GIURISPRUDENZA PENALE

La responsabilità dell'Internet Service Provider per i reati in materia di diritto d'autore.

di ***Davide Costa***

Sommario. 1. Premessa e scopo dell'elaborato – **2.** Le diverse qualificazioni dell'Internet Provider nell'ordinamento in relazione all'attività svolta online. I servizi di mere conduit, caching e hosting – **3.** Il regime di responsabilità dell'ISP nel panorama legislativo nazionale e comunitario – **3.1.** Le prospettive in tema di responsabilità degli ISP in materia di diritto d'autore nella legislazione comunitaria e nazionale: la Direttiva UE 790/2019, il D.Lgs. 177/2021 e il Digital Service Act – **4.** La responsabilità penale dell'Internet Provider: i criteri di responsabilizzazione dell'ISP per i reati contro la proprietà intellettuale commessi dagli utenti – **4.1.** L'ISP come concorrente attivo dei reati commessi dagli utenti della rete: i casi paradigmatici e gli indirizzi dottrinali – **4.2.** Segue: Gli interventi giurisprudenziali in merito alla responsabilità concorsuale dell'hosting provider "attivo" per i delitti contro il diritto d'autore nella società dell'informazione – **4.3.** L'ISP "controllore": il concorso per omissione e la posizione di garanzia dell'Internet Provider – **4.4.** Segue: Le linee guida dettate dalla sentenza "Google c. Vividown" – **4.5.** Actual knowledge ed elemento soggettivo nell'accertamento della responsabilità penale dell'Internet Provider – **4.6.** Le conseguenze penalmente rilevanti dell'inerzia dell'ISP dopo la commissione del reato – **4.7.** La responsabilità amministrativa ex D.Lgs. 231/2001 dell'Internet Provider – **5.** Conclusioni: lo stato dell'arte e prospettive future.

1. Premessa e scopo dell'elaborato

Lo sviluppo delle tecnologie dell'informazione ha determinato, a partire dalla seconda metà del secolo scorso, un profondo impatto sulle forme ed i modi di essere dei rapporti sociali, economici, politici e culturali nell'ambito della società globalizzata.

Ed invero, la rivoluzione "cibernetica" costituisce un fenomeno che senza soluzione di continuità investe ogni sfera della vita e degli interessi dei singoli e della collettività, rendendo accessibile l'informazione e consentendo lo scambio di conoscenza potenzialmente a chiunque, a qualsiasi distanza, in qualsiasi luogo e in qualsiasi momento.

Come autorevolmente evidenziato dalla letteratura[1], inoltre, le tecnologie dell'informazione non si limitano a fornire agli individui un accesso potenzialmente sconfinato all'informazione e alle elaborazioni di cui gli stessi hanno bisogno nella vita privata e professionale, ma vanno altresì a sostituire le tradizionali modalità di interazione sociale.
Staccatosi dalla sua dimensione fisica e materiale, infatti, grazie alla semplice disponibilità di una connessione alla rete e di un dispositivo di accesso alla stessa il singolo diventa protagonista attivo nella creazione di nuovi contenuti, nella scelta e nell'utilizzo di quelli messi a sua disposizione, nella partecipazione ad attività individuali e collettive di ogni tipo.
Senonché, lo sviluppo delle tecnologie dell'informazione e la trasposizione delle attività e dei rapporti umani dal mondo fisico ad una nuova dimensione dematerializzata e virtuale hanno rappresentato, fin dall'origine, un terreno fertilissimo per il proliferare di comportamenti criminosi lesivi di diritti ed interessi meritevoli di protezione giuridica che, proprio a causa del loro manifestarsi online, appaiono più facilmente aggredibili da condotte poste in essere tramite lo strumento informatico.[2]
Fattori quali l'istantaneità delle comunicazioni e delle attività telematiche, la loro delocalizzazione e dematerializzazione, così come la possibilità per gli autori di nascondersi dietro al più completo anonimato costituiscono indubbiamente un incentivo alla perpetrazione tanto di reati tradizionali posti in essere mediante apparecchi digitali (c.d. reati informatici in senso ampio[3]) quanto di nuove fattispecie la cui realizzazione si estrinseca necessariamente

[1] V. SARTOR G., *L'informatica giuridica e le tecnologie dell'informazione. Corso d'informatica giuridica,* III edizione, 2016, Giappichelli Editore, Torino e relativa bibliografia.

[2] Sul punto emblematica è la definizione di cyberspazio quale "*wild west della globalizzazione del crimine",* contenuta in FLOR R., *La giustizia penale della rete? Tutela della riservatezza versus interesse all'accertamento e alla prevenzione dei reati nella recente giurisprudenza della Corte di Giustizia dell'Unione Europea*, in FLOR R., FALCINELLI D., MARCOLINI S., *La giustizia penale nella "rete". Le nuove sfide della società dell'informazione nell'epoca di internet,* I Convegno Nazionale del Laboratorio Permanente di Diritto Penale, 19 settembre 2014, Perugia, 153 ss.

[3] Si pensi, tra le molteplici ipotesi di reato realizzabili tanto off-line quanto in rete che costantemente confluiscono nei registri delle Procure della Repubblica, alla diffamazione, alle sostituzioni di persona e agli atti persecutori posti in essere a mezzo *social network,* alle estorsioni realizzate con strumenti telematici, alla diffusione di contenuti pedopornografici, alla vendita online di prodotti recanti marchi contraffatti e alle plurime ipotesi di truffe realizzate su piattaforme di vendita virtuali.

tramite e/o nei confronti del *device* connesso in rete (c.d. reati informatici "propri" o in senso stretto).[4]

La necessità di rispondere alle istanze di tutela nei confronti di quelle condotte penalmente rilevanti che, oggi come non mai, si consumano online ha visto, a partire dalla fine del secolo scorso, un susseguirsi di interventi legislativi in materia penalistica e processual-penalistica che, con alterne fortune, hanno cercato di introdurre e ridisegnare fattispecie e strumenti investigativi che potessero arginare il diffondersi degli illeciti posti in essere nell'ambiente di rete.[5]

Malgrado siano molteplici le fattispecie di reato astrattamente commissibili sulla rete internet, tra i settori maggiormente sensibili agli effetti dello sviluppo tecnologico e alle difficoltà in cui è incorso il diritto penale nel tentativo di stare al passo con l'evolversi della società dell'informazione deve indubbiamente ricomprendersi quello del diritto d'autore.[6]

Ed invero, proprio nell'ambito della proprietà intellettuale l'avvento dell'era di internet ha determinato i cambiamenti più significativi sia sotto il piano della concezione stessa di "opere dell'ingegno" sia sulle modalità di circolazione, riproduzione, messa a disposizione del pubblico, diffusione e fruizione illecita delle stesse.

I frammentari interventi legislativi sul Titolo III della L. 633/1941 che si sono susseguiti in maniera disordinata nel tentativo di approntare una risposta penale agli illeciti contro le creazioni intellettuali perpetrati in contesti

---

[4] Per tutti PICOTTI L., *Diritto penale e tecnologie informatiche: una visione d'insieme,* in CADOPPI A., CANESTRARI S., MANNA A., PAPA M., *Cybercrime,* 2019, Utet Giuridica.

[5] Si fa riferimento in particolare al D.Lgs. 518/1992 attuativo della Direttiva 91/250 CEE relativa alla tutela giuridica dei programmi per elaboratore, che nello specifico ha esteso ai programmi per elaboratore la tutela prevista per le opere dell'ingegno e ha introdotto l'art. 171 *bis* alla L. 633/1941 volto a sanzionare penalmente l'illecita duplicazione dei programmi per elaboratore; alla L. 547/1993, che ha introdotto nel codice penale i c.d. "reati informatici in senso stretto" quali, tra quelli che hanno trovato maggior fortuna applicativa, l'accesso abusivo ad un sistema informatico o telematico *ex* art. 615 *ter* c.p. e la frode informatica *ex* art. 640 *ter* c.p.; alla L. 248/2000, che oltre a modificare l'art. 171-*bis* L. 633/1941 estendendo la tutela penale anche alle banche di dati elettroniche ha inserito i delitti di pirateria agli artt. 171-*ter* ss., in seguito più volte modificati; alla L. 48/2008 che, in recepimento della Convenzione di Budapest del Consiglio d'Europa del 2001, ha introdotto nel codice penale le fattispecie di danneggiamento a programmi e sistemi informatici di cui agli artt. 635*bis* ss. c.p. ed è intervenuta sul Libro III e V del codice di procedura penale in merito di ispezioni, perquisizioni, accertamenti e sequestri di dati, programmi e sistemi informatici e telematici; al D.Lgs. 101/2018 di adeguamento della normativa nazionale al Regolamento 679/2016, che ha modificato gli artt. 167 ss. del D.Lgs. 196/2003.

[6] *Amplius* sul tema FLOR R., *La tutela penale dei diritti d'autore e connessi,* in CADOPPI A., CANESTRARI S., MANNA A., PAPA M., *Cybercrime,* 2019, Utet Giuridica.

informatici e telematici hanno dato vita ad un sistema di tutela caratterizzato da una molteplicità di norme incriminatrici a tutela fortemente anticipata[7], talvolta sovrabbondanti e poco coordinate sia tra di loro che con l'impianto sistematico della legge, e che, salvo sporadici casi di applicazione giurisprudenziale, sono rimaste per la maggior parte lettera morta.
La disomogeneità degli interventi si rileva dalla stessa analisi delle fattispecie incriminatrici della legge 633/1941: se queste, infatti, erano originariamente riassunte nel disposto dell'articolo 171 del testo legislativo, le numerose novelle successive hanno poi determinato il passaggio ad un approccio casistico e fondato sulla previsione di un numero abnorme di fattispecie speciali, le quali, nel tentativo di disciplinare un'ampia pluralità di condotte ricadenti su beni digitali ed informatici, hanno determinato la sostanziale inefficienza del dato normativo.
L'inefficacia della sanzione penale per i delitti in materia di diritto d'autore non deve tuttavia lasciare oltremodo stupiti; ed invero, il diritto penale della proprietà intellettuale nell'epoca della *information society* appare tra i settori maggiormente penalizzati dalle difficoltà tipiche dei reati commessi in contesti digitali e di rete, relative in particolare all'individuazione degli autori[8], alla determinazione del *locus commissi delicti,* alla raccolta di materiale indiziario e probatorio e alla dimensione spesso transnazionale di tali delitti.
A ciò deve peraltro aggiungersi una, seppur ingiustificata, tendenza a considerare condotte aventi ad oggetto l'illecita diffusione sulla rete di opere dell'ingegno protette dal diritto d'autore quali comportamenti connotati da un più ridotto disvalore e un minor allarme sociale, attesa l'assenza di un danno immediato e direttamente percepibile sofferto dalla collettività dei consociati che, al contrario, si trova di fronte all'opportunità di accedere in ogni momento e da ogni luogo a materiale d'interesse e di poterne fruire senza dover sostenere particolari oneri economici altrimenti dovuti ai titolari dei diritti di proprietà intellettuale (oltreché, nella maggior parte dei casi, senza grandi rischi di incorrere in sanzioni).

---

[7] Si pensi, ad esempio, alla disposizione di cui all'art. 171-*ter* lett. F *bis)* L. Aut., che punisce penalmente già quei comportamenti prodromici all'effettiva violazione dei diritti di proprietà intellettuale sulle opere dell'ingegno nel mercato elettronico, proteggendo strumenti e tecniche di "autotutela tecnologica" adottate dai titolari dei diritti sui contenuti digitali attraverso l'incriminazione di condotte preparatorie all'aggiramento e all'elusione delle misure tecnologiche di protezione di cui all'art. 102 *quater* L. Aut. .

[8] Sul punto, emblematica è la richiesta di archiviazione presentata dal Pubblico Ministero presso il Tribunale di Roma in relazione ad una denuncia in materiale di *file sharing* su una piattaforma *peer to peer,* commentata da RICCI S., VACIAGO G., *Sistemi peer-to-peer: rilevanza penale delle condotte in violazione dei diritti d'autore e diritti connessi,* Diritto dell'Internet, 3/2008, 277 ss.

In un simile contesto si inserisce una delle principali problematiche con cui il diritto in generale e, per quanto qui interessa, il diritto penale ha dovuto confrontarsi negli ultimi anni in concomitanza con la progressiva e pervasiva evoluzione tecnologica, la quale attiene indubbiamente alla configurabilità di una responsabilità per quei soggetti – c.d. *Internet Service Providers* (di seguito anche "ISP") - che forniscono le infrastrutture digitali e gli spazi virtuali nel quale gli utenti possono interagire e scambiarsi dati, informazioni, conoscenza e contenuti, anche illeciti.
Nati infatti con lo scopo di fornire un accesso alle principali reti di comunicazione elettronica e di consentire la diffusione passiva di contenuti, gli *Internet Service Providers* hanno, con l'evolversi dell'*information society*, cambiato radicalmente volto: abbandonando via via la propria veste di "intermediari neutri" in favore di un ruolo maggiormente attivo, questi soggetti sono diventati dei veri e propri accentratori delle informazioni e dei contenuti scambiati e creati dagli utenti sulla rete.
Ciò ha consentito ai prestatori dei servizi di rete, ed in particolare ai ben noti *big* del mercato dell'informatica e del digitale, di acquisire la concreta possibilità di intervenire direttamente sui contenuti pubblicati dagli utenti (quali, ad esempio, i c.d. *user generated contents*[9]) allo scopo di aumentarne la visibilità, incrementarne le potenzialità di interazione e consentirgli maggiori opportunità di diffusione.
Parimenti, l'incremento del volume di informazioni gestito dalle piattaforme online, unito al progresso tecnologico nell'elaborazione dell'intelligenza artificiale e nell'uso di quegli strumenti di individuazione, profilazione e filtraggio automatico, emblematici del nuovo modello di business delle grandi aziende digitali che Shoshana Zuboff ha definito "capitalismo della sorveglianza"[10], ha attribuito alle maggiori realtà del mercato digitale la

[9] Il termine si è iniziato ad utilizzare con la diffusione delle piattaforme sociali. Secondo l'OCSE, per essere qualificato
come *user generated content* un contenuto deve essere: (i) pubblicamente accessibile su un sito Internet o un social network; (ii) il risultato di un certo apporto creativo; (iii) creato al di fuori di attività professionali o imprenditoriali. Si veda sul punto Organization for Economic Co-operation and Development, Participative web: user-created content, DSTI/ICCP/IE(2006)7/FINAL, 12/04/2007, consultabile al sito https://www.oecd.org/sti/38393115.pdf.

