, innovazione tecnologica e tutela giuridica. Il futuro del diritto si misurerà sulla capacità di integrare il linguaggio informatico, il codice, con quello giuridico. Gli NFT possono essere considerati il naturale proseguimento e sviluppo degli smart contract, automatizzando la fruizione e il possesso delle opere digitali in rete.

3.1.4 Caso: Juventus F.C. v. Blockeras s.r.l.

Contesto e fatti della controversia

Il caso della *Juventus F.C.* contro la *Blockeras s.r.l.* simboleggia il primo precedente giurisprudenziale italiano per quanto concerne gli NFT e segni distintivi, nonché uno dei primi nel contesto europeo a collegare la tutela dei marchi e dei diritti d'autore con la tecnologia della blockchain.

Era il 2022 quando la società Blockeras, molto attiva nel campo della crypto art e del fantasy football, pubblico una collezione di NFT player cards denominate "The Lega Serie A – Crypto Cards". Tra i vari token digitali che venivano offerti figuravano anche delle immagini riportanti l'ex calciatore Christian Vieri con indosso la divisa della Juventus ed, ovviamente, il logo del club sportivo, entrambi elementi distintivi di proprietà della società sportiva.

Fu proprio la Juventus F.C. a presentare ricorso al Tribunale di Roma andando a denunciare un uso illecito dei proprio marchi registrati e chiedendo quindi il blocco immediato della vendita online degli NFT incriminati. La società sportiva sosteneva che le immagine dei token riportavano segni distintivi noti del club, utilizzati tra l'altro a fini commerciali, violando quindi la normativa sui marchi e configurando un illecito concorrenziale [43, p. 30-31].

Analisi giuridica: marchi, diritto d'autore e nuove tecnologie

Con l'ordinanza del 20 luglio 2022 il Tribunale di Roma accolse le istanze presentate dalla Juventus, imponendo a Blockeras di ritirare dalla loro piattaforma digitale le card NFT contestate e di astenersi dall'utilizzo dei marchi distintivi del club [44]. Il tribunale ha applicato in modo estensivo i principi del diritto d'autore e dei marchi, riconoscendo comunque la novità della tecnologia blockchain, affermando che:

1. I non-fungible token non sono dei semplici file digitali ma prodotti in grado di distinguere beni e servizi, di conseguenza soggetti alla disciplina dei marchi;
2. L'utilizzo del logo della Juventus sulla maglia del giocatore nella card NFT costituisce un uso illecito del marchio, creando confusione nel pubblico riguardo l'origine e l'autorizzazione dei token;
3. L'impiego di questi segni distintivi integra una violazione anche nel diritto all'immagine e diritto morale d'autore, poche l'opera digitale riproduce contenuti coperti da tutela autoriale.

La decisione nel suo complessivo ha dunque ricordato che anche nel metaverso o nelle piattaforme blockchain sono in vigore le stesse regole di licenze, consenso e autorizzazione previste per le opere tradizionali. La semplice registrazione di un token sulla blockchain non attribuisce automaticamente alcun diritto di sfruttamento economico sull'opera sottostante senza il consenso del titolare originale [43, p. 37].

Implicazioni e riflessi nel diritto d'autore digitale

Il caso Juventus v. Blockeras ha un grande valore significativo per il sistema della proprietà intellettuale nell'era digitale. Questa controversia seppur nata in materia di marchi apre la strada a una nuova interpretazione del diritto d'autore applicati alla tokenizzazione delle opere. Viene inoltre evidenziato il crescente ruolo della responsabilità delle piattaforme, e degli autori dei token, nella corretta gestione dei diritti digitali. Questi soggetti dovrebbero inoltre adottare procedure di verifica e autorizzazione per evitare casi come questo di commercializzazione di contenuti protetti. La blockchain può sicuramente servire come strumento potente di prova e di trasparenza, ma non come "scudo" rispetto alle responsabilità legali, come i principi della proprietà intellettuale ai quali deve invece integrarsi.

Conclusioni

Concludendo, questa vicenda ha mostrato come ogni innovazione in ambito tecnologico porta sempre con se nuove sfide interpretative per il diritto. Se finora la blockchain e gli NFT hanno aperto la strada alla certificazione e alla tracciabilità delle opere digitali, l'evoluzione tecnologica ancor più recente dell'intelligenza artificiale generativa, pone ancor più interrogativi sul piano del diritto, e sul rapporto tra uomo, codice e algoritmo.

3.2 Intelligenza Artificiale e diritto

3.2.1 Fondamenti tecnici dell'IA e dei modelli generativi

L'intelligenza artificiale, abbreviata in *IA*, può essere intesa come un complesso di strumenti e metodi informatici che vogliono riprodurre e simulare quelle che sono le capacità cognitive proprie degli esseri umani, come il ragionamento, l'apprendimento, o il potere decisionale. Da una prospettiva tecnica invece l'IA si basa su modelli matematici che elaborano dati apprendendo schemi e correlazioni, capaci di aggiornare continuamente i propri parametri, basandosi soprattutto sulle esperienze precedenti. Questi modelli si differenziano in approcci, detti [45, p. 83-84]:

- *model-based*: dove il comportamento dell'IA è gestito da regole precedentemente ed esplicitamente programmate;
- *data-driven*: dove invece l'IA apprende in autonomia dai dati grazie a vari processi statistici e reti neurali.

L'evoluzione verso il machine learning e il deep learning

Risalgono addirittura agli anni Cinquanta le prime applicazioni dell'intelligenza artificiale, quando ancora si fondavano su sistemi esperti programmati con regole logiche rigide. Sono state poi la maggiore potenza computazionale e di calcolo e la disponibilità di importanti quantità di dati, definiti *big data*, che negli anni Duemila circa hanno consentito di affermare un nuovo paradigma: l'apprendimento automatico, definito *machine learning* [45, p. 45-47]. Non sono più necessarie istruzioni esplicite, grazie a questo approccio, che indichino al sistema come individuare le relazioni tra le variabili. Si sfruttano invece tecnologie come le *reti neurali* artificiali, che sono strutture ispirate al cervello umano. Queste reti neurali sono organizzate in livelli, i *neuroni artificiali*, che elaborano i dati in modo stratificato. Per produrre risultati in output sempre più accurati per ogni input si aumenta la profondità della rete incrementando gli strati intermedi, da qui il termine *deep learning*.

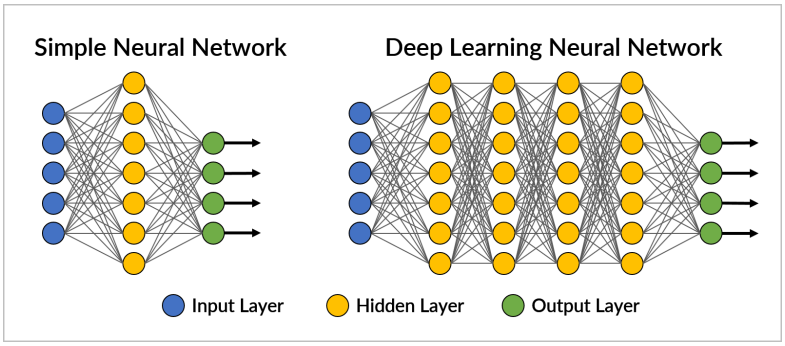


Figura 3.6: Livelli dei neuroni artificiali nelle reti neurali
Fonte: Ray Bernard Consulting Services

Tale processo di apprendimento si basa sull'uso di grandi schemi di dati di addestramento, detti appunto *traning data*. Queste banche dati sono la base

statistica su cui i modelli riconoscono poi schemi, relazioni ed associazioni [45, p. 48]. L'affidabilità e l'accuratezza dei risultati che otteniamo sono dunque fortemente influenzate dalla qualità, quantità e correttezza di tali dati. Ciò pone questioni rilevanti sul piano giuridico ed etico riguardo la tutela e la provenienza di questi contenuti. Questi schemi inoltre soffrono di una peculiare caratteristica, l'opacità intrinseca: persino i tecnici informatici che si occupano di addestrare i sistemi machine learning sono spesso in difficoltà nel ricavare una motivazione degli output forniti, non riuscendo a comprendere il percorso logico che porta questi algoritmi a determinati risultati.

Dall'IA tradizionale ai modelli generativi

Tra le evoluzioni del settore dell'IA la più significativa e di recente sviluppo è quella dell'intelligenza artificiale generativa, dall'inglese *Generative AI*. Possiamo definirla come "un tipo di intelligenza artificiale in grado di apprendere e imitare grandi quantità di dati per creare contenuti come testo, immagini, musica, video, codice e altro ancora, sulla base di input o di richieste". Anche tali modelli utilizzano le reti neurali profonde, precedentemente illustrate, capici quindi di riconoscere complessi schemi all'interno di vari dataset, si dividono però in due categorie [46, p. 3-4]:

- i modelli *unimodali*: in grado di produrre contenuti solo della stessa natura dell'input, esempio: testo → testo;
- i modelli *multimodali*: in grado di combinare più linguaggi, ad esempio: testo → immagine o audio → testo.

La generazione autonoma di contenuti è stata resa possibile grazie alle principali architetture, che sono [46, p. 5-8]:

1. le *GANs*, ancronimo di *Generative Adversarial Networks*: introdotte nel 2014 da Goodfellow, composte da ben due reti neurali di diverso tipo, una generativa ed una discriminativa, che reciprocamente si migliorano fino ad ottenere dei risultati indistinguibili da quelli umani;

2. le *VAE*, ancronimo di *Variational Autoencoders*: che riducono i dati in una rappresentazione semplificata per poi ricostruirli generando dei nuovi contenuti simili agli originali, come immagini o suoni;

3. i *Transformer*: architetture capaci di analizzare le relazioni tra parole o elementi di tipo testuale su sequenze lunghe, per poi generare output contestualizzati. Su queste architetture si basano modelli come GPT o DALL-E;

4. i *Diffusion Models*: in grado di apprendere ripulendo dei dati rumorosi, ricostruendo la versione originale. Specializzati nella creazione di immagini e video con altissimi livelli di realismo.