[10] ZUBOFF, S., *Il capitalismo della sorveglianza,* LUISS University Press, 10 ottobre 2019. L'opera, notissima, offre un'ampia disamina del sistema noto come "capitalismo della sorveglianza", che l'autrice identifica nello scenario alla base del nuovo ordine economico in forza del quale le immense aziende operanti nel mercato della società dell'informazione hanno iniziato a sfruttare l'esperienza umana sotto forma di dati come materia prima per pratiche commerciali segrete, imponendo il proprio dominio sulla società, sfidando la democrazia e mettendo a rischio la stessa libertà della collettività.

possibilità di valutare già a monte di quali contenuti impedire la diffusione nel cyberspazio; il riconoscimento, anche legislativo, di una simile facoltà ha pertanto esteso i confini della responsabilizzazione degli ISP, portando a riconoscere in capo agli stessi un vero e proprio *ius vigilandi* sull'attività degli utenti della rete internet e sull'*upload* di contenuti online .[11]

A questo mutamento di funzione si è accompagnato, com'era inevitabile, anche un cambio di prospettiva sul piano della responsabilità penale, divenendo imprescindibile chiedersi se e in che misura sussista a carico degli ISP un qualche obbligo di controllo rispetto alla diffusione illecita di contenuti protetti da parte di terzi, a che titolo possano essere chiamati a risponderne qualora abbiano concretamente influito nella veicolazione di materiale illecito e, infine, quale persona fisica all'interno dell'organizzazione imprenditoriale si possa individuare come destinatario del rimprovero e, di conseguenza, della sanzione penale.[12]

Le criticità sottese a questo cambio di prospettiva, del resto, non sono ininfluenti. È indubitabile che una responsabilizzazione dei fornitori di servizi informatici e di rete, facenti capo ad enti imprenditoriali e persone fisiche ben determinate, consentirebbe, quantomeno in astratto, di fornire una risposta penale alle istanze di tutela di quegli interessi lesi da condotte di singoli che nel ciberspazio risultano spesso impossibili da individuare e perseguire e rispetto alle quali le vittime si trovano spesso prive di rimedi in autotutela[13], atteso che, di norma, un utente offeso da un reato commesso in rete non ha la possibilità diretta di rimuoverne gli effetti pregiudizievoli senza l'intervento, tanto preventivo quanto successivo alla condotta illecita, del gestore della rete stessa.

---

[11] A conferma del mutamento della funzione degli ISP in materia di diritto d'autore e tutela delle opere dell'ingegno sulla rete internet può richiamarsi il considerando n. 59 della Direttiva D2001/29/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 (c.d. Direttiva "InfoSoc"), ove afferma come, in ambito digitale, i servizi degli intermediari (ossia gli ISP) possono essere sempre più utilizzati da terzi per attività illecite, riconoscendo al contempo la maggiore idoneità di siffatti intermediari, in molti casi, a porre fine a dette attività illecite.

[12] Si vedano sul punto INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?,* in LUPARIA L. (a cura di), *Internet Provider e giustizia penale: modelli di responsabilità e forme di collaborazione processuale,* 2012, Giuffrè Editore;

[13] Emblematico sul punto l'orientamento della giurisprudenza di legittimità, da ultimo ribadito con la sentenza Cass. Pen. n. 12427 del 31/03/2021 in un caso di truffa online, secondo cui la natura dematerializzata del cyberspazio, e la conseguente distanza intercorrente tra la vittima e l'autore, che può così schermare la propria identità, consentirebbe di ritenere sussistente l'aggravante della minorata difesa *ex* art. 61 n. 5 c.p. con riferimento alle circostanze di luogo.

A parere di chi scrive, tra l'altro, pur nel rispetto e nei limiti degli inderogabili principi di materialità e di colpevolezza, la canalizzazione del rimprovero penale (anche) verso il gestore della piattaforma online rispetto alle violazioni penalmente rilevanti del diritto d'autore commesse dai fruitori dei suoi servizi rappresenterebbe, da un lato, un forte incentivo per gli ISP all'adozione di comportamenti virtuosi finalizzati a contrastare già *ex ante* la commissione di condotte contrastanti con il concetto di una rete internet sicura, libera e nella quale gli utenti possano effettivamente esprimere la propria personalità e vedere tutelate le proprie creazioni intellettuali e, dall'altro, una concreta garanzia per le vittime che, nell'ottica dell'esercizio dell'azione civile in sede penale, potrebbero rivolgersi a soggetti facilmente individuabili e, indubbiamente, maggiormente solvibili rispetto alle persone fisiche materialmente autrici dei reati, spesso mascherate dietro un'impenetrabile rete di server o soggette ad ordinamenti di paesi situati a migliaia di kilometri di distanza dal nostro.

Tuttavia, se in ambito civilistico una parziale risposta al quesito inerente all'*accountability* degli ISP per le informazioni trasmesse e memorizzate è stata fornita dal D.Lgs. 70/2003, attuativo della Direttiva CE 2001/30 sul commercio elettronico, su cui si tornerà *infra,* in materia penale sembra permanere una difficoltà di fondo nell'individuare i margini per l'applicazione dei tradizionali modelli di responsabilità per concorso *ex* art. 110 c.p. e/o per omissione *ex* art. 40 c. 2 c.p. nei confronti dei fornitori di servizi di rete.

In particolare, come meglio si rappresenterà nel prosieguo, le problematiche nell'individuazione di uno statuto penale dell'ISP discendono, oltre che da una serie di questioni legate al difficile accertamento dell'elemento soggettivo, dalla complessità di definire i tre principali profili di responsabilità ascrivibile al *provider* in relazione ai contenuti illeciti trasmessi e ospitati sui propri server. Tali profili di responsabilità, come si vedrà*,* possono infatti ricondursi, rispettivamente, al caso in cui lo stesso *provider* abbia tenuto una condotta attiva agevolatrice dei reati posti in essere dai fruitori dei suoi servizi, al caso in cui si riconosca in capo all'ISP una qualche posizione di garanzia, penalmente sanzionata, diretta ad impedire la commissione di delitti all'interno degli ambienti di rete da lui amministrati e, infine, al caso in cui, una volta a conoscenza dell'avvenuta commissione del reato, il *provider* rimanga inerte e ometta di adottare le misure volte a far cessare gli effetti dell'illecito.

Vero è altresì che alle lacune legislative in merito hanno fatto da contraltare apprezzabili tentativi della giurisprudenza nazionale e comunitaria finalizzati a chiarire, con pronunce che ormai possono considerarsi *leading cases* in materia, i parametri di attribuzione della responsabilità penale a carico degli ISP per gli illeciti commessi dagli utenti sulle piattaforme online, ancorché non tutti inerenti alla violazione di opere dell'ingegno.

Da ultimo, con particolare riferimento alla responsabilizzazione dei fornitori di servizi ed infrastrutture di rete per i contenuti illeciti pubblicati dai singoli negli ambienti di rete da loro gestiti, non possono ignorarsi i recenti interventi del legislatore europeo nel settore del diritto d'autore e dei diritti connessi nel mercato digitale con la Direttiva UE 2019/790 (recentissimamente recepita a livello interno dal D.Lgs. n. 177 del 08/11/2021) e la Proposta di Regolamento della Commissione Europea COM(2020)825 sul mercato unico dei servizi digitali (c.d. "*Digital Service Act*"), le quali, pur non incidendo direttamente in materia penale, aprono ed apriranno nuove prospettive nell'ottica di delimitare in maniera puntuale le funzioni, gli obblighi e le responsabilità degli ISP, ed in particolare delle maggiori organizzazioni imprenditoriali che gestiscono le maggiori piattaforme di *upload* e di condivisione online, in relazione alle opere dell'ingegno diffuse dagli utenti nel contesto digitale in violazione dei diritti di proprietà intellettuale, offrendo spunti utili anche agli operatori del diritto penale.
Ciò premesso, la presente trattazione si propone di indagare, nei limiti concessi dall'ampiezza della materia, se e in che misura possa configurarsi una responsabilità penale a carico dei fornitori di servizi online per le condotte poste in essere dagli utenti che popolano la rete internet lesive dei diritti di proprietà intellettuale e quali tra le categorie tradizionali dell'attribuzione della responsabilità penale appaiano più idonee ad applicarsi alla peculiare figura dell'*Internet Service Provider*, tenuto altresì conto delle prospettive *de jure condendo* offerte dalla giurisprudenza e dal legislatore comunitario nei recentissimi interventi in materia di tutela delle opere dell'ingegno nell'ambito della società dell'informazione.

2. Le diverse qualificazioni dell'Internet Provider nell'ordinamento in relazione all'attività svolta online. I servizi di *mere conduit, caching* e *hosting*.

La disamina dei possibili profili di responsabilità penale degli ISP per i reati consumati nel "ciberspazio" trova come necessario punto di partenza un preliminare inquadramento giuridico della figura stessa del prestatore di servizi digitali e delle differenti funzioni che, nel contesto della rete internet, questi può venire a svolgere nell'ambito del tipo di servizio fornito agli utenti.
Al riguardo, può preliminarmente rilevarsi che *l'Internet Service Provider* è un prestatore intermediario che esercita in maniera economica ed organizzata un'attività imprenditoriale in rete, basata sulla prestazione di servizi della società dell'informazione, da intendersi, come "*qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta*

individuale di un destinatario di servizi"[14] e, più in generale, "*attività economiche svolte in linea – online*".[15]
È interessante evidenziare, in primo luogo, la frequenza con cui il legislatore, specialmente in ambito sovranazionale si è preoccupato di attribuire una definizione generale all'*Internet Provider* nei differenti interventi normativi diretti a tenere il passo con l'evoluzione della società dell'informazione.
Particolarmente estesa è, ad esempio, la nozione di "*service provider*" fornita dall'art. 1 della Convenzione di Budapest del 2001 del Consiglio d'Europa sul *Cybercrime*[16], recepita nel nostro ordinamento dalla L. 48/2008 che, come noto, ha inciso con non poche modifiche sul codice penale e, soprattutto, sul codice di rito.
Ai sensi della Convenzione, infatti, con il termine "*Internet Provider*" si può intendere "*qualunque entità pubblica o privata che fornisce agli utenti dei propri servizi la possibilità di comunicare attraverso un sistema informatico*" nonché "*qualunque altra entità che processa o archivia dati informatici per conto di tale servizio di comunicazione o per utenti di tale servizio*".
Tale nozione pare senz'altro idonea ad abbracciare pressoché ogni soggetto che, direttamente o indirettamente, mette a disposizione della collettività un servizio relativo all'utilizzo di un'infrastruttura informatica e telematica, ancorché non abbia ad oggetto un'attività svolta in rete.
Ad ogni modo, la definizione di *Internet Provider* che maggiormente interessa in questa sede è quella contemplata dall'art. 2 n. 6 della Direttiva UE 2019/790 sul Diritto d'Autore nel Mercato Unico Digitale, innovativa ed integrativa della precedente Direttiva CE 2001/29, recepita a livello nazionale dal recentissimo D.Lgs. 177/2021[17], sui quali si tornerà più approfonditamente nel prosieguo.
Basti qui evidenziare che la Direttiva, nella più ampia ottica di prevedere un particolare regime di responsabilizzazione per i *provider* di servizi digitali, si preoccupa altresì di dare un'espressa nozione alla figura del "*prestatore di servizi di condivisione di contenuti online*", qualificato come il "*prestatore di servizi della società dell'informazione il cui scopo principale o uno dei principali scopi è quello di memorizzare e dare accesso al pubblico a grandi quantità di opere protette dal diritto d'autore o altri materiali protetti caricati dai suoi utenti, che il servizio organizza e promuove a scopo di lucro*".[18]

---

[14] Tale è la definizione di servizio della società dell'informazione riportata dall'art. 1 della Direttiva CE 1998/34, cui rinvia l'art. 2 lett. A) della Direttiva CE 2000/31.
[15] Nozione riportata dall'art. 1 lett. A) del D.Lgs. 70/2003 sul commercio elettronico, in attuazione della Direttiva CE 2000/31.
[16] Consultabile online, in inglese, al sito https://rm.coe.int/1680081561.
[17] Il Decreto, entrato in vigore il 12/12/2021, pubblicato in G.U. Serie Generale n. 283 del 27/11/2021, è reperibile al sito https://www.cyberlaws.it/2021/dlgs-177-2021/.
[18] Peraltro, la stessa Direttiva 790/2019, al Considerando 62, prevede un'espressa limitazione dell'estensione della definizione di "prestatore di servizi di condivisione

Tale definizione, riprodotta in maniera pressoché identica dal nuovo art. 106 *sexies* L. Aut. introdotto *ad hoc* dal D.Lgs. 177/2021, risulta assai puntuale nella misura in cui individua quelle che, in concreto, sono le due principali attività svolte dagli ISP nella prestazione dei servizi della società dell'informazione per quanto riguarda le opere dell'ingegno digitali: la memorizzazione e l'accesso fornite dietro la percezione di un corrispettivo.
Muovendo oltre le definizioni generali dell'ISP, ci si deve ora concentrare sulle specifiche attività svolte dai fornitori di servizi internet cui la legge attribuisce rilevanza nella previsione di una responsabilità per i contenuti e le informazioni trasmesse e memorizzate dai medesimi.
Deve innanzitutto premettersi che ciò che comunemente viene definita "rete internet", spesso erroneamente assimilata al concetto di "*world wide web*" (il quale altro non è che uno dei differenti servizi fruibili sulla rete internet stessa), comprende una rete di computer tale da consentire a tutti coloro che vi si collegano di avere accesso ai dati contenuti o immagazzinato in elaboratori ovunque situati, purché connessi alla rete e dotati di un indirizzo *Internet Protocol* (IP).
La trasmissione di dati sulla rete avviene mediante l'invio di "pacchetti" di impulsi elettrici, che possono rappresentare qualsiasi tipo di informazione e contenuto, compresi, per quanto qui di interesse, testi, immagini, video, musica, programmi per elaboratore ed altre opere dell'ingegno, che possono così essere scambiate e fruite dagli utenti.
Alle due estremità della comunicazione dei dati su internet vi sono, da un lato, il computer del "*content provider",* ossia il fornitore del contenuto che immette i dati nell'"*host server",* il server che mette a disposizione l'ambiente virtuale nel quale i dati risiedono e vengono resi accessibili al pubblico, e, dall'altro, il computer del singolo utente che riceve i dati medesimi su richiesta[19].

---

di contenuti online", la quale, ai sensi e per gli effetti della Direttiva, comprende unicamente "*i servizi online che svolgono un ruolo importante sul mercato dei contenuti online, in concorrenza con altri servizi di contenuti online, come i servizi di streaming audio e video online, per gli stessi destinatari*", mentre sono esclusi i servizi che hanno uno scopo principale diverso da quello di consentire agli utenti di caricare e condividere una grande quantità di contenuti protetti dal diritto d'autore allo scopo di trarre profitto da questa attività, quali i prestatori di servizi cloud da impresa a impresa e di servizi cloud, che consentono agli utenti di caricare contenuti per uso personale, come i cyberlocker, o di mercati online la cui attività principale è la vendita al dettaglio online, e che non danno accesso a contenuti protetti dal diritto d'autore, nonché "*i prestatori di servizi quali le piattaforme di sviluppo e di condivisione di software open source, i repertori scientifici o didattici senza scopo di lucro e le enciclopedie online senza scopo di lucro*".