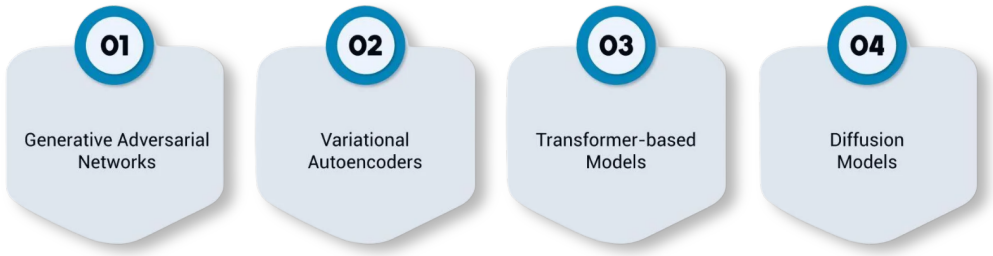


Figura 3.7: Tipologie di modelli di IA generativa
Fonte: Splore

Tutte queste architetture sopra elencate sono ad oggi impiegate in una grande varietà di campi: dalla generazione di musica e video, alla sintesi di immagini o alla elaborazione di dati scientifici.

Conclusioni

Riassumendo, i modelli generativi di intelligenza artificiale si basano su complicati processi di auto-apprendimento, alimentati da grandi quantità di dati e da reti neurali profonde, in grado di trovare schemi e produrre nuovi contenuti. Ciò offre enormi potenzialità, ma solleva questioni cruciali: il ruolo e la provenienza dei dataset usati in fase di addestramento, che possono includere contenuti coperti dai diritti d'autore, e la scarsa trasparenza dei meccanismi interni. L'uso dei dati e l'opacità algoritmica verranno infatti nei prossimi paragrafi approfonditi.

3.2.2 L'Artificial Intelligence Act: verso una regolazione europea dell'intelligenza artificiale

L'Unione Europea visti i recenti sviluppi e l'evoluzione dell'intelligenza artificiale ha deciso di voler intervenire con un quadro normativo, finalizzato a garantire uno sviluppo di queste tecnologie in linea con principi di affidabilità, sicurezza e rispetto dei diritti fondamentali. Il 21 aprile 2021 in Commissione Europea è stata presentata la proposta di legge dal titolo *Artificial Intelligence Act (AIA)*, che rappresenta il primo tentavo di una regolazione orizzontale dell'IA. [47, p. 38].

Un modello di regolazione basato sul rischio

L'AIA utilizza un approccio basato sul rischio, detto per l'appunto *risk-based*, ovvero classifica i sistemi di IA basandosi sul livello di rischio che essi comportano per la sicurezza, gli interessi pubblici ed i diritti fondamentali. Questo regolamento per la prima volta tenta di disciplinare in modo estensivo anche la progettazione e lo sviluppo dei sistemi IA, non limitandosi semplicemente alla protezione dei dati o alla responsabilità connesse. Per farlo la proposta prevede quattro livelli di rischio, che determinano diversi obblighi [48, p. 98-99]:

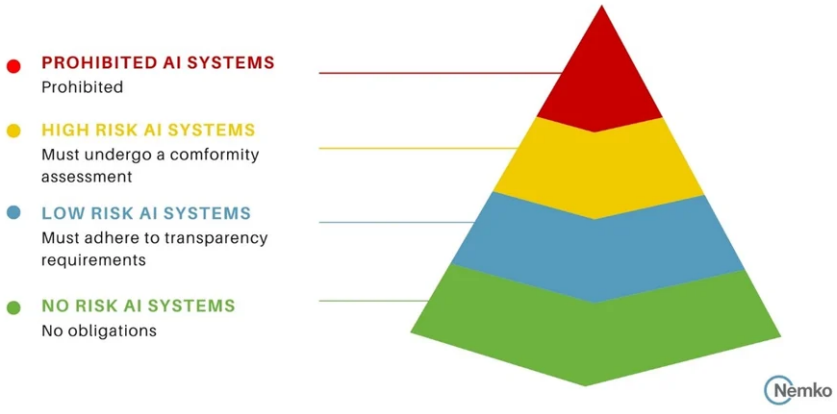


Figura 3.8: Livelli di rischio previsti dall'AI ACT
Fonte: Nemko

Tabella 3.1: Livelli di rischio previsti dall'Artificial Intelligence Act

Livello	**Descrizione**	**Esempi**	**Regime giuridico**
Rischio inaccettabile	Sistemi che minacciano gravemente i diritti fondamentali o la sicurezza.	Manipolazione della psiche, riconoscimento facciale.	Vietati.
Alto rischio	Sistemi che incidono su i diritti fondamentali, la sicurezza o dei processi decisionali.	IA in ambito giudiziario, sanitario, occupazionale o educativo.	Autorizzati ma solo con degli obblighi di trasparenza, conformità e supervisione umana.
Rischio limitato	Sistemi con effetti discriminatori o ingannevoli ma non gravi.	Chatbot, deepfake, assistenti virtuali.	Obbligo di trasparenza nei confronti dell'utente.
Rischio minimo o assente	Sistemi con impatti minimi sulla sicurezza e sui diritti.	Filtri contro lo spam, videogiochi, applicazioni ludico-ricreative.	Utilizzo libero, nessun obbligo specifico.

La logica implicita è quella di voler equilibrare l'innovazione e la tutela, cercando di evitare una regolamentazione troppo stringente, detta *over-regulation*, che soffocherebbe la ricerca e lo sviluppo, ma di evitare anche che sia troppo permissiva, *under-regulation*, che priverebbe delle adeguate protezioni i cittadini europei.

Valutazione dell'impatto sui diritti fondamentali e problematiche di implementazione

Uno degli aspetti principali dell'IA Act è l'istituzione della valutazione di impatto sui diritti fondamentali, dall'inglese *Fundamental Rights Impact Assessment (FRIA)*, prevista obbligatoriamente nei sistemi ad alto rischio. Questa valutazione

è sicuramente una novità rilevante ma anche un nodo critico in quanto la normativa rimane vaga nell'individuare precisamente che cosa possa costituire un impatto significativo sui diritti, lasciando dei margini di incertezza [48, p. 112].