[19] Una menzione specifica va fatta, sul punto, per quanto riguarda le reti che consentono lo scambio di contenuti "*Peer-to-peer*" (P2P), ovvero da utente a utente.

La trasmissione effettiva dei dati all'utente finale avviene, in ogni caso, tramite i *router,* ossia altri computer "di transito" che, svolgendo la funzione tecnica di nodi di comunicazione, leggono l'indirizzo sui pacchetti contenenti le informazioni e si adoperano affinché questi giungano tutti alla destinazione corretta nell'ordine corretto.[20]

Così descritto, sia pure in maniera sommaria, il funzionamento di base della circolazione delle informazioni sulla rete internet, possono meglio comprendersi le tre principali funzioni che la normativa sull'*e-commerce,* la prima ad occuparsi espressamente dello *status* giuridico degli ISP, attribuisce a tali figure nell'ambito della loro attività di prestazione di servizi di rete, e dalle quali fa derivare obblighi e responsabilità.

Nell'ambito della suddetta tripartizione di funzioni si può individuare, in primo luogo, l'attività di semplice trasporto (c.d. *mere conduit*), classificata dall'art. 12 della Direttiva CE 2000/31, il cui dettato è riportato dall'art. 14 D.Lgs. 70/2003, come la "*prestazione di un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione*", cui accede altresì "*la memorizzazione automatica, intermedia e transitoria delle informazioni trasmesse, a condizione che questa serva solo alla trasmissione sulla rete di comunicazione e che la sua durata non ecceda il tempo ragionevolmente necessario a tale scopo*".

Rientrano, pertanto, nell'ambito di tale prestazione sia le attività dei server di transito e dei nodi di comunicazioni (c.d. *routers*) che consentono la

---

Tramite la rete P2P ogni computer diventa contemporaneamente fornitore e fruitore di contenuti. Particolarità della rete P2P, specie nell'ambito della condivisione di contenuti, è che il fornitore del servizio si limita ad indicizzare gli indirizzi di rete (ossia i singoli computer) nel quale sono registrati i file di cui si richiede la fruizione. Occorre in ogni caso tener presente che tale funzione apparentemente passiva non è scevra di ricadute sul piano giuridico in materia di diritto d'autore, atteso che, come noto, non sono sporadiche le sentenze con cui la Corte di Giustizia dell'UE ha ritenuto che la fornitura di piattaforme di condivisione online mediante l'indicizzazione di metadati relativi ad opere protette deve ritenersi ricompresa nella nozione di "comunicazione al pubblico" rilevante ai fini dell'applicazione della tutela per le opere dell'ingegno.

Per gli aspetti tecnici ed informatici della rete *Peer-to-peer* si rinvia a SARTOR G., *L'informatica giuridica e le tecnologie dell'informazione. Corso d'informatica giuridica;* si v. in merito anche RICCI S., VACIAGO G., *Sistemi peer-to-peer: rilevanza penale delle condotte in violazione dei diritti d'autore e diritti connessi.*

[20] Per una più ampia disamina sul funzionamento della rete internet in correlazione con la messa a disposizione delle opere dell'ingegno v. ERCOLANI S., *Il diritto d'autore e i diritti connessi. La legge n. 633/1941 dopo l'attuazione della direttiva n. 2001/29/CE,* 2004, Giappichelli Editore, Torino, 356 ss.

trasmissione dei pacchetti e la circolazione delle informazioni sulla rete, sia le attività di quei *providers* la cui funzione consiste nel fornire agli utenti, normalmente dietro un corrispettivo, accesso alla rete internet stessa (c.d. *access providers*).
La seconda funzione degli *Internet Provider* tipizzata dalla legislazione sul commercio elettronico è rappresentata dal c.d. "*caching*" o memorizzazione temporanea di dati e informazioni; si tratta di una funzione peculiare e che si presenta in maniera meno univoca rispetto alle operazioni di *mere conduit,* accesso e all'attività di *hosting* su cui si tornerà *infra*.
L'art. 13 della Direttiva 31 e l'art. 15 del D.Lgs. 70/2003 definiscono il *caching* come la prestazione di servizi della società dell'informazione avente ad oggetto la "*memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta*".
Tale è l'attività di riproduzione provvisoria di dati richiesti da un utente, automaticamente realizzata dal sistema e conservata per un tempo limitato: le copie dei dati rimangono per qualche tempo nei server del *provider*, cosicché un'eventuale successiva richiesta dei dati medesimi possa essere soddisfatta inoltrando la sola copia senza reperire le informazioni originali alla fonte.[21]
Oltre ad agire come semplice fornitore di accesso alla rete, vettore di informazioni o riproduttore di copie temporanee, l'ISP svolge una terza fondamentale funzione nel cyberspazio, consistente, secondo quanto previsto dall'art. 16 del D.Lgs. 70/2003, nella "*prestazione di un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio*".
Per quanto breve e puntuale, dietro tale definizione si cela l'attività degli ISP che presenta maggiori sfumature e criticità per quanto attiene alle possibili responsabilità dei fornitori di servizi di rete per gli illeciti commessi dagli utenti.
Il servizio di *hosting,* infatti, altro non è che la messa a disposizione a terzi, sulla base di un contratto di prestazione di servizi, di un sito web sui server dell'ISP o, più in generale, dell'ambiente virtuale nel quale gli utenti pongono in essere, in ogni momento e da ogni luogo, le proprie operazioni sulla rete internet. Peraltro, nel contratto di *hosting,* a tale prestazione principale si

[21] Come sottolinea ERCOLANI S., *Il diritto d'autore e i diritti connessi. La legge n. 633/1941 dopo l'attuazione della direttiva n. 2001/29/CE,* 364 ss., la funzione di *system caching* rappresenta la soluzione tecnica comunemente applicata dagli ISP al fine di diminuire il traffico sulla rete e limitare i rischi di intasamento del sistema a causa di picchi di richieste simultanee, riducendo al tempo stesso il tempo di attesa del servizio.

aggiungono, di norma, ulteriori servizi accessori ad essa collegati, quali, ad esempio, l'assistenza tecnica e lo sviluppo di software.
Si tratta, come intuibile, dell'attività nella quale comunemente vengono immedesimati gli *Internet Service Provider,* essendo quella che più di tutte rappresenta il mezzo per i fruitori del cyberspazio di disegnarne i tratti e di riempirlo di contenuti e dati che vengono memorizzati dall'ISP stesso e resi accessibili agli utenti. Per il vero, la nozione di *hosting provider* è più ampia e può comprendere diversi attori, quali i fornitori di servizi di *cloud computing* e *web hosting,* i gestori di mercati online, le piattaforme di condivisione di video e di contenuti musicali, di foto, i social network, i siti web di blogging o i siti web di recensioni fino alle sezioni dei commenti degli utenti sulle pagine delle notizie.
Come tale, peraltro, il servizio di *hosting* è quello che più di tutti si presta ad impegnare eventuali responsabilità dell'ISP per gli illeciti commessi dagli utenti della rete, atteso che è proprio all'interno degli spazi e delle piattaforme di creazione e condivisione di contenuti gestite dagli *host* che si materializzano e diventa percepibile ai consociati il disvalore delle diverse ipotesi di reato che possono configurarsi online, ivi comprese (soprattutto) le fattispecie aventi ad oggetto la violazione dei diritti di proprietà intellettuale sulle opere dell'ingegno digitali.[22]
A mente di ciò, non stupisce che anche la stessa Commissione Europea, nella sua Comunicazione n. 555 al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni del 28/09/2017 abbia preso atto di come proprio "*le piattaforme online* (ossia gli *hosting provider* n.d.r.) *che gran parte degli utenti di Internet consultano per accedere ai contenuti hanno la pesante responsabilità, nei confronti della società, di proteggere gli utenti e il pubblico in generale nonché prevenire lo sfruttamento dei loro servizi da parte di criminali e altri soggetti coinvolti in attività illegali online […] La diffusione di contenuti illegali online può chiaramente indebolire la fiducia dei cittadini nei confronti dell'ambiente digitale, ma potrebbe anche minacciare l'ulteriore sviluppo economico degli ecosistemi delle piattaforme e del mercato unico digitale. Le piattaforme online dovrebbero intensificare con fermezza le loro azioni per affrontare tale problema, come parte della responsabilità derivante dal loro ruolo centrale nella società*".[23]

---

[22] Le maggiori criticità sottese all'attività dell'*hosting provider* rispetto alle altre funzioni degli ISP sono ben evidenziate da PANATTONI B., *Gli effetti dell'automazione sui modelli di responsabilità: il caso delle piattaforme online,* Diritto Penale Contemporaneo, 2/2019.

[23] V. COM (2017) 555 del 28/09/2017 "*Lotta ai contenuti illeciti online. Verso una maggiore responsabilizzazione delle piattaforme online",* consultabile https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52017DC0555&from=IT.

Di conseguenza, è nei confronti della figura dell'*hosting provider* che deve focalizzarsi maggiormente l'attenzione in relazione all'esistenza e ai limiti degli obblighi, a carico degli ISP, di vigilanza sui contenuti illeciti pubblicati dagli utenti, di rimozione degli stessi e di collaborazione con l'autorità pubblica per il perseguimento degli autori dei reati commessi sulla rete internet, nonché alla corrispondente, eventuale, responsabilità penale per l'inosservanza di tali doveri.

3. Il regime di responsabilità dell'ISP nel panorama legislativo nazionale e comunitario.

Ferme restando le nuove prospettive apertesi con la Direttiva UE 790/2019 e con la Proposta di Regolamento nota come *Digital Service Act,* la disciplina in tema di responsabilità degli Internet Service Providers attualmente in vigore è contenuta, in linea di massima, nella direttiva europea sul commercio elettronico 2000/31/CE, e, a livello nazionale, nel relativo decreto legislativo di attuazione n. 70/2003. Tanto nella direttiva quanto nel decreto di recepimento si rinvengono quattro disposizioni dedicate al generale regime di responsabilità dei prestatori intermediari di servizi della società dell'informazione, le quali, seppur non dirette a disciplinarne i profili penalistici, meritano un breve accenno nell'ottica di porre le basi per la successiva trattazione dei possibili risvolti penali relativi alle funzioni esercitate nella rete dagli ISP.[24]

Nel dettaglio, i presupposti di esonero da responsabilità variano in base alla prestazione effettuata.

Con riferimento all'attività di *mere conduit*, non è configurata alcuna responsabilità del *provider*, nei limiti in cui lo stesso non partecipi alla produzione delle informazioni o non le modifichi, oppure non selezioni direttamente il destinatario della trasmissione.[25]

Si può notare, sul punto, come l'esenzione di responsabilità del *mere conduit provider* prevista dalla legislazione sull'*e-commerce* si sovrapponga alla norma, prevista dall'art. 68 *bis* della L. 633/1941, sull'eccezione per la riproduzione temporanea di copie nel corso di un procedimento tecnologico, eseguite all'unico scopo di consentire la trasmissione in rete tra terzi con l'intervento di un intermediario, o un utilizzo legittimo di un'opera o di altri materiali.[26]

---

[24] Sul tema della responsabilità civile degli ISP v. TOSI E., *L'evoluzione della responsabilità civile dell'Internet Service Provider passivo e attivo,* Il Diritto Industriale, 6/2019, 590 ss.

[25] V. art. 12 Direttiva 2000/31 e art. 14 D.Lgs. 70/2003.

[26] Deve in ogni caso rammentarsi che lo stesso art. 68 *bis* l. aut. fa espressamente salve le norme in materia di responsabilità degli ISP in materia di commercio

Quanto all'attività di *caching,* il *provider* non risponde della memorizzazione automatica, intermedia e temporanea delle informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta, a condizione che, oltre a non modificare le informazioni, non interferisca con l'uso lecito[27] di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni e agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitarne l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione.[28]
Infine, con riferimento all'*hosting provider,* questi viene esonerato da responsabilità per l'eventuale illiceità delle informazioni memorizzate a richiesta di un utente laddove non sia effettivamente a conoscenza dell'antigiuridicità dell'informazione o comunque di circostanze che ne rendano manifesta l'illiceità ovvero qualora, non appena a conoscenza della natura illecita delle informazioni memorizzate, su richiesta delle autorità, agisca immediatamente per rimuovere le informazioni o disabilitarne l'accesso[29] (c.d. procedura di "*notice and take down*" già nota alla normativa statunitense a tutela del diritto d'autore contenuta nel *Digital Millennium Copyright Act* del 1998, precursore e norma ispiratrice di tutta la disciplina

elettronico. *Amplius* sul tema v. ERCOLANI S., *Il diritto d'autore e i diritti connessi. La legge n. 633/1941 dopo l'attuazione della direttiva n. 2001/29/CE,* 375 ss.

[27] Sul punto v. STEA G., *La responsabilità penale dell'Internet Provider,* Giurisprudenza Penale, 11/2016, il quale evidenzia che l'aggettivo lecito sottolinea la necessità che il prestatore agisca secondo correttezza e senza interferire direttamente nella selezione delle informazioni.

[28] V. art. 13 Direttiva 2000/31 e art. 15 D.Lgs. 70/2003.

[29] V. art. 14 Direttiva 2000/31 e art. 16 D.Lgs. 70/2003. Si noti come l'art. 16 del D.Lgs. 70/2003, differenza di quanto indicato nella Direttiva, condizioni il formarsi dell'obbligo di rimozione alla previa notifica da parte di un'autorità (amministrativa o giudiziaria). Di conseguenza, facendo esclusivamente leva sul dato letterale, *l'hosting provider* sarebbe tenuto a procedere alla rimozione del contenuto soltanto in presenza di una conoscenza "qualificata", ossia laddove la notifica della manifesta illiceità gli pervenga da una delle sopra dette autorità e non anche quando l'abbia autonomamente acquisita. Condividono tale assunto*;* MANNA A., DI FLORIO M., *Riservatezza e diritto alla privacy: in particolare, la responsabilità per omissionem dell'Internet Provider,* in CADOPPI A., CANESTRARI S., MANNA A., PAPA M., *Cybercrime,* 2019, Utet Giuridica, 908 ss.; BARTOLI R., *Brevi considerazioni sulla responsabilità penale dell'Internet Service Provider,* Diritto Penale e Processo, 5/2013, 602.

legislativa europea in materia di responsabilità degli ISP e tutela delle opere dell'ingegno su internet[30]).
Sempre con riferimento *all'hosting provider,* deve precisarsi che il comma secondo dell'art. 16 sancisce l'ovvia inapplicabilità del regime di esclusione della responsabilità del prestatore di servizi se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore.[31]
La disposizione di chiusura della complessa quanto apparentemente succinta disciplina della responsabilità degli ISP è rappresentata dall'art. 17 del D.Lgs. 70/2003, attuativo dell'art. 15 della Direttiva 31.
Tale disposizione risulta effettivamente centrale nel processo di delimitazione della responsabilità, anche penale, dei *providers* e di individuazione degli obblighi cui gli stessi sono tenuti per le informazioni trasmesse dai destinatari dei loro servizi.
La norma sancisce infatti l'assenza di un obbligo generale di sorveglianza dell'ISP sulle informazioni trasmesse o ospitate nel suo server, ed esclude altresì un dovere di ricerca "attivo" di fatti o circostanze che indichino la presenza di attività illecite.
Senonché, al comma secondo l'art. 17 attribuisce all'ISP, qualunque sia la funzione dal medesimo svolta nella prestazione di servizi della società dell'informazione, un onere comunicativo *ex post* nei confronti dell'autorità giudiziaria o amministrativa avente funzione di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un utente, a cui si associa l'obbligo di fornire, seppur a richiesta delle autorità competenti e non di propria autonoma iniziativa, le informazioni in suo possesso che consentano l'identificazione del destinatario dei servizi con cui ha accordi di memorizzazione/*hosting* dei dati, al fine di individuare e prevenire attività illecite.
L'ultimo comma della disposizione sancisce infine la responsabilità (civile) dell'ISP per l'eventuale illiceità dei contenuti memorizzati o trasmessi in tutti i casi in cui, su intimazione dell'autorità giudiziaria o amministrativa non ha agito prontamente per impedire l'accesso ai medesimi[32], ovvero se, avendo

[30] La procedura di *notice and take down* trova in Italia una puntuale regolamentazione nel Regolamento AGCOM in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuativa ai sensi del D.Lgs. 70/2003, Allegato A alla Delibera n. 680/13/CONS del 12/12/2013.
[31] TOSI E., *L'evoluzione della responsabilità civile dell'Internet Service Provider passivo e attivo* rileva la natura anti-elusiva della disposizione in nota, evidenziando che "*le cause di esclusione della responsabilità non possono essere pretestuosamente invocate da chi controlla - in via di fatto o di diritto - il destinatario del servizio, destinatario privo di autonomia che agisce eseguendo le indicazioni del prestatore del servizio*".
[32] Sul punto, preme osservare che la stessa Corte di Giustizia dell'Unione Europea, con sentenza CGUE, 25/10/2017, Causa C-18/18, Eva Glawischnig-Piesczek contro Facebook Ireland Ltd. ha precisato che l'art. 15 della Direttiva 31/2000 (tradotto

avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non ha provveduto ad informarne l'autorità competente.

Nell'esame della disciplina relativa alla responsabilità dell'ISP prevista dalla Direttiva e dal relativo decreto attuativo, si deve in ogni caso tenere a mente che, secondo quanto previsto dallo stesso Considerando n. 42 della Direttiva[33] e ribadito più volte dalla giurisprudenza della Corte di Giustizia dell'Unione Europea[34], il sostanziale regime di *favor* è rivolto esclusivamente all'intermediario la cui attività sia di ordine "*meramente tecnico, automatico e passivo*", ossia l'ipotesi in cui quest'ultimo, oltre a non aver partecipato attivamente alla diffusione di contenuti illeciti, non abbia in ogni caso alcuna conoscenza o controllo sulle informazioni trasmesse o memorizzate.

Tale principio è stato peraltro affermato, di recente, anche in relazione all'attività dei gestori di piattaforme online che consentano la condivisione di

---

nell'art. 17 del D.Lgs. 70/2003), "*non osta a che un giudice di uno Stato membro possa ordinare a un prestatore di servizi di hosting di rimuovere le informazioni da esso memorizzate e il cui contenuto sia identico a quello di un'informazione precedentemente dichiarata illecita o di bloccare l'accesso alle medesime, qualunque sia l'autore della richiesta di memorizzazione di siffatte informazioni; ordinare ad un prestatore di servizi di hosting di rimuovere le informazioni da esso memorizzate e il cui contenuto sia equivalente a quello di un'informazione precedentemente dichiarata illecita o di bloccare l'accesso alle medesime, purché la sorveglianza e la ricerca delle informazioni oggetto di tale ingiunzione siano limitate a informazioni che veicolano un messaggio il cui contenuto rimane sostanzialmente invariato rispetto a quello che ha dato luogo all'accertamento d'illeceità e che contiene gli elementi specificati nell'ingiunzione e le differenze nella formulazione di tale contenuto equivalente rispetto a quella che caratterizza l'informazione precedentemente dichiarata illecita non sono tali da costringere il prestatore di servizi di hosting ad effettuare una valutazione autonoma di tale contenuto*".

[33] Considerando n. 42 della direttiva 2000/31/CE: "*Le deroghe alla responsabilità stabilite nella presente direttiva riguardano esclusivamente il caso in cui l'attività di prestatore di servizi della società dell'informazione si limiti al processo tecnico di attivare e fornire accesso ad una rete di comunicazione sulla quale sono trasmesse o temporaneamente memorizzate le informazioni messe a disposizione da terzi al solo scopo di rendere più efficiente la trasmissione. Siffatta attività è di ordine meramente tecnico, automatico e passivo, il che implica che il prestatore di servizi della società dell'informazione non conosce né controlla le informazioni trasmesse o memorizzate*".

[34] Cfr. *ex multis* CGUE, Grande Sezione, 12/07/2011, Causa C-324/09, L'Oréal SA e a. contro eBay Internation Ag e a., consultabile al sito https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62009CJ0324&from=IT; si veda altresì la più recente CGUE, III Sezione, 07/08/2018, Causa C-521/17, Cooperatieve Vereniging SNB-REACT U.A. contro Deepak Mehta, consultabile al sito https://curia.europa.eu/juris/document/document.jsf?text=&docid=204736&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=352928.

opere dell'ingegno (nel caso di specie, opere musicali), i quali andranno pertanto esenti da responsabilità qualora non svolgano un ruolo attivo idoneo a conferirgli una conoscenza o un controllo dei contenuti caricati sulla sua piattaforma.[35]

Per contro, la disciplina in esame non trova applicazione nei confronti dell'ISP "attivo", il quale, secondo l'orientamento più recente della Suprema Corte[36] intervenuta in ambito di responsabilità dell'ISP, è tale quando non pone in essere un'attività di ordine meramente tecnico, automatico e, appunto, passivo la quale non consente di conoscere e controllare le informazioni trasmesse o memorizzate dalle persone alle quali è fornito il servizio, bensì

[35] Cfr. CGUE, Grande Sezione, 22/06/2021, Cause C-682/18 e C-683/18, Frank Peterson contro Google LLC e a., nella quale la Corte ha specificato che l'art. 3 della Direttiva 2001/29/CE, e, di riflesso, l'art. 14 della Direttiva 2000/31/CE, devono interpretarsi *"nel senso che il gestore di una piattaforma di condivisione di video o di una piattaforma di hosting e di condivisione di file, sulla quale utenti possono mettere illecitamente a disposizione del pubblico contenuti protetti, non effettua una «comunicazione al pubblico» di detti contenuti, ai sensi di tale disposizione, salvo che esso contribuisca, al di là della semplice messa a disposizione della piattaforma, a dare al pubblico accesso a siffatti contenuti in violazione del diritto d'autore. Ciò si verifica, in particolare, qualora tale gestore sia concretamente al corrente della messa a disposizione illecita di un contenuto protetto sulla sua piattaforma e si astenga dal rimuoverlo o dal bloccare immediatamente l'accesso ad esso, o nel caso in cui detto gestore, anche se sa o dovrebbe sapere che, in generale, contenuti protetti sono illecitamente messi a disposizione del pubblico tramite la sua piattaforma da utenti di quest'ultima, si astenga dal mettere in atto le opportune misure tecniche che ci si può attendere da un operatore normalmente diligente nella sua situazione per contrastare in modo credibile ed efficace violazioni del diritto d'autore su tale piattaforma, o ancora nel caso in cui esso partecipi alla selezione di contenuti protetti comunicati illecitamente al pubblico, fornisca sulla propria piattaforma strumenti specificamente destinati alla condivisione illecita di siffatti contenuti o promuova scientemente condivisioni del genere, il che può essere attestato dalla circostanza che il gestore abbia adottato un modello economico che incoraggia gli utenti della sua piattaforma a procedere illecitamente alla comunicazione al pubblico di contenuti protetti sulla medesima".*

[36] Il riferimento è a Cass. Civ. Sez. I, n. 19 marzo 2019, n. 7708, con nota di CASSANO G., *La Cassazione civile si pronuncia sulla responsabilità dell'internet service provider. Nota a sentenza Cass. Civ. Sez. I, n. 19 marzo 2019, n. 7708,* in Il Diritto Industriale, n. 4/2019; si vedano anche ZANOVELLO F., *La responsabilità dell'Internet Service Provider. Brevi note a Cass. 19 marzo 2019, nn. 7708 e 7709,* Studium Iuris, 5/2020, 557 ss. e TORMEN L., *La linea dura della Cassazione in materia di responsabilità dell'hosting provider (attivo e passivo),* La Nuova Giurisprudenza Civile Commentata, 5/2019, 1039 ss.

un'attività che in qualche modo comporta una "manipolazione", in senso ampio, dei dati.[37]
Tra tali attività, la stessa Cassazione indica alcuni indici esemplificativi, fra i quali rientrano le attività di filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione o promozione dei contenuti, operate mediante una gestione imprenditoriale del servizio, come pure l'adozione di una tecnica di valutazione comportamentale degli utenti volta ad aumentarne la fidelizzazione: dacché si tratta condotte che, in sostanza, hanno l'effetto di completare ed arricchire in modo non passivo la fruizione dei contenuti da parte di utenti indeterminati.
L'esclusione del *provider* attivo dal regime di favore previsto dal D.Lgs. 70/2003 è stata peraltro affermata anche da consolidata giurisprudenza di merito nazionale, la quale, in materia di diritto d'autore, ha espressamente rilevato che quando l'attività del gestore di una piattaforma di condivisione di video online non può essere qualificata come fornitura di servizi di semplice "*hosting neutro e passivo*", identificandosi invece in una complessa organizzazione di sfruttamento pubblicitario ed economico dei contenuti immessi in rete dagli utenti attraverso un'organizzazione dei contenuti audiovisivi, è inapplicabile, in relazione a questa attività, l'art. 16 del D.Lgs. n. 70/2003 e la relativa esenzione da responsabilità, ma trova invece applicazione il regime della responsabilità aquiliana *ex* art. 2043 c.c.[38]
Oltre che ai fini della responsabilità civile, la distinzione tra *provider* attivo e passivo, come si vedrà nel prosieguo presenta importanti risvolti pratici nell'individuazione dei criteri di attribuzione della responsabilità penale nei confronti dei prestatori dei servizi della società dell'informazione, atteso che

[37] La sopravvenuta inadeguatezza della distinzione tra *hosting provider* passivo ed attivo è stata rilevata a PANATTONI B., *Gli effetti dell'automazione sui modelli di responsabilità: il caso delle piattaforme online,* 45 ss.
[38] Cfr. Trib. Roma, Sez. XVII Civ., n. 693 del 10/01/2019. Analoga in merito Trib. Milano 9 settembre 2011, secondo cui "*L'associazione di messaggi pubblicitari ai contenuti immessi in rete dagli utenti, la regolamentazione contrattuale con cui il prestatore di servizi si riserva determinati diritti sui materiali caricati sulla propria piattaforma, il servizio di segnalazione dell'eventuale illiceità del contenuto immesso, la predisposizione di un servizio di visualizzazione automatica di altri video correlati a quello prescelto dall'utente, sono tutti elementi che portano a differenziare la posizione di tale prestatore da quello puramente addetto alla fornitura di uno spazio per la memorizzazione delle informazioni trasmesse dagli utenti e alla visualizzazione delle stesse da parte di terzi; in particolare, detti elementi contribuiscono a qualificare i sopra menzionati servizi come di hosting attivo, così esorbitando da qualsiasi posizione di pretesa neutralità del prestatore e rendendo inapplicabile la disciplina di cui all' art. 16, D.Lgs. n. 70 del 2003 a favore di una valutazione della sua condotta secondo le comuni regole della responsabilità civile*".

il comportamento dell'*hosting provider* passivo potrebbe astrattamente e non senza difficoltà sussumersi nello schema della responsabilità omissiva *ex* art. 40 c. 2 c.p., laddove quello dell'*hosting provider* attivo in quello, invece, della responsabilità per concorso nella condotta di azione altrui.
Da ultimo, in materia di diritto d'autore non ci si può esimere dall'evidenziare che l'intera disciplina della responsabilità (civile) degli ISP prevista dal D.Lgs. 70/2003 dev'essere coordinata con le disposizioni di cui alla L. 633/1941 che, in via incidentale, possono chiamare in causa anche il prestatore di servizi della società dell'informazione per le violazioni dei diritti di proprietà intellettuale commesse online.
Su tutte, meritano un cenno in particolare gli artt. 156 e 163 della suddetta legge, i quali prevedono una particolare azione inibitoria proponibile da chiunque abbia ragione di temere la violazione di un diritto di utilizzazione economica a lui spettante al fine di accertare i diritti spettanti al medesimo e, in caso di violazioni, al fine di ottenere una pronuncia giurisdizionale che vieti il proseguimento della violazione.[39]
Ed invero, le norme menzionate consentono al titolare di privative economiche su opere dell'ingegno di agire non solo verso l'autore effettivo delle violazioni, ma altresì verso l'intermediario i cui servizi sono utilizzati per le violazioni medesime, il quale, in caso di accoglimento della domanda cautelare, dovrà necessariamente attivarsi per impedire la protrazione degli abusi commessi sulle piattaforme di rete a lui facenti capo.
È evidente che, nell'ipotesi di cui agli 156 e 163 L. Aut. , il *provider* destinatario dell'ordine inibitorio del giudice o della richiesta di rimozione proveniente dal privato, ancorché *ex ante* estraneo alle violazioni commesse dagli utenti dei propri servizi, non potrà più avvalersi del regime di esonero dalla responsabilità previsto dalla normativa sul commercio elettronico; ed invero, oltre a non poter certamente eccepire la mancata effettiva conoscenza dell'illecito, lo stesso *provider* dovrà attivarsi prontamente per impedire l'accesso ai contenuti illeciti, andando incontro, in difetto, al regime di responsabilità previsto dall'ultimo comma dell'art. 17 D.Lgs. 70/2003.

3.1. Le prospettive in tema di responsabilità degli ISP in materia di diritto d'autore nella legislazione comunitaria e nazionale: la Direttiva UE 790/2019, il D.Lgs. 177/2021 e il Digital Service Act.