Il regolamento soffre di altre problematiche di implementazione:

- *Predeterminazione dei livelli di rischio*: vengono fissati in modo eccessivamente rigido le quattro categorie di rischio, in quanto non si tiene conto della rapidità con cui queste tecnologie evolvono e cambiano nel tempo [48, par. 4.1];

- *Genericità del giudizio di significatività del rischio*: si lasciano margini troppo ampi di interpretazione su quanto sia significativo un rischio per i diritti fondamentali, potrebbe portare ad applicazioni non uniformi tra gli Stati membri ed incertezza per sviluppatori ed utenti [48, par. 4.2];

- *Indeterminatezza della valutazione d'impatto sui diritti fondamentali*: la FRIA è sicuramente essenziale per prevenire le violazione dei diritti umani, ma non vengono specificati in modo dettagliato i criteri e le metodologie da adottare per gestire tale analisi. Si corre il rischio che rimanga un puro adempimento formale e privo di reale valore [48, par. 4.3].

Tutte queste criticità dimostrano come sia difficile conciliare un sistema normativo statico con l'evoluzione rapida dell'intelligenza artificiale, che utilizza algoritmi con possibili mutamenti funzionali durante il ciclo di vita del sistema, di cui l'analisi del rischio ex ante non tiene conto.

Conclusioni

In sintesi l'IA Act rappresenta dunque un ambizioso tentativo di realizzare un quadro normativo europeo in grado di orientare l'innovazione tecnologica rimanendo dentro confini etici e giuridici precisi. Presenta però criticità importanti legate alla valutazione preventiva dei rischi e all'effettiva protezione dei diritti fondamentali. Proprio questa tensione tra controllo e imprevidibilità che evidenzia un nodo delicato: la trasparenza nei processi algoritmici che guidano i sistemi IA. Comprendere chiaramente e rendere spiegabili le decisioni della macchina è un passaggio sicuramente difficile che ha implicazioni anche sul piano giuridico,

proprio per questo il tema è infatti al centro della successiva riflessione sull'opacità algoritmica e le conseguenza giuridiche.

3.2.3 Opacità algoritmica e profili giuridici della trasparenza

I modelli di IA, in particolar modo quelli generativi, introducono nel panorama giuridico una questione importante: la crescente opacità dei processi decisionali. L'*opacità algoritmica* "si riferisce alla difficoltà di comprendere come vengano prese le decisioni all'interno di algoritmi complessi, rendendo poco trasparenti i processi decisionali" [49]. Questo fenomeno è spesso frequente nei sistemi IA che durante le fasi di elaborazione dati effettuano scelte dalla logica difficilmente comprensibile. Sono dunque noti l'input e l'output, ma non il percorso logico che li collega, in quanto il modello apprende autonomamente gli schemi e le correlazioni che non vengono esplicitamente pre-programmate.

GDPR e processi decisionali automatizzati

Il principio di trasparenza nel diritto europeo rappresenta una colonna importante nel trattamento dei dati personali. Già nel GDPR all'articolo 5, comma 1, lettera a, viene imposto che i dati vengano trattati in "*modo lecito, corretto e trasparente nei confronti dell'interessato*". Ancor più rilevante per i sistemi automatizzati, come l'IA, è l'articolo 22 che sancisce il "*diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*".

Il legislatore europeo ha quindi già riconosciuto che l'automazione delle decisione tramite algoritmi informatici non può far venire a meno le possibilità di controllo e contestazione all'utente finale. È anche vero però che nei sistemi deep learning spesso i nessi logici interni tra i livelli della rete neurale artificiale risultano sconosciuti persino ai progettisti, ed è dunque molto difficile, se non impossibile, attuare tali normative.

L'AI Act e la trasparenza

Nella nuova proposta dell'AIA si cerca quindi di colmare questa lacuna, introducendo nuovi obblighi di trasparenze e governace, sopratutto per i sistemi IA ad alto rischio, che mettono in evidenza i seguenti aspetti fondamentali [49, par. 4]:

1. *Trasparenza by design*: si impone che i sistemi IA vengano progettati dell'origine per garantire la tracciabilità delle decisioni e la possibilità di successivi audit;

2. *Comprensibilità e spiegabilità*: si richiede che gli output possano essere interpretati da personale umano qualificato, deve essere possibile ricostruire i criteri decisionali adottarti e le regole di funzionamento;

3. *Accessibilità delle informazioni*: gli sviluppatori devono garantire l'accesso alle autorità, agli utenti professionali ed al pubblico in specifici casi riguardo tutte le informazioni rilevanti sul funzionamento del modello IA;

4. *Sorveglianza umana*: si impone che sia l'uomo a mantenere un potere effettivo di controllo e interruzione del sistema, tale principio viene definito *human oversight*;

5. *Esattezza dei dati*: i dataset utilizzati nelle fasi di addestramento devono essere aggiornati e accurati, poiché questi dati determinano la qualità delle decisioni algoritmiche;

6. *Documentazione*: i fornitori di questi sistemi IA ai controlli dell'autorità devono poter fornire la documentazione tecnica completa, che consenta la verifica della riproducibilità e della conformità;

7. *Mitigazione del rischio di bias e discriminazioni*: eventuali effetti discriminatori devono essere obbligatoriamente identificati, valutati e ridotto al minimo il loro rischio.