Come anticipato nelle pagine precedenti, la *vexata quaestio* della responsabilità dell'ISP per le opere protette dal diritto d'autore pubblicate e diffuse, in un contesto di rete, dai fruitori della rete internet è stata oggetto,

[39] La norma in commento costituisce il recepimento dell'art. 8 della Direttiva 2001/29/CE, il quale, al comma 3, impone agli Stati membri di assicurare che "*i titolari dei diritti possano chiedere un provvedimento inibitorio nei confronti degli intermediari i cui servizi siano utilizzati da terzi per violare un diritto d'autore o diritti connessi*".

recentemente, di un profondo interesse da parte del legislatore comunitario, volto ad adeguare l'ordinamento giuridico al sempre più rapido sviluppo delle tecnologie informatiche e alle nuove istanze di tutela dei diritti sulle opere dell'ingegno che da tale sviluppo è derivato.
Tale interesse è andato concretizzandosi mediante l'adozione, da un lato, della Direttiva UE 2019/790 da parte del Consiglio e del Parlamento Europeo, e, dall'altro, della Proposta di Regolamento relativo ad un mercato unico dei servizi digitali, promossa dalla Commissione Europea, nota come "*Digital Service Act",* diretta alla modifica della Direttiva 2000/31/CE ad oggi vigente.
Data l'ampiezza delle tematiche e dei dibattiti inerenti tali provvedimenti, in questa sede ci si limiterà ad accennare gli aspetti di maggior rilievo che interessano la responsabilità dell'*Internet Provider* e che possono fornire utili spunti per un successivo approccio ai profili penalistici dell'attività del fornitore di servizi di rete nel contesto del diritto d'autore, rinviando a più adeguate sedi per una più completa trattazione della materia[40].
Partendo dalla Direttiva 790[41], si osserva che la medesima intende far seguito alle precedenti Direttive 96/9/CE e 2001/29/CE, rispettivamente volte a disciplinare la tutela delle privative d'autore sulle banche dati e del diritto d'autore e dei diritti connessi nella società dell'informazione, e che ormai appaiono non più in grado di tenere il passo con il progredire dell'innovazione tecnologica e delle problematiche che ne discendono per la protezione delle opere dell'ingegno.
Come già illustrato *supra,* la Direttiva contempla, tra i propri destinatari, la figura del "*prestatore di servizi di condivisione di contenuti online*" ("*online content-sharing service provider*"), sulla cui nozione, offerta dall'art. 2 n. 6), ci si è già soffermati in precedenza.
Una prima definizione dei contorni degli obblighi e delle conseguenti responsabilità in capo a tale soggetto, il quale, di regola, altro non è che una manifestazione particolare dell'*hosting provider* di cui all'art. 16 del D.Lgs. 70/2003, è fornita dai Considerando 62 e seguenti.
Tali Considerando vengono tradotti in norma di legge dall'art. 17 della Direttiva, disposizione centrale in materia di responsabilità del prestatore di

[40] Per una più ampia disamina della Direttiva 790/2019 sia consentito rinviare a RUOTOLO G.M., *A Season in the Abyss. Il nuovo copyright UE tra libertà di informazione, diritti fondamentali e mercato unico digitale,* in Il diritto dell'Unione Europea, 2/2019, 367 ss.; si veda altresì DI COCCO C., *Il diritto d'autore nell'era digitale: la tutela dei beni informatici*, in DI COCCO C., SARTOR G. (a cura di), *Temi di diritto dell'informatica*, Giappichelli, Torino, 2020, 195 ss.
[41] 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 e che modifica le direttive 96/9/CE e 2001/29/CE, consultabile in italiano al sito https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019L0790&from=RO

servizi di condivisione online all'interno del testo legislativo nonché nell'intero sistema di *accountability* degli ISP per le violazioni dei diritti di proprietà intellettuali seguenti all'illecita diffusione di opere dell'ingegno nel *world wide web*.
Occorre premettere che, richiamando il regime di responsabilità dei fornitori di servizi della società dell'informazione previsto dalla normativa sul commercio elettronico, l'art. 17, al comma 8, sancisce come principio generale l'assenza di un obbligo di sorveglianza in campo al *provider;* in forza di ciò, deve ritenersi che l'applicazione della norma, ai fini della responsabilizzazione del prestatore di servizi di condivisione online, presupponga che quest'ultimo svolga comunque un ruolo attivo nell'*upload* e nella diffusione dei contenuti coperti dal diritto d'autore.
Tale presupposto può ben dedursi dal primo comma dell'articolo *de quo,* che infatti prevede, come regola generale, che il prestatore di servizi di condivisione di contenuti online effettua un atto di comunicazione al pubblico o un atto di messa a disposizione del pubblico, ossia una condotta rilevante secondo la normativa in materia di diritto d'autore, quando concede l'accesso al pubblico a opere protette o altri materiali protetti caricati dai suoi utenti.
Quale conseguenza logica di tale premessa, pertanto, lo stesso comma 1 prescrive al *provider* di ottenere un'autorizzazione, anche mediante accordi di licenza, da parte dei titolari dei diritti sulle opere che intende mettere a disposizione dei fruitori del suo servizio.[42]
Peraltro, una volta ottenuta tale autorizzazione, la stessa si estende anche agli atti di comunicazione e messa a disposizione del pubblico di opere protette posti in essere da parte degli stessi utenti del servizio fornito dal *provider:* questi, pertanto, non dovrebbe incorrere in violazioni per condotte dei singoli, purchè i medesimi, per espressa previsione del comma 2 dell'art. 17, non agiscano per fini commerciali o comunque non ottengano ricavi significativi dalla diffusione dei contenuti protetti oggetto di autorizzazione.
Il comma 4 regola invece le ipotesi di responsabilità dei *providers* in caso di mancato ottenimento dell'autorizzazione da parte dei titolari dei diritti, prevedendo un onere della prova rafforzato a carico dei prestatori di servizi

[42] Secondo CICCOLO S., *Pirateria digitale in ambito editoriale, misura di prevenzione e azioni di tutela online del diritto d'autore: il caso Telegram,* in Il Diritto Industriale, n. 2, 1 marzo 2021, p. 194, la norma in esame mira a colmare il c.d. "*value gap*", ovvero la mancanza di corrispondenza tra i ricavi ottenuti dall'industria culturale e dai titolari dei diritti di sfruttamento delle opere, rispetto ai guadagni delle principali piattaforme del web che, quali intermediari tecnici (motori di ricerca, social network, aggregatori di contenuti, piattaforme audio/video), mettono a disposizione i contenuti agli utenti del web.

di condivisione di contenuti online, fondato su di un, forse eccessivamente generico, concetto di "massimo sforzo" ("*best effort*").
Questi ultimi, in tali situazioni, andranno infatti esenti da responsabilità per atti non autorizzati di comunicazione al pubblico, compresa la messa a disposizione del pubblico, di opere e altri materiali protetti, a patto che dimostrino di aver compiuto i massimi sforzi per ottenere un'autorizzazione dai titolari dei diritti d'autore e, in ogni caso, di aver agito tempestivamente, dopo aver ricevuto una segnalazione sufficientemente motivata dai titolari dei diritti, per disabilitare l'accesso o rimuovere dai loro siti web le opere o altri materiali oggetto di segnalazione e, infine, di aver compiuto i massimi sforzi per impedirne il caricamento in futuro.
Dal tenore letterale del suddetto comma può dedursi la duplice manifestazione di responsabilità dell'ISP per la violazione di diritti di proprietà intellettuale. Una prima manifestazione, *ex ante,* si avrà quando l'ISP non ottenga l'autorizzazione per la diffusione di materiale protetto (o non ponga in essere i "massimi sforzi" in tal senso); una seconda, *ex post,* si avrà quando l'ISP, venuto a conoscenza della presenza, sui propri server, di contenuti illeciti, rimanga inerte a fronte di richieste di rimozione degli stessi, le quali potranno provenire, oltre che dall'autorità giudiziaria secondo quanto previsto dalla normativa sull'*e-commerce,* anche dai singoli titolari dei diritti violati.[43]
Ad avviso di chi scrive, la Direttiva in commento, ancorando la responsabilità del *content-sharing service provider* (qualità che, a ben vedere, ad oggi può attribuirsi alla gran parte degli *hosting providers*) ad un parametro obiettivo quale quello dell'ottenimento dell'autorizzazione da parte dei titolari dei diritti sulle opere dell'ingegno diffuse su internet consente di superare, almeno nell'ambito del diritto d'autore, alcuni dei dubbi interpretativi che tutt'ora continua a sollevare la disciplina generale prevista dalla legislazione sull'*e-commerce* nelle definizione chiara e specifica delle soglie entro le quali l'ISP non viene chiamato a rispondere per gli illeciti compiuti dagli utenti della rete.
La centralità del tema della responsabilità dei *provider* di contenuti protetti nella società dell'informazione delineato dalla Direttiva 790 è comprovata

[43] Peraltro, la Direttiva, al Considerando 66, prevede comunque un limite al pericolo di una possibile oggettivizzazione della responsabilità del *provider* per gli atti di comunicazione al pubblico di opere senza l'autorizzazione dei titolari dei diritti. Tale limite, che sembra orientarsi verso una maggiore responsabilizzazione dei titolari di privative sulle opere dell'ingegno diffuse su internet, troverà applicazione nei casi in cui gli stessi titolari dei diritti non forniscano ai prestatori di servizi di condivisione le informazioni pertinenti e necessarie sulle loro opere specifiche o quando non provvedano, in ogni caso, a notificare una richiesta di disabilitazione dell'accesso o alla rimozione di specifiche opere non autorizzate.

dall'inusuale celerità che il legislatore italiano ha dimostrato nel recepire il provvedimento comunitario. Ed invero, è del 5 novembre 2021 il D.Lgs. n. 177 attuativo della suddetta direttiva nell'ordinamento interno.
Tale decreto, in vigore dal 12 dicembre 2021, traspone la disciplina dedicata ai fornitori di servizi di rete nel contesto della tutela della proprietà intellettuale nel nuovo Titolo II *quater* della L. 633/1941, rubricato "Utilizzo di contenuti protetti da parte dei prestatori di servizi di condivisione di contenuti online", in cui sono confluiti gli artt. 102 *sexies* e ss. della L. Aut., introdotti appositamente per fare spazio all'integrale normativa che la Direttiva riassume nel succitato art. 17 e nei relativi Considerando, ai quali, data la sostanziale identità tra le prescrizioni dei due testi di legge, si può rinviare.
In ogni caso, tra le disposizioni introdotte dalla novella del 2021 all'interno della Legge sul diritto d'autore merita una menzione particolare l'art. 102 *septies,* più specificamente dedicato alla responsabilità dei prestatori di servizi di condivisione di contenuti online per gli atti non autorizzati di comunicazione e messa a disposizione del pubblico in mancanza dell'autorizzazione dei titolari dei diritti prevista al precedente art. 102 *sexies,* all'esclusione di detta responsabilità in caso di compimento dei "massimi sforzi" diretti a prevenire la diffusione indebita delle opere dell'ingegno sulla rete internet e all'affermazione della mancanza di un generale obbligo di sorveglianza in capo ai *provider*.
Significativa, anche per quanto riguarda i possibili risvolti applicativi in sede penale delle nuove disposizioni di ispirazione comunitaria, è altresì la clausola, invero di difficile interpretazione sistematica, contenuta all'ultima comma dell'art. 102 *sexies*, secondo la quale, nelle ipotesi ricadenti nella sfera applicativa del nuovo Titolo II *quater* L. Aut., "*non si applica la limitazione di responsabilità di cui all'art. 16 del decreto legislativo 9 aprile 2003 n. 70"*.
Da una primissima lettura, la norma sembrerebbe escludere dallo speciale regime di *favor* previsto dalla normativa sull'*e-commerce* quei *provider* che mettono a disposizione del pubblico sulle proprie piattaforme online contenuti coperti da privative intellettuali senza quell'autorizzazione proveniente dagli autori prevista dall'art. 102 *sexies* L. Aut.; sicché, esemplificando, l'*hosting provider* che concede l'accesso a siti web su cui gli utenti possono fruire, duplicare, condividere o riprodurre opere dell'ingegno per le quali lo stesso *provider* non ha ottenuto l'autorizzazione o la licenza da parte dei soggetti legittimati non potrebbe più addurre, a propria discolpa, la mancanza di un'effettiva conoscenza delle attività illecite poste in essere dagli utenti.
Tuttavia, a parere di chi scrive, la severità di tale disposizione mal si concilia con l'opposto principio statuito dal successivo art. 102 *septies* L. Aut., secondo il quale il *provider* rimane esente da qualsivoglia obbligo di sorveglianza; esenzione il cui fondamento non si spiegherebbe laddove, al

contempo, il *provider* fosse chiamato a rispondere anche nelle ipotesi in cui, proprio in virtù dell'assenza del suddetto dovere di controllo, non gli potevano comunque essere note le condotte antigiuridiche poste in essere dai fruitori dei propri servizi di condivisione online.
Al fine di chiarire i dubbi interpretativi sollevati da tale apparente *impasse* legislativo sembra, pertanto, opportuno attendere le prime applicazioni giurisprudenziali del nuovo sistema di responsabilità dei *provider* in materia di diritto d'autore di ispirazione comunitaria.
Di rilievo è altresì la previsione di cui all'art. 102 *decies* della L. 633/1941 introdotto dal D.Lgs. 177/2021, il quale attribuisce ai titolari dei diritti di utilizzazione economica delle opere digitali la possibilità di chiedere direttamente al prestatore di servizi di condivisione di contenuti online (senza dunque attendere il provvedimento giurisdizionale inibitorio di cui agli artt. 156 e 163 della medesima legge) di disabilitare l'accesso a loro specifiche opere o ad altri materiali o di rimuoverli, indicando i motivi della richiesta. Se la richiesta è fondata, il prestatore dovrà immediatamente attivarsi per bloccare l'accesso al contenuto protetto oggetto di segnalazione e dare immediata comunicazione agli utenti dell'avvenuta disabilitazione o rimozione, nonché, ai sensi dell'art. 102 *septies* lett. c), porre in essere il massimo sforzo per impedirne il caricamento in futuro.
Infine, anche e soprattutto ai fini dei temi che saranno trattati nel prosieguo non può non menzionarsi la norma "di chiusura" prevista dal comma 2 dell'art. 102 *septies,* che con una formula forse giuridicamente infelice esclude ogni possibile limitazione di responsabilità del *provider* per l'illecita diffusione di materiali protetti sul web viene in ogni caso meno per il prestatore di servizi di condivisione di contenuti online "*che pratica o facilita la pirateria in materia di diritto d'autore*".
Le novità introdotte dal legislatore europeo con la Direttiva 790 e, di riflesso, dal legislatore nazionale con il D.Lgs. 177/2021 sembrano poter aprire nuove prospettive anche verso una più chiara demarcazione della possibile responsabilità penale degli ISP per i delitti in materia di diritto d'autore commessi dai destinatari dei servizi della società dell'informazione, tenendo comunque a mente che, al fine di poter effettuare ulteriori valutazioni in merito, specie in materia penale, non può che attendersi una prima casistica applicativa dei nuovi artt. 102 *sexies* ss. L. Aut.
La Direttiva 790/2019, tuttavia, appare solo il primo passo all'interno di un più ampio percorso di riforme della disciplina giuridica della società dell'informazione intrapreso dal legislatore comunitario. La necessità di assicurare l'equità del mercato digitale e, al contempo, di armonizzare la responsabilità delle piattaforme online e dei fornitori di servizi di rete ha dato infatti nuovi stimoli al legislatore europeo; stimoli concretizzatisi nella Proposta della Commissione per una legge sui servizi digitali (c.d. *Digital*

Service Act[44]) del 15 dicembre 2020, bozza di regolamento che, se e quando adottata dalle istituzioni legislative dell'Unione Europea, andrà a sostituire parzialmente le norme di armonizzazione dell'attività di prestazione transfrontaliera di servizi digitali nel mercato unico europeo, attualmente contenute nella direttiva 2000/31/CE sul commercio elettronico.
Rinviando ad altre sedi la trattazione più esaustiva dei contenuti del Digital Service Act[45], ci si può qui limitare a tratteggiare gli aspetti di novità di maggior rilievo per la responsabilità delle piattaforme online e dei grandi *players* del mercato dell'informatica, nei cui confronti la Proposta intende estrinsecare i propri effetti giuridici.
Nella sostanza, l'obiettivo di fondo del Digital Service Act consiste nel definire, in capo agli ISP, doveri di trasparenza e obblighi di informazione e di contrasto proattivo dei contenuti illegali, oltreché i requisiti che gli stessi sono tenuti a rispettare per beneficiare di esenzioni da responsabilità rispetto ai contenuti che ospitano, rimettendo agli Stati membri la quantificazione delle sanzioni irrogabili in caso di violazione di tali obblighi e requisiti da parte delle piattaforme online.
La Proposta si preoccupa altresì di fornire una nuova nozione di piattaforma online, focalizzando l'attenzione, all'art. 2 lett. H), sui prestatori di servizi di *hosting* che su richiesta di un destinatario del servizio, memorizzano e diffondono al pubblico informazioni, con esclusione delle attività aventi ad oggetto l'esecuzione di funzioni minori e puramente accessorie di un altro servizio e, per ragioni oggettive e tecniche, non possa essere utilizzata senza tale altro servizio.[46]
Quanto alla responsabilità delle piattaforme online per i contenuti trasmessi e memorizzati, il Digital Service Act non presenta particolari innovazioni rispetto alla vigente disciplina contenuta nella legislazione sull'*e-commerce*.

---

[44] Proposta di Regolamento COM(2020)825 del Parlamento Europeo e del Consiglio relativo ad un mercato unico dei servizi digitali che modifica la direttiva 2000/31/CE, consultabile in italiano al sito https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52020PC0825&from=IT .

[45] Una completa visione d'insieme della Proposta di Regolamento in esame è contenuta nel Dossier 51 del 12 maggio 2021 dell'Ufficio Rapporti con l'Unione Europea della Camera dei Deputati, consultabile al sito http://documenti.camera.it/leg18/dossier/pdf/ES051.pdf; sugli sviluppi più recenti del DSA si v. anche FULCO D., *Mercato unico digitale, il lavoro dell'Europa su DSA e DMA,* in Agenda Digitale, 31/10/2021, consultabile al sito https://www.agendadigitale.eu/mercati-digitali/mercato-unico-digitale-parlamento-ue-associazioni-e-centri-studi-al-lavoro-sul-dsa-e-dma/ .

[46] Ai sensi dell'art. 2 lett. I), inoltre, "*per diffusione al pubblico si intende la messa a disposizione di un numero potenzialmente illimitato di terzi di informazioni su richiesta del destinatario del servizio che le ha fornite*".

Ed invero, la Proposta, pur abrogando formalmente gli artt. 12, 13, 14 e 15 della Direttiva 31/2000, ne riproduce essenzialmente il contenuto. Peraltro, oltre a mantenere le esenzioni dalla responsabilità per i prestatori (seppur ammettendo all'art. 6 la possibilità per gli ISP di procedere ad indagini di propria iniziativa volte a individuare contenuti illegali), il DSA sancisce nuovamente il principio generale dell'insussistenza di un obbligo di sorveglianza "coattivo" in capo agli stessi, conformemente all'interpretazione già datane dalla Corte di Giustizia.[47]

Il Digital Service Act continua così a distinguere tra i *provider* (*access, mere conduit* e *caching providerss*) che forniscono solo servizi di connettività e archiviazione, e che quindi hanno scarse o nulle capacità di moderazione dei contenuti illegali[48] diffusi dai loro clienti, dai fornitori di servizi di *hosting,* oggetto di specifica attenzione da parte della Proposta di Regolamento in quanto, data la loro maggiore capacità di conoscenza, e quindi di moderazione, risultano destinatari di specifiche disposizioni in tema di obblighi e responsabilità e, inoltre, sono assoggettati a penetranti poteri di controllo e di ispezione da parte della stessa Commissione.[49]

Ulteriori disposizioni sono poi dedicate esclusivamente ai fornitori di servizi di *hosting,* che sono chiamati a predisporre meccanismi di notifica attivabili dagli utenti al fine di rendere nota al *provider* l'esistenza di contenuti illeciti memorizzati da quest'ultimo, nonché alle piattaforme online di grandi dimensioni (c.d. *gatekeepers*)[50], destinatarie di specifici obblighi di trasparenza e di valutazione dei rischi connessi alla loro attività giustificati

[47] A conferma di ciò si veda il Considerando 18, secondo cui "*le esenzioni dalla responsabilità stabilite nel presente regolamento non dovrebbero applicarsi allorché, anziché limitarsi a una fornitura neutra dei servizi, mediante un trattamento puramente tecnico e automatico delle informazioni fornite dal destinatario del servizio, il prestatore di servizi intermediari svolga un ruolo attivo atto a conferirgli la conoscenza o il controllo di tali informazioni*".

[48] L'art. 2 lett. G) della Proposta definisce come contenuto illegale "*qualsiasi informazione che, di per sé o in relazione ad un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme alle disposizioni normative dell'Unione o di uno Stato membro, indipendentemente dalla natura o dall'oggetto specifico di tali disposizioni*".

[49] Si vedano gli artt. 51 e seguenti della Proposta.

[50] Ai sensi dell'art. 25 della Proposta, sono considerate tali le piattaforme online che prestano i loro servizi a un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a 45 milioni. Tali soggetti hanno l'obbligo di individuare, analizzare e valutare eventuali rischi sistemici significativi derivanti dal funzionamento e dall'uso dei loro servizi nell'Unione, tra cui rientra, in particolare, la diffusione di contenuti illegali tramite i loro servizi.

dalla pervasività all'interno della collettività che caratterizza oggi i servizi forniti da tali piattaforme.
Ai fini della presente trattazione merita un cenno altresì l'art. 21 della Proposta, che pare attribuire un ruolo fortemente propulsivo agli ISP in relazione agli illeciti di cui vengono a conoscenza, seppur limitato ad ipotesi poco concretizzabili in un contesto digitale. Ed invero, la norma prevede uno specifico obbligo di denuncia in capo a tutte le piattaforme online, che sono tenute ad informare senza indugio le autorità giudiziarie dello Stato membro qualora vengano a conoscenza di informazioni che fanno sospettare che sia stato commesso, si stia commettendo o probabilmente sarà commesso un reato grave che comporta una minaccia per la vita o la sicurezza delle persone.
Pur tenendo conto dei tempi richiesti per l'attuazione in regolamento vincolante e generalmente applicabile del Digital Service Act, nonché di tutte i possibili emendamenti che potranno sopravvenire nelle more della conversione in legge del medesimo, è indubbio il carattere dirompente che assumerà la nuova normativa sulla responsabilità degli ISP. Peraltro, seppur non prevedendo direttamente sanzioni penali applicabili alle piattaforme online, a parere di chi scrive non può escludersi che il Digital Service Act costituirà un possibile incentivo, per il legislatore nazionale, ad intervenire anche in materia penale con la previsione di un più puntuale statuto penale dell'*Internet Provider* che possa sciogliere i dubbi e risolvere le problematiche sollevate dalla ricerca di un criterio di individuazione delle conseguenze penali delle condotte, attive ed omissive, poste in essere dagli ISP.

4. La responsabilità penale dell'*Internet Provider:* i criteri di responsabilizzazione dell'ISP per i reati contro la proprietà intellettuale commessi dagli utenti

Dalla suesposta illustrazione del quadro generale della responsabilità degli intermediari nella prestazione di servizi internet si possono dedurre una serie di principi fondamentali regolanti l'attività degli ISP, utili per muoversi nel delicato terreno dello statuto penale applicabile a tali soggetti.
In particolare, può affermarsi che la Direttiva 31/2000/CE ed il D.Lgs. 70/2003 garantiscono agli ISP una sorta di "*safe harbour",* escludendo che le attività di *mere conduit, caching* e *hosting* (quantomeno passivo) possano essere fonte di responsabilità *ex ante* per i contenuti illeciti trasmessi e memorizzati a condizione che il fornitore si limiti ad un'attività sostanzialmente tecnica e automatizzata e non abbia effettiva conoscenza dei suddetti contenuti illeciti. Tale necessaria "effettiva conoscenza", unitamente all'assenza di un obbligo di controllo preventivo sull'attività degli utenti della rete gestita dall'ISP (e, a *fortiori,* di impedimento dei reati commessi mediante l'utilizzo dei servizi offerti) sembrerebbe escludere, in astratto, la configurabilità di una penale responsabilità per tutti i casi in cui il *provider* non abbia agito attivamente e

offerto un proprio contributo materiale attivo alla perpetrazione di reati nel ciberspazio, ivi compresa l'illecita diffusione e trasmissione online di materiale coperto dal diritto d'autore.
Di conseguenza, oltre a non poter apparentemente fondare una responsabilità per *omissionem ex* art. 40 c. 2 c.p., in assenza di un'espressa posizione di garanzia positivamente determinata, la disciplina vigente sembrerebbe ostativa altresì alla contestazione, all'ISP, dei delitti commessi dai fruitori della rete a titolo di concorso *ex* art. 110 per il solo fatto di aver messo a disposizione le strutture e le piattaforme digitali che hanno permesso, o comunque agevolato, la commissione del fatto.[51]
Analoghe perplessità sorgono in relazione alla circostanza in cui il *provider*, venuto comunque a conoscenza dell'esistenza di contenuti illeciti memorizzati o trasmessi sui propri spazi di rete, pur non avendo concorso nella commissione del reato rimanga inerte nell'adempiere i propri doveri di collaborazione e notificazione all'autorità giudiziaria ovvero nella successiva rimozione del materiale caricato e diffuso *contra ius.*[52]
Ed invero, se l'omessa attivazione della procedura di *notice and take down* appare idonea ad impegnare la responsabilità civile del *provider* ai sensi dell'art. 17 D.Lgs. 70/2003, degli artt. 156 e 163 della L. 633/1941, non vi è alcuna disposizione che tipizzi una sanzione penale per tale specifico inadempimento; di conseguenza, l'effettività della tutela penale a garanzia della corretta esecuzione dei doveri di cooperazione in capo all'ISP imporrà l'individuazione di norme di diritto sostanziale applicabili al caso concreto.
Tale disciplina, tuttavia, se da un lato si conforma ai principi cardine del diritto penale, primi fra tutti quello di personalità e di colpevolezza, per altro verso rischia di andare a frustrare quelle altrettanto cardinali esigenze di tutela giuridica imposte dallo sviluppo della società dell'informazione e dall'innovazione tecnologica menzionate nelle pagine iniziali.
Sulla base di questa considerazione, pertanto, dottrina e giurisprudenza, ancor prima del legislatore, hanno intrapreso un percorso ermeneutico diretto a individuare, spesso mediante il ricorso a criteri dogmatici non sempre condivisibili, e cristallizzare alcuni "modelli", ricavati dagli istituti di parte generale del codice penale, di responsabilizzazione penale dell'ISP per

[51] Così PICOTTI L., *Diritto penale e tecnologie informatiche: una visione d'insieme,* 81 ss.
[52] Come evidenziato da BARTOLI R., *Brevi considerazioni sulla responsabilità penale dell'Internet Service Provider,* Diritto Penale e Processo, 5/2013, 602, riguardo alla responsabilità penale dell'ISP si pongono soprattutto due problemi: "*da un lato, la configurazione della condotta tipica in contesti di attività automatizzate; dall'altro lato, la problematica dell'impedimento del reato: ma attenzione, non solo, e non tanto, nella prospettiva ex ante, al momento dell'ingresso del dato che costituisce reato, quanto piuttosto nella prospettiva ex post, nel periodo di permanenza e protrazione del reato all'interno della rete*".

i reati posti in essere dagli utenti nel ciberspazio, andando a specificare i casi e le condizioni per la loro applicabilità.
In particolare, in dottrina è stata elaborata una convincente "tripartizione" dei paradigmi ideali di responsabilizzazione penale cui può ricondursi l'*Internet Provider* in base alla propria cooperazione, attiva od omissiva, *ex ante* o *ex post,* all'illecito del fruitore della rete[53].
Il primo paradigma pone l'*Internet Provider* sullo stesso piano degli altri utenti della rete internet e del ciberspazio, sicché non sono previsti particolari doveri di controllo o obblighi di denuncia rispetto a condotte altrui né oneri di collaborazione con le autorità nella repressione degli illeciti.
La rilevanza del comportamento dell'ISP sul piano penale, in questo senso, è limitata alle ipotesi di autoria diretta, qualora il *provider* si renda direttamente responsabile per uno degli illeciti tipizzati dalla L. 633/1941 (ad esempio effettuando lui stesso l'*upload* di opere protette o laddove sia lui stesso il *content provider*) ovvero di concorso commissivo materiale o morale (doloso) nel fatto altrui ai sensi dell'art. 110 c.p.
Il secondo modello focalizza invece l'attenzione sul potere degli ISP di limitare già preventivamente la diffusione di contenuti illeciti sulle proprie piattaforme e sul controllo che questi è in grado di mantenere sulle informazioni e dati da lui trasmessi e memorizzati. In quest'ottica, il criterio di responsabilità sarà quello del concorso omissivo improprio *ex* art. 40 c. 2 c.p. e, in particolare, il rimprovero consisterà nel non aver impedito un reato altrui in violazione di una posizione di garanzia la cui fonte legittimante, come si vedrà nel prosieguo, non è di facile individuazione.
Il terzo ed ultimo paradigma di responsabilizzazione si concentra non tanto sulla cooperazione, attiva od omissiva, del *provider* nella diffusione di contenuti illegali online, bensì sugli obblighi insorgenti in capo al medesimo successivamente alla commissione del reato. Tra questi, possono individuarsi in particolare l'attivazione della procedura di *notice and take down* e la cooperazione con l'autorità giudiziaria nell'individuazione degli autori: l'ISP non avrà più l'obbligo di impedire l'immissione di materiale illecito in rete, ma dovrà invece attivarsi per ridurre le conseguenze di reati già commessi e per agevolare la punizione degli autori. In questo caso, come anticipato,

[53] Il modello *de quo* è stato efficacemente sviluppato da INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine.* Sul punto si v. anche Ibidem*, Responsabilità penale degli internet service provider: attualità e prospettiva,* Diritto Penale e Processo, 12/2017; BARTOLI R., *Brevi considerazioni sulla responsabilità penale dell'Internet Service Provider,* Diritto Penale e Processo, 5/2013; FLOR R., *La tutela penale dei diritti d'autore e connessi;* PICOTTI L., *Fondamento e limiti della responsabilità penale dei service-provider in internet,* Diritto Penale e Processo, 3/1999, 379 ss.; Ibidem, *La responsabilità penale dei service-providers in Italia,* Diritto Penale e Processo, 4/1999, 501 ss.

ferma restando l'eventuale responsabilità omissiva per non aver impedito il reato a monte, sarà necessario comprendere a che titolo, a fini penali, poter contestare la violazione del suddetto obbligo al *provider*.[54]
Tale tripartizione, a parere di chi scrive, appare quella più idonea a risolvere le maggiori problematiche connesse allo statuto penale del prestatore di servizi della società dell'informazione: si ritiene opportuno, pertanto, proseguire nella trattazione attenendosi ai suddetti modelli di responsabilizzazione.