Questi principi traducono la trasparenza in una responsabilità che va dalla progettazione alla supervisione, fino al controllo di autorità preposte. Tuttavia

tale trasparenza rimane abbastanza formale, molto orientata alla rendicontazione più che ad una vera comprensione dei processi. L'AI Act prova dunque a rendere tracciabile il funzionamento di questi sistemi ma non necessariamente riesce a renderlo comprensibile.

3.2.4 Caso: l'avvocato di Firenze e le sentenze inventate da ChatGPT

Il Tribunale Ordinario di Firenze, sezione imprese, il 14 marzo 2025 ha emesso una decisione che è entrata nella storia italiana come il primo provvedimento in cui la giustizia si confronta con l'intelligenza artificiale generativa e gli errori da lei commessi. Questi errori sono stati individuati nelle memorie difensive di una delle due parti in un processo per violazione del diritto d'autore e del marchio relativo alla vendita di t-shirt, trattasi in particolare di precedenti giurisprudenziali inesistenti generati da ChatGPT senza verifica dell'autenticità. L'IA aveva infatti restituito citazioni verosimili, con persino il numero di registro, apparentemente giuste ma in realtà totalmente inventate, che erano state ignaramente inserite nell'atto, determinando così la prima "allucinazione giurisprudenziale" [50].

Il caso e la decisione

Il Tribunale avendo scoperto l'anomalia presente negli atti, ha chiesto quindi alle parti coinvolte di chiarire l'origine di suddetti riferimenti giurisprudenziali inesatti. La difesa ha ammesso l'errore dovuto non ad un intento doloso ma dichiarando che erano state generate da un modello di Intelligenza Artificiale. In questo caso il Giudice ha riconosciuto la buona fede escludendo l'applicazione sulla responsabilità aggravata, art. 96 c.p.c, mancando gli elementi di malafede [51, p. 11].

È stato però ribadito il disvalore dall'omessa verifica degli output forniti dell'IA, sottolineando la necessità di mantenere un controllo umano costante ed effettivo. La decisione del giudice non ha fini sanzionatori ma sicuramente ci mette in guardia: l'IA è sicuramente un supporto ma solo se accompagnata da una consapevolezza, verifica delle fonti e conoscenza dei suoi limiti tecnici.

Un riflesso diretto dei principi di trasparenza e responsabilità

Dal punto di vista tecnico si evidenzia come in questi modelli non sia possibile ricostruire i vari processi logici interni che portano alla generazione degli output, ciò porta a risultati che posano apparire coerenti, come le sentenze citate, ma che possano invece rivelarsi concettualmente o fattualmente errati.

Sul piano giuridico questa vicenda si collega ai principi di trasparenza e spiegabilità che la proposta di AI Act vuole introdurre nel quadro normativo europeo. Secondo la proposta infatti, i sistemi di IA dovrebbero essere sviluppati ed utilizzati in modo tale da consentire la comprensione dei processi decisionali e sia garantita la tracciabilità delle informazioni che portano alla generazione degli output. Inoltre il principio di human oversight prevederebbe la presenza di un controllo umano effettivo in modo da prevenire abusi o errori. In casi come questo l'applicazione di un regolamento come l'AI Act ed i suoi principi avrebbe sicuramente portato ad uno sviluppo più positivo della vicenda.

L'intelligenza artificiale può essere un valido strumento al servizio della giustizia e dei suoi operatori - in termini di efficacia, efficienza e riduzione di costi e tempi - ma, come dimostrano i casi citati, occorre adeguata formazione e sperimentazione, per acquisire consapevolezza dei rischi [50].

Conclusioni

Il caso fiorentino ci mostra in modo abbastanza emblematico come l'IA, se adoperata senza un'adeguata comprensione dei limiti, introduca errori difficilmente riconoscibili. Questo strumento potenzialmente utile, utilizzato in assenza di trasparenze e controllo, lo ha trasformato in un fattore distorsione cognitiva e procedurale di distorsione d procedurale e cognitiva. Non è solo l'errore tecnico a destare preoccupazione, ma anche e soprattutto la cieca fiducia automatica in un sistema che genera risultati non spiegabili e non verificabili.

Bibliografia

[1] Giulio Mazzolini. Privilegi, censure e diritto d'autore. dai privilegi degli stampatori nel '500 al diritto d'autore passando attraverso la censura ecclesiastica. In *Diritto d'autore, copyright e copyleft nell'audiovisivo. Norme e posizioni a confronto*, pages 33–40. Annali AAMOD, 2010.

[2] Simone Aliprandi. Quadro sinottico della materia. In *Diritto d'autore, copyright e copyleft nell'audiovisivo. Norme e posizioni a confronto*, pages 27–32. Annali AAMOD, 2010.

[3] United States Code. 17 u.s.c. § 201 — ownership of copyright. `https://www.law.cornell.edu/uscode/text/17/201`, 1976. Consultato il 23 settembre 2025.

[4] Digital Cultural Heritage ICOM ITALIA. Faq diritto d'autore, copyright e licenze aperte per la cultura nel web, 2021.

[5] Parlamento europeo e Consiglio dell'Unione Europea. Direttiva 2006/116/ce del parlamento europeo e del consiglio del 12 dicembre 2006 sulla durata di protezione del diritto d'autore e di alcuni diritti connessi. `https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:32006L0116`, 2006. Consultato il 23 settembre 2025.

[6] Giovanni Spedicato. *Il diritto d'autore in ambito universitario*. Alma Mater Studiorum, Università di Bologna, 2011.

[7] Simone Aliprandi. *Il diritto d'autore nell'era digitale. Una ricerca empirica su comportamenti, percezione sociale e livello di consapevolezza tra gli utenti della rete*. PhD thesis, Università di Milano-Bicocca, 2012.

[8] Pamela Samuelson. Digital media and the law. *Communications of the ACM*, 34(10):23–28, October 1991. doi: 10.1145/125223.125289. URL https://dl.acm.org/doi/pdf/10.1145/125223.125289. Consultato il 23 settembre 2025.

[9] Susanna Vezzadini. Realtà virtuale e nuove forme di vittimizzazione: quale spazio per il riconoscimento? In Antonio Pitasi, editor, *Webcrimes. Normalità, devianze e reati nel cyberspace*, pages 165–170. Guerini Studio, Milano, 2007. URL https://hdl.handle.net/11585/42035.

[10] Giulia Petri. The public domain vs. the museum. *Journal of Conservation and Museum Studies*, 12(2):1–10, 2014. doi: 10.5334/jcms.1021217. URL https://jcms-journal.com/articles/10.5334/jcms.1021217. Consultato il 24 settembre 2025.

[11] Giulio Libero Mangieri. La digitalizzazione del patrimonio culturale: opportunità e criticità, 2020. URL https://tesi.luiss.it/42490/1/160623_LIBERO%20MANGIERI_GIULIO.pdf?utm_source=chatgpt.com. Consultato il 25 settembre 2025.

[12] Parlamento europeo e Consiglio dell'Unione Europea. Direttiva (ue) 2019/790 del parlamento europeo e del consiglio del 17 aprile 2019 sul diritto d'autore e sui diritti connessi nel mercato unico digitale. https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32019L0790, 2019. Consultato il 24 settembre 2025.

[13] Mirco Modolo. Il diritto d'autore in archivio: concetti, problemi e prospettive alla luce della direttiva (ue) 2019/790. In *Le Muse in archivio. Itinerari nelle carte d'arte e d'artista*. ANAI, Roma, 2023.

[14] Iryna Solodovnik. *Repository Istituzionali Open Access e strategie Linked Open Data. Per una migliore comunicazione dei prodotti della ricerca scientifica*. Firenze University Press, Firenze, 2015. ISBN 978-88-6655-928-3. URL http://digital.casalini.it/9788866559283.

[15] Deborah De Angelis. Creative commons: un modello di semplificazione? In Barbara Pasa and Gianni Sinni, editors, *Transparency by Design. Incontro*

interdisciplinare sul principio di trasparenza dei dati personali, pages 118–129. Bembo Edizioni, Venezia, 2022. URL https://bemboedizioni.it/public/libri/bembooe_V4.pdf#page=119.

[16] Alfredo Vettorato. Profili giuridici delle licenze open source. Tesi di laurea magistrale, Alma Mater Studiorum – Università di Bologna, Bologna, 2011. URL https://amslaurea.unibo.it/id/eprint/2811. Corso di Laurea Magistrale in Scienze di Internet. Relatore: Prof.ssa Giusella Dolores Finocchiaro.

[17] Barbara Pasa and Gianni Sinni. Note introduttive: cronaca della giornata di studi. In Barbara Pasa and Gianni Sinni, editors, *Transparency by Design. Incontro interdisciplinare sul principio di trasparenza dei dati personali*, pages 10–25. Bembo Edizioni, Venezia, 2022. URL https://bemboedizioni.it/public/libri/bembooe_V4.pdf#page=10.

[18] Carlo Piana. *Open Source, Software Libero e altre libertà. Un'introduzione alle libertà digitali*. Ledizioni, Milano, 2017. ISBN 978-88-6705-766-5. URL https://www.vimelug.org/wp-content/uploads/2022/02/opensource.pdf. Prefazione di Roberto Di Cosmo, postfazione di Simone Aliprandi. Disponibile in Open Access con licenza CC BY 4.0.

[19] Direttiva 2009/24/ce del parlamento europeo e del consiglio, del 23 aprile 2009, relativa alla tutela giuridica dei programmi per elaboratore. Gazzetta ufficiale dell'Unione europea, L 111/16, 5 maggio 2009, 2009. URL https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32009L0024.

[20] Filippo Ricca e Paolo Tonella. Reverse engineering di sistemi software. *Mondo Digitale*, (3):52–63, 2006. URL https://archivio-mondodigitale.aicanet.net/Rivista/06_numero_4/Ricca_p._52-63_.pdf.

[21] Lorenzo Orlando and Giulia Capaldo. Osservatorio giuridico sulla innovazione digitale. In *Osservatorio Giuridico sulla Innovazione Digitale*, pages 137–152. Sapienza Università Editrice, 2022. URL https://www.editricesapienza.it/sites/default/files/6207_Annuario_

2022_Osservatorio_Giuridico_Innovazione_Digitale_interior.pdf. Accesso in data 4 ottobre 2025.

[22] Legge 22 aprile 1941, n. 633 – protezione del diritto d'autore e di altri diritti connessi al suo esercizio. Gazzetta Ufficiale della Repubblica Italiana, n. 166 del 16 luglio 1941, 1941. URL https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1941-04-22;633!vig=.