4.1. L'ISP come concorrente attivo dei reati commessi dagli utenti della rete: i casi paradigmatici e gli indirizzi dottrinali.

Il primo, e probabilmente meno problematico, paradigma di responsabilizzazione penale dell'ISP su cui concentrarsi è quello che vede il *provider* partecipare in modo commissivo nei delitti contro la proprietà intellettuale che vengono realizzati negli ambienti di rete da lui gestiti e mediante i servizi messi a disposizione degli utenti.
L'addebito di una responsabilità *ex* art. 110 c.p. al fornitore di servizi di rete che cooperi nell'illecita diffusione e riproduzione di contenuti protetti dal diritto d'autore richiede, tuttavia, una ferrea delimitazione dei caratteri che tale cooperazione deve manifestare.
In via preliminare, a mente della disciplina generale del concorso di persone nel reato, si deve rammentare che il contributo causale del concorrente morale può manifestarsi attraverso forme differenziate e atipiche della condotta criminosa, quali istigazione o determinazione all'esecuzione del delitto, agevolazione alla sua preparazione o consumazione, rafforzamento del proposito criminoso di altro concorrente, mera adesione o autorizzazione o approvazione per rimuovere ogni ostacolo alla realizzazione di esso[55]. Ciò che è necessario è che il giudice di merito fornisca compiuta motivazione sulla prova dell'esistenza di una reale partecipazione nella fase ideativa o preparatoria del reato e precisare sotto quale forma essa si sia manifestata, in rapporto di causalità efficiente con le attività poste in essere dagli altri concorrenti.
Ciò premesso, può osservarsi che, con riferimento al concorso nel reato del *provider,* secondo un primo autorevole orientamento dottrinale la semplice

[54] Secondo INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine,* ad ognuno di tali paradigmi corrisponde un diverso ruolo dell'ISP in relazione ai reati presupposto della sua responsabilità: nel primo caso, l'autore parla di ISP come "comune cittadino"; nel secondo, di ISP come "controllore – censore", che decide cosa può esistere nel ciberspazio con effetti giuridicamente rilevanti; nel terzo caso, si parla invece di ISP "tutore dell'ordine".
[55] Il principio, ormai consolidato, è stato espresso dalle Sezioni Unite della Corte di Cassazione, con sentenza n. 45276 del 30/10/2003.

fornitura e mantenimento, da parte degli ISP, dei servizi e delle prestazioni, tramite *hardware* e *software* messi a disposizione degli utenti al fine di consentire loro l'*upload* e la circolazione di contenuti risulterebbero di per sé sufficienti a fondare un'imputazione *ex* art. 110 c.p. nei confronti del *provider* per i delitti commessi dai fruitori dei servizi suddetti, salvi gli altri requisiti soggettivi ed oggettivi necessari richiesti dalla disciplina sul concorso di persone nel reato.[56]

Secondo la suesposta tesi, pertanto, già la semplice attività svolta dall'ISP, sia essa di *mere conduit, caching* o *hosting,* dovrebbe ritenersi contributo causalmente idoneo, quanto meno nella forma dell'agevolazione, alla commissione dei reati da parte degli utenti della rete, e come tale sufficiente a fondare la responsabilità concorsuale del *provider*.

A parere di chi scrive, tuttavia, tale approccio dev'essere ad oggi rivisitato alla luce del mutamento delle caratteristiche essenziali del ruolo del *service provider* nella moderna società dell'informazione (e, in particolare, dei fornitori di servizi di *mere conduit* e *caching* temporaneo) e dell'ormai elevatissima automazione delle procedure e degli algoritmi che permettono ai singoli di accedere, condividere e caricare contenuti online: in tali circostanze, infatti, l'attività dell'ISP presenta, in astratto, un contenuto assolutamente neutro e comunque lecito.

Di conseguenza, sembra necessario individuare un *quid pluris* che, accanto al mero criterio della prestazione svolta dall'ISP, possa fondare una rimproverabilità *ex* art. 110 c.p. nei confronti di quest'ultimo.

A tal fine, si comprende perché, come anticipato a più riprese, la sopravvenuta disciplina legislativa sull'*e-commerce* costituisca ad oggi il

---

[56] Così, in particolare, PICOTTI L., *La responsabilità penale dei service-providers in Italia,* Diritto Penale e Processo, 4/1999, 501 ss., il quale osserva che, secondo i principi generali in materia di responsabilità concorsuali, applicabili anche agli ISP, "*qualsiasi contributo atipico, causale o anche solo agevolatore, pur se "di minima importanza" […] che riguardi la preparazione ovvero l'organizzazione od esecuzione del reato, può fondare la responsabilità penale, a titolo quantomeno di partecipazione materiale: mentre se il contributo concerne la stessa esecuzione del fatto tipico, si dovrebbe più correttamente parlare addirittura di (co)autoria"*. Si oppone a questa tesi SEMINARA S., *La pirateria su internet e il diritto penale*, in *Riv. trim. dir. pen. eco.*, 1997, secondo il quale il ruolo decisivo dell'ISP nel ciberspazio impone per lo stesso uno statuto speciale più garantista in tema di responsabilità concorsuale, ed in particolare "*la costruzione di una responsabilità concorsuale del provider passa attraverso la notazione che la sua attività presenta un contenuto assolutamente neutro e in sé consentito dall'ordinamento giuridico, i cui connati di liceità o illiceità vanno ricercati nelle modalità di svolgimento del servizio stesso e possono attingersi all'esterno solo quando siano assistiti da un dolo di partecipazione particolarmente inteso e da un'oggettiva possibilità di impedire la commissione del reato"*.

punto di partenza irrinunciabile per la delimitazione della responsabilità penale dell'*Internet Provider*.

Come noto, i principi ricavabili dal D.Lgs. 70/2003 che possono determinare l'accertamento della responsabilità concorsuale attiva del *provider* sono essenzialmente due, nei quali possono identificarsi, rispettivamente, l'elemento oggettivo e soggettivo del reato ascrivibile all'ISP: il carattere non meramente tecnico e passivo dell'attività svolta e l'effettiva conoscenza dell'antigiuridicità dei contenuti trasmessi e memorizzati.

L'applicazione di tali corollari agli *access, mere conduit* e *caching* provider porta, di fatto, a rendere assai arduo ipotizzare una possibile responsabilità *ex* art. 110 c.p. in capo ai fornitori dei suddetti servizi, stante, da un lato, la natura essenzialmente neutra e, ad oggi, pressoché pienamente automatizzata dell'attività svolta dai medesimi e, dall'altro, la difficoltà di attribuire ad essi un'effettiva consapevolezza del contenuto delle informazioni e dei dati da loro trasportati nel ciberspazio. Difficoltà che, del resto, risulta pienamente coerente con uno dei valori cardine dell'informatica giuridica e del funzionamento della rete, ossia la *net neutrality*.[57]

Ragionando diversamente, infatti, a parere dell'autore si rischierebbe di pervenire all'inaccettabile conseguenza per cui la semplice stipulazione di un contratto di accesso ad internet con un numero indefinito di utenti potrebbe di per sé costituire fondamento per l'addebito di una responsabilità concorsuale attiva in capo al prestatore del servizio per ogni violazione penalmente rilevante del diritto d'autore compiuta dai suddetti utenti, sul presupposto per cui senza la fornitura del servizio di collegamento alla rete la diffusione illecita di materiale protetto non potrebbe, già *ex ante,* venire ad esistenza.

---

[57] La neutralità della rete rappresenta, oltre che un principio fondamentale dell'informatica giuridica, la base del funzionamento di internet secondo i protocolli TCP-IP, in forza del quale gli intermediari che amministrano la trasmissione dei pacchetti contenenti le informazioni che viaggiano sul *network* mantengono, rispetto ai contenuti dei pacchetti stessi, una sostanziale imparzialità e indifferenza. Ciò presuppone che, per lo stesso corretto e trasparente funzionamento del sistema i servizi di *mere conduit* e *caching* temporaneo si disinteressino dei dati trasportati e della loro eventuale illiceità, sicché appare complesso, soprattutto in riferimento alla sussistenza del dolo di concorso, poter ritenere i relativi *provider* come concorrenti attivi nel reato. Sulla definizione di neutralità della rete si v. la definizione di LONGO A., *"Che cos'è la net neutrality"*, Il Sole 24 Ore, 22/12/2010: "*per neutralità della rete s'intende il principio secondo cui gli operatori devono gestire il proprio traffico senza discriminazioni che danneggino concorrenza, innovazione e, in generale, i diritti degli utenti e delle aziende web*". Per una più esaustiva trattazione del tema si rinvia a SARTOR G., *L'informatica giuridica e le tecnologie dell'informazione. Corso d'informatica giuridica,* 20 ss.

Un ragionamento più analitico deve invece operarsi per l'*hosting provider*. Come infatti detto in precedenza, questo soggetto, soprattutto in materia di diritto d'autore, appare il reale destinatario dello statuto penale del fornitore di servizi internet, essendo colui che, di fatto, consente la diffusione e l'accesso al pubblico ad eventuale materiale coperto da proprietà intellettuale oggetto di violazioni.
Come illustrato in precedenza, il sostanziale regime di *favor* previsto dagli artt. 16 e 17 del D.Lgs. 70/2003 trova applicazione soltanto nei confronti del *hosting provider* c.d. "passivo", ossia l'intermediario che si limita a mettere a disposizione dell'utenza un protocollo di comunicazione ed uno spazio su cui allocare un contenuto, esercitando così quel servizio di ordine "meramente tecnico, automatico o passivo" che gli preclude tanto il controllo quanto la conoscenza sulle informazioni memorizzate (salvo il dovere di attivarsi a seguito di una comunicazione dell'autorità competente per la rimozione delle informazioni illecite ai sensi dell'art. 17 D.Lgs. 70/2003); sicchè, nei confronti del medesimo, sembra ragionevole poter operare il medesimo discorso già svolto per il *mere conduit* ed il *caching provider* quanto all'esclusione, almeno in astratto, di una responsabilità per concorso materiale o morale attivo nei reati commessi dagli utenti del ciberspazio, residuando invece spazi per una contestazione *ex* art. 40 c. 2 c.p. su cui si tornerà *infra*.
Per contro, la prospettiva si capovolge quando l'*hosting provider* non si limita più a giocare un ruolo neutrale e puramente tecnico rispetto al materiale memorizzato, ma inizia a porre in essere attività che, pur estrinsecandosi in forma di numeri binari, risultano sintomatiche di una sua cooperazione attiva nella condotta dei fruitori del servizio e, soprattutto, di tangibile consapevolezza del contenuto del materiale coperto da "*copyright*" di cui permette o agevola la diffusione e la riproduzione.
Ed invero, è proprio siffatta partecipazione attiva e consapevole nell'attività dei *content providers* della rete che potrebbe fondare una contestazione *ex* art. 110 c.p. a carico del fornitore di servizi di *hosting* in caso di illeciti realizzati dalle persone fisiche. Non è casuale, pertanto, che sia proprio nei confronti di tali soggetti che la tematica è stata affrontata, *in primis,* dalla giurisprudenza penale in tema di responsabilità dei *providers* per delitti in materia di diritto d'autore e, più di recente, dal legislatore nazionale con l'introduzione dell'art. 102 *septies* L. Aut., che, come visto poc'anzi, al comma 2 preclude già a monte ogni limitazione di responsabilità per la piattaforma di condivisione online che abbia agevolato la commissione di delitti di pirateria digitale.
In concreto, tuttavia, si pone il problema dell'individuazione delle condotte indiziarie di un concorso causale e agevolatore, materiale o morale, rispetto al reato del singolo utente.

Sul punto, in dottrina sono state esemplificate, quali attività in grado di impegnare la responsabilità penale per concorso dell'*hosting provider* attivo, l'adozione di meccanismi automatici di filtraggio, indicizzazione, selezione o organizzazione dei contenuti, i quali comproverebbero, in capo all'ISP, un potere di controllo *ex ante* dei materiali da memorizzarsi, tanto che la pubblicazione in rete non sia automatica ma passi, necessariamente, da un'azione del *provider* stesso, o quest'ultimo intervenga direttamente sui contenuti, modificandoli o manipolandoli.[58]

Si pensi, ad esempio, ai casi di *blog*, *newsletter* o *forum* in cui i messaggi, magari a contenuto diffamatorio, sono inviati al moderatore che decide se diffonderli ed eventualmente con quale contenuto ovvero dell'ISP che, in concorso col gestore di un sito di *e-commerce,* agevola la pubblicazione sulla pagina web di offerte di vendita di beni ricomprendenti altresì merce con marchi contraffatti *ex* art. 473 c.p.