[23] Sas institute inc. v. world programming ltd., 2012. URL https://curia.europa.eu/juris/document/document.jsf?text=&docid=122362&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=163357. Causa C-406/10, sentenza del 2 maggio 2012, Corte di Giustizia dell'Unione Europea.

[24] Redazione Altalex. La tutela del software dopo il caso sas institute, 2013. URL https://www.altalex.com/documents/news/2013/02/27/la-tutela-del-software-dopo-il-caso-sas-institute. Accesso in data 06 Ottobre 2025.

[25] Top system sa v. belgian state, 2021. URL https://eur-lex.europa.eu/legal-content/it/TXT/?uri=CELEX:62020CJ0013. Causa C-13/20, sentenza del 6 ottobre 2021, Corte di Giustizia dell'Unione Europea.

[26] Emanuele Gruppioni. Strumenti e protocolli per il controllo dello streaming, 2004. URL https://www.lia.deis.unibo.it/Staff/LucaFoschini/MUM/pdfDocs/MUM/egruppioni.pdf. Relatore: Prof. Antonio Corradi; correlatore: Ing. Luca Foschini.

[27] Direttiva 2001/29/ce del parlamento europeo e del consiglio del 22 maggio 2001 sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione. Gazzetta ufficiale delle Comunità europee, L 167, 22 giugno 2001, p. 10–19, 2001. URL https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32001L0029. Conosciuta come Direttiva InfoSoc.

[28] Giuseppe Cassano and Bruno Tassone, editors. *Diritto industriale e diritto d'autore nell'era digitale*. Giuffrè Francis Lefebvre, Milano,

2022. ISBN 9788828839248. URL https://www.giuffre.it/catalogo/diritto-industriale-e-diritto-d-autore-nell-era-digitale-9788828839248. Prefazione di Cesare Galli; Introduzione di Vincenzo Franceschelli.

[29] Enciclopedia della Scienza e della Tecnica. Ugc (user generated contents). Istituto della Enciclopedia Italiana Treccani, 2013. URL https://www.treccani.it/enciclopedia/ugc_(Enciclopedia-della-Scienza-e-della-Tecnica)/. Consultata il 10/10/2025.

[30] Giovanni D'Ippolito. L'esigenza di un nuovo bilanciamento per il diritto d'autore: gli user generated content e l'ipotesi di un'eccezione per le opere creative e trasformative. *Ciberspazio e Diritto*, 18(59):530–569, 2017. URL https://www.academia.edu/42833033/L_esigenza_di_un_nuovo_bilanciamento_per_il_diritto_d_autore_gli_user_generated_content_e_l_ipotesi_di_un_eccezione_per_le_opere_creative_e_trasformative.

[31] Direttiva 2000/31/ce del parlamento europeo e del consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (direttiva sul commercio elettronico). Gazzetta ufficiale delle Comunità europee L 178 del 17 luglio 2000, p. 1–16, 2000. URL https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32000L0031.

[32] Roberto Caso. *Il commercio delle informazioni digitali tra contratto e diritto d'autore. Digital Rights Management*. CEDAM, Padova, 2004. ISBN 88-13-25253-6. Ristampa digitale a cura dell'Università di Trento, 2006. Licenza Creative Commons Attribuzione-NonCommerciale-NoOpereDerivate 2.0 Italy.

[33] Amir Rafi, Carlton Shepherd, and Konstantinos Markantonakis. A first look at digital rights management systems for secure mobile content delivery. *arXiv preprint*, 2023. URL https://arxiv.org/abs/2308.00437.

[34] Roberto Caso, editor. *Digital Rights Management: Problemi teorici e prospettive applicative*. Università degli Studi di Trento, Trento, 2008. ISBN 978-88-8443-220-9. Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 21 e 22 marzo 2007. Pubblicato con licenza Creative Commons Attribuzione-NonCommerciale-NonOpereDerivate 2.5 Italia.

[35] Daniele Giardino. Digital watermarking. Tesina, Università degli Studi di Salerno, 2009. Corso di Sicurezza su Reti 2; Docente: Prof. Alfredo De Santis; Anno Accademico 2008/2009.

[36] Funzionamento di content id. URL `https://support.google.com/youtube/answer/2797370?hl=it`. ccesso in data 18 Ottobre 2025.

[37] Davide Bellemo. Studio della tecnologia blockchain e sue possibili applicazioni in ambito sanitario, 2018. Tesi di Laurea in Ingegneria Informatica.

[38] Simone Brina. Blockchain e smart contract: definizioni, funzionamento, profili giuridici ed applicativi, 2022. Tesi di Laurea in Informatica Giuridica.

[39] Decreto-legge 14 dicembre 2018, n. 135. Gazzetta Ufficiale della Repubblica Italiana n. 290 del 14 dicembre 2018, 2018. URL `https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2018-12-14;135!vig=`. Convertito, con modificazioni, dalla Legge 11 febbraio 2019, n. 12.

[40] Maria Cristina Galluccio. La blockchain e la tutela dei dati personali, 2020. Tesi di Laurea in Giurisprudenza.

[41] Antonello Campo. Blockchain, nft e crypto art: Stato dell'arte di una nuova tecnologia, approccio e sviluppi, 2021. URL `https://webthesis.biblio.polito.it/`. Relatore: Prof. Maurizio D'Addona.

[42] Arianna Maceratini. Il digitale nell'attività creativa, tra diritto d'autore e nft. *European Public & Social Innovation Review*, 10(1):1–13, 2025. doi: 10.31637/epsir-2025-1950. URL `https://u-pad.unimc.it/handle/11393/351210`. Articolo di ricerca, Università di Macerata, ISSN 2529-9824. Licenza CC BY-NC-ND 4.0.

[43] Stella Ruberti and Sofia Casagrande. Il caso juventus v. blockeras – un'inibitoria di riferimento nel panorama europeo. *Olympia Lex Review*, 3 (2):29–39, 2023. URL https://www.olympialex.com/olympialex_review/pdf/03_2022/O_Rev_03-2022_02_Ruberti-Casagrande.pdf.

[44] Tribunale di Roma, Sezione Imprese. Ordinanza 20 luglio 2022 (rg n. 32072/2022) – juventus f.c. v. blockeras s.r.l. PDF documento ufficiale, 2022. URL https://www.ga-p.com/wp-content/uploads/2023/01/Rome-Court-NFTs.pdf. Diciassettesima Sezione, provvedimento inibitorio relativo a NFT e marchi sportivi.

[45] Luca Rinaldi. *L'intelligenza artificiale come nuova frontiera dei diritti fondamentali*. Tesi di dottorato in studi giuridici comparati ed europei, Università degli Studi di Trento, Trento, 2023. URL https://iris.unitn.it/handle/11572/372247. Relatori: Prof. Carlo Casonato, Dott. Paolo Traverso.

[46] Silvia Sabau. Intelligenza artificiale generativa e professioni legali: Applicazioni, prospettive e implicazioni etiche, 2023. URL https://thesis.unipd.it/handle/20.500.12608/59539. Relatrice: Prof.ssa Claudia Sandei.

[47] G. R. Marseglia. Ai act: Impatti e proposte. opportunità e rischi dell'over- e under-regulation. *i-Lex. Scienze Giuridiche, Scienze Cognitive e Intelligenza Artificiale*, 14(2), 2021. ISSN 1825-1927. URL https://www.i-lex.it/articles/Volume14/Fascicolo2RegulationOfAI/Marseglia_AI_Act_Impatti_e_proposte.pdf.

[48] Claudio Novelli. L'artificial intelligence act europeo: alcune questioni di implementazione. *Federalismi.it*, (2):94–113, 2024. ISSN 1826-3534. URL https://philarchive.org/archive/NOVLIA.

[49] Maria Lilia La Porta e Gaia Leoncini Luca Tufarelli. Ai act e gdpr, tra opacità algoritmica e principio di trasparenza. *Diritto Bancario – Approfondimenti, Governance e Controlli*, ottobre 2024. URL https://www.dirittobancario.it/art/

ai-act-e-gdpr-tra-opacita-algoritmica-e-principio-di-trasparenza/. Accesso in data 29 ottobre 2025.

[50] Fabrizio Testa. Le prime allucinazioni giurisprudenziali dell'ia: il caso chatgpt al tribunale di firenze. aprile 2025. URL https://www.opendotcom.it/pct-processo-civile-telematico/blog/allucinazioni-giurisprudenziali-ia-chatgpt-tribunale-firenze/18874. Accesso in data 30 ottobre 2025.

[51] Tribunale di Firenze, Sezione Imprese. Ordinanza del tribunale di firenze, sezione imprese, 14 marzo 2025. In Banca Dati del Merito - Ministero della Giustizia, marzo 2025. URL https://www.opendotcom.it/aspx/download.aspx?file=processo-civile-telematico/item-18874-ordinanza_tribunale_di_firenze_14_03_2025_chatgpt.pdf. Primo provvedimento giudiziario italiano sul fenomeno delle "allucinazioni giurisprudenziali" generate da ChatGPT.

[52] Andrea Miccichè. La normativa sugli audiovisivi dal secondo dopoguerra ad oggi. In *Diritto d'autore, copyright e copyleft nell'audiovisivo. Norme e posizioni a confronto*, page 107. Annali AAMOD, 2010.

[53] Lorenzo Casalini. Accesso e digitalizzazione nella direttiva copyright. *Persona e Mercato*, 2021(2):190–191, 2021. doi: 10.13132/1827-4357/189. URL https://www.rivisteweb.it/doi/10.13132/1827-4357/189.

[54] Sentenza della corte di giustizia dell'unione europea (quinta sezione) 16 luglio 2009, causa c-5/08, *Infopaq International A/S v. Danske Dagblades Forening*, 2009. URL https://curia.europa.eu/juris/document/document.jsf?docid=72482&doclang=IT.

[55] Google LLC. Content id su youtube, 2025. URL https://support.google.com/youtube/answer/2797370?hl=it. Consultata il 10/10/2025.

[56] Alessandro Stocco. Digital right management (drm). Tesi di laurea magistrale, Corso di Laurea magistrale in Informatica, 2014. Relatore: Ch. Prof. Riccardo Focardi. Anno Accademico 2013/2014.

[57] Anna Veronesi. Attacchi e contrattacchi al watermarking astratto. Tesi di laurea, Università degli Studi di Verona, Facoltà di Scienze Matematiche, Fisiche e Naturali, Corso di Laurea in Informatica, 2006. Relatore: Prof. Roberto Giacobazzi; Correlatore: Dott.ssa Mila Dalla Preda; Anno Accademico 2005/2006.