Volgendo lo sguardo più strettamente al tema del diritto d'autore, le fattispecie ipotizzabili in astratto sono plurime: si pensi, ad esempio, al caso, tutt'altro che infrequente, del fornitore di servizi di *hosting* che ricavi un lucro dalla messa a disposizione di piattaforme online costituite appositamente per l'*upload* e la non autorizzata diffusione *in streaming* di opere digitali protette. Ancora, vi è chi ha ipotizzato una responsabilità per concorso *ex* art. 110 c.p. del *provider* che indicizzi i dati riconducibili alle opere digitali protette o consenta il loro *upload* attraverso le sue strutture, che potrebbe concretizzarsi nel mettere a disposizione link, software, opere multimediali in

[58] Si v. INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?*; TOSI E., *L'evoluzione della responsabilità civile dell'Internet Service Provider passivo e attivo;* PICOTTI L., *La responsabilità penale dei service-providers in Italia,* il quale contempla la responsabilità *ex* art. 110 c.p. del *provider* che "*addirittura inserisca i dati illeciti nel circuito comunicativo, dopo un vaglio contenutistico (ad es. in newsgroups personalmente moderati od in mailing-list da lui stesso compilate)";* BARTOLI R., *Brevi considerazioni sulla responsabilità penale dell'Internet Service Provider,* 605 ss., il quale pone l'accento sull'importanza, ai fini dell'individuazione di una responsabilità per concorso attivo dell'ISP, del prevalente contesto eventualmente automatizzato in cui la condotta illecita si realizza: sicché se il totale automatismo si fa coincidere con l'assenza di un comportamento umano previamente finalizzato a legarsi al comportamento dell'utente, la responsabilità dell'ISP potrà essere esclusa qualora siano stati predisposti dispositivi la cui operatività, pur agevolando e migliorando la trasmissione delle informazioni, si basa su meccanismi predefiniti rispetto all'attività dell'utente ovvero affermata quando i nuovi meccanismi si legano a un'attività dell'utente preesistente agli stessi; BACCIN A., *Responsabilità penale dell'Internet Service Provider e concorso degli algoritmi negli illeciti online: il caso Force v. Facebook,* Sistema Penale, 7 maggio 2020, 96 ss.

streaming e informazioni utili alla fruizione non autorizzata di un'opera dell'ingegno, eventualmente a scopo di lucro.[59]
In tali ipotesi potrebbero rinvenirsi gli estremi di una responsabilità commissiva concorsuale, in quanto il fornitore ha contribuito a mettere a disposizione del pubblico l'opera protetta, immettendola in un sistema di reti telematiche. In tal caso, laddove si accerti che vi sia stata un'effettiva agevolazione dell'indebita circolazione dell'opera ovvero la cooperazione dolosa nell'immissione della stessa in un sistema di reti telematiche, a carico dell'ISP si potrebbero configurare i delitti di cui agli artt. 171 c. 1 lett. A) e A-*bis),* 171 *bis,* nel caso in cui l'opera digitale *de quo* sia costituita da un programma per elaboratore o da una banca di dati online, ovvero ancora diverse tra le plurime fattispecie di cui all'art. 171 *ter* c. 1 e c. 2 L. Aut.
Inoltre, non può certamente escludersi che il fornitore attivo potrebbe anche contribuire alla commercializzazione o comunicazione online, se non anche alla pubblicizzazione o al noleggio, o alla detenzione per scopi commerciali di componenti o servizi che abbiano la finalità o l'uso commerciale di eludere misure tecniche di protezione o siano progettati, prodotto o adattati con il fine di rendere possibile l'elusione di tali misure, sì da ipotizzare nei suoi confronti un concorso attivo nel reato di cui all'art. 171 *ter* lett. F-*bis* L. Aut.
In ogni caso, sarà pur sempre necessario accertare che il contributo causale offerto dall'ISP, all'interno dell'*iter* esecutivo, emerga quale indispensabile anello causale, quantomeno agevolatore, nell'immissione in rete del materiale protetto o in altra condotta rilevante ai sensi della L. 633/1941.

4.2. *Segue:* Gli interventi giurisprudenziali in merito alla responsabilità concorsuale dell'*hosting provider* "attivo" per i delitti contro il diritto d'autore nella società dell'informazione.

Oltre che in letteratura, il tema della responsabilità concorsuale del fornitore di servizi digitali *ex* art. 110 c.p. per la messa in circolazione nella rete internet di opere protette dal diritto d'autore senza averne diritto è stato oggetto di una serie di pronunce della giurisprudenza di legittimità che, considerata anche la loro portata mediatica, possono ritenersi senza dubbio dei veri e propri *leading cases* in materia.
Come noto, possono considerarsi all'ordine del giorno i provvedimenti dell'autorità giudiziaria, sia Pubblici Ministeri che Giudici per le Indagini Preliminari, che dispongono sequestri ed oscuramenti di siti web, a finalità tanto probatoria quanto cautelare, al fine di contrastare la proliferazione di spazi telematici finalizzati alla condivisione, alla fruizione e al *download* di

[59] Per tutti FLOR R., *La tutela penale dei diritti d'autore e connessi,* 1159 ss.; si v. anche ERCOLANI S., *Il diritto d'autore e i diritti connessi. La legge n. 633/1941 dopo l'attuazione della direttiva n. 2001/29/CE,* 376 ss.

opere digitali senza l'autorizzazione dei titolari delle privative d'autore sulle medesime.
Proprio nell'ambito di questi procedimenti si inserisce la nota sentenza della Cassazione[60] che, in sede cautelare, si è pronunciata in merito al sequestro preventivo disposto sulla piattaforma svedese di *sharing* nota coma "*The Pirate Bay*": tale pronuncia, risulta, infatti, centrale nel panorama ermeneutico della responsabilità per concorso *ex* art. 110 c.p. degli *hosting providers* gestori di siti internet, e fornisce altresì utili spunti, anche tecnici, per comprendere lo *status* giuridico delle reti *peer-to-peer* e delle condotte penalmente rilevanti che possono aver luogo al loro interno.
Il sito "www.thepiratebay.org", infatti, sul modello dettato dai *case studies* Napster e Peppermint, consentiva lo scambio di materiale protetto da diritto d'autore mediante il ricorso a protocolli *peer-to-peer*. Come già evidenziato in precedenza, tali sistemi consentono la condivisione di file audiovisivi mediante l'interconnessione tra utenti, i quali sono al contempo fornitori e fruitori dei contenuti scambiati. In tale complessa architettura, ogni utilizzatore ha pari grado ed acquista tanto un ruolo passivo (attività di *download*), quanto un ruolo attivo (attività di *upload*) nello scambio dei contenuti digitali.
In breve, la vicenda trae origine dal sequestro preventivo disposto dal Giudice per le Indagini Preliminari di Bergamo verso un sito web, il cui gestore risultava indagato per il reato di cui all'art. 171 *ter* c. 2 lett. A *bis* L. Aut.[61], rispetto al quale aveva stabilito un oscuramento realizzato mediante l'ingiunzione a tutti gli Internet Provider italiani di predisporre il blocco IP e DNS del sito svedese, conformemente a quanto disposto dalla normativa sull'*e-commerce*.
Dopo l'annullamento dell'ordinanza del G.I.P. da parte del Tribunale del Riesame, con una motivazione assai peculiare cui si rinvia in nota[62], la

[60] Cfr. Cass. Pen. Sez. III, n. 49437 del 23/12/2009, commentata esaustivamente da MERLA F., "*Diffusione abusiva di opere in internet e sequestro preventivo del sito web: il caso "The Pirate Bay"*", in Diritto dell'informazione e dell'informatica, 3/2010, 448 ss.
[61] Ai sensi della norma citata, "*è punito con la reclusione da uno a quattro anni e con la multa da cinque a trenta milioni di lire chiunque: a-bis) in violazione dell'articolo 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa*".
[62] Si riporta il relativo passaggio della pronuncia: "*il tribunale riteneva la sussistenza del fumus delicti, alla luce di quanto evidenziato dalla Guardia di Finanza, che riferiva di un elevatissimo numero di contatti al sito in questione, registrati sul territorio nazionale, che operavano il downloading di opere coperte da diritto d'autore senza averne diritto. Risultava quindi in punto di fatto che gli indagati, attraverso il sito www.thepiratebay.org e con un'innovativa tecnologia informatica di trasferimento di file (cd. peer-to-peer a mezzo di file torrent), mettevano a disposizione del pubblico*

questione veniva infine sottoposta all'esame della Suprema Corte, che, per quel che interessa in questa sede, individuava i caratteri minimi che la condotta dell'*hosting provider* deve possedere per essere penalmente rilevante *ex* art. 110 c.p. nel caso in cui metta in comunicazione utenti che compiono un'illecita attività di *uploading*.

Orbene, dopo una prima disamina tecnica delle reti *peer-to-peer,* la Corte rilevava che, in tali sistemi, atteso che la diffusione dell'opera protetta non avviene da un server centrale verso una periferia di utenti, bensì da utente *uploader* ad altri utenti riceventi, il reato di illecita diffusione di materiale coperto dal diritto d'autore è da ascriversi all'utente che carica l'opera sul sito a scopo di lucro (ravvisato, nel caso in esame, dagli introiti delle inserzioni pubblicitarie a pagamento).

Successivamente, i giudici di legittimità si soffermavano sulla posizione della pagina web che mette in comunicazione gli utenti che, in via principale, commettono un delitto contro la proprietà intellettuale.

In via generale, osserva la Corte, "*se il sito web si limitasse a mettere a disposizione il protocollo di comunicazione (quale quello peer-to-peer) per consentire la condivisione di file, contenenti l'opera coperta da diritto d'autore,*

---

della rete Internet opere dell'ingegno protette; condotta questa riconducibile a quella tipizzata nell'art. 171 ter, comma 2, lett. a bis), citato. Il tribunale inoltre riconosceva sussistere anche il periculum, osservando che l'elevatissimo numero di connessioni rilevate induceva a ritenere l'attualità della condotta del delitto ipotizzato.

Osservava poi in diritto che le misure cautelari - e segnatamente i sequestri - secondo l'ordinamento processuale penale hanno carattere di numerus clausus; che di conseguenza non è giuridicamente possibile emettere un sequestro preventivo al di fuori delle ipotesi nominate per le quali l'istituto è previsto; che il sequestro preventivo ha una evidente natura reale, in quanto si realizza con l'apposizione di un vincolo di indisponibilità sulla res, sottraendo il bene alla libera disponibilità di chiunque; che dunque l'ambito di incidenza del sequestro preventivo deve essere ristretto alla effettiva apprensione della cosa oggetto del provvedimento.

Invece nella specie - riteneva il tribunale - la censurata ordinanza del g.i.p. aveva il contenuto di un ordine imposto dall'Autorità Giudiziaria a soggetti (allo stato) estranei al reato, volto ad inibire, mediante la collaborazione degli stessi, ogni collegamento al sito web in questione da parte di terze persone. Tale misura cautelare, seppur astrattamente in linea con la previsione del D.Lgs. n. 70 del 2003, artt. 14 e 15, si risolveva in una inibitoria atipica, che spostava l'ambito di incidenza del provvedimento da quello reale, proprio del sequestro preventivo, a quello obbligatorio, in quanto indirizzato a soggetti determinati (i cd. provider), ai quali veniva ordinato di conformare la propria condotta (ossia di non fornire la propria prestazione), al fine di ottenere l'ulteriore e indiretto risultato di impedire connessioni al sito in questione.

In conclusione riteneva il tribunale che l'utilizzo del provvedimento cautelare di cui all'art. 321 c.p.p., quale inibitoria di attività, non poteva essere condiviso, in quanto produceva l'effetto di sovvertirne natura e funzione, di talchè il sequestro doveva essere annullato in quanto illegittimo".

ed il loro trasferimento tra utenti, il titolare del sito stesso sarebbe in realtà estraneo al reato".
Diversamente, se l'*host* del sito realizza anche un'attività di indicizzazione delle informazioni che gli vengono dagli utenti autori degli *"uploadings"* illeciti, sicchè queste informazioni (*rectius,* le chiavi per accedere al materiale protetto), essenziali perchè gli utenti possano orientarsi chiedendo il downloading di quell'opera piuttosto che un'altra, sono in tal modo elaborate e rese disponibili nel sito (ad esempio a mezzo di un motore di ricerca o con delle liste indicizzate), il sito cessa di essere un mero "corriere" che organizza il trasporto dei dati.[63]
In questo caso, infatti, la piattaforma online pone in essere quel *quid pluris* che rende disponibile all'utenza del sito anche una indicizzazione costantemente aggiornata che consente di percepire il contenuto dei file suscettibili di trasferimento. A quel punto, pertanto, l'attività di trasporto dei file non è più "agnostica", ma si caratterizza come trasporto di dati contenenti

[63] Proseguendo nella parte motiva, la Corte rileva che *"la tecnologia peer-to-peer decentra sì l'uploading (la diffusione in rete dell'opera), ma non ha anche l'effetto, per così dire, di decentrare l'illegalità della diffusione dell'opera coperta da diritto d'autore senza averne diritto. Rimane comunque un apporto del centro (ossia del titolare del sito web) a ciò che fa la periferia (gli utenti del servizio informatico che, utilizzando quanto reso disponibile nel sito web, scaricano l'opera protetta dal diritto d'autore), apporto che, nel nostro ordinamento giuridico, consente l'imputazione a titolo di concorso nel reato previsto dal cit. art. 171 ter, comma 2, lett. a bis). Se poi si considerano in particolare più sofisticate tecnologie di tale trasferimento di file - quale quella che frammenta l'opera in modo da coinvolgere più utenti nell'attività di uploading (a mezzo dei cd. file torrent) - si ha in realtà che, sotto il profilo giuridico appena considerato, non cambia nulla. La diffusione dell'opera coperta da diritto d'autore avviene sempre da utente ad utente tramite un più sofisticato protocollo peer-to-peer che, frammentando l'attività di uploading, ha l'effetto di velocizzarla e di evitare le "code" di attesa nel caso in cui tale attività sia operata da un unico utente. Questa possibile frammentazione dell'attività di uploading comporta che la messa in rete dell'opera è riferibile non più ad un determinato utente, ma ad una pluralità di essi che concorrono tutti diffondendo una parte dell'opera coperta da diritto d'autore. Portando al limite questa frammentazione si può anche ipotizzare che il singolo utente diffonda un frammento dell'opera che, preso in sè, non sia sufficientemente significativo sotto il profilo strettamente giuridico, sì da non potersi considerare di per sè solo coperto da diritto d'autore. Ma, ricomponendo i frammenti secondo le istruzioni di tracciamento che sono nel sito* web, si ha il trasferimento dell'opera intera (o di parti di essa), la cui diffusione è ascrivibile innanzi tutto ai singoli utenti. Mentre l'attività di indicizzazione e di tracciamento, che è essenziale perchè gli utenti possano operare il trasferimento dell'opera (che in tal *caso va da una pluralità di utenti autori dell'uploading verso una potenziale pluralità di utenti ricettori del downloading) è ascrivibile al (gestore del) sito web e quindi rimane l'imputabilità a titolo di concorso nel reato di cui all'art. 171 ter, comma 2, lett. a-bis)*".

materiale coperto da diritto d'autore. Ed allora, benché lo scambio dei file avvenga da utente ad utente, l'attività del sito web (al quale è riferibile il protocollo di trasferimento e l'indicizzazione di dati essenziali) diventa quella che consente ciò e pertanto c'è un apporto causale a tale condotta: è, di conseguenza, con il ricorrere dei citati presupposti che la condotta del gestore del sito può essere inquadrata in una partecipazione imputabile a titolo di concorso di persone *ex* art. 110 c.p.
Benché le conclusioni della sentenza "*Pirate Bay*" possano definirsi ad oggi le linee guida per la materia della responsabilità concorsuale degli *hosting provider* attivi per i reati di cui alla L. 633/1941, già in precedenza la Corte di Cassazione ebbe ad intervenire sul tema, con un'altra sentenza rilevante sia per le conclusioni raggiunte dal collegio che per le critiche cui è andata incontro[64].
Come da prassi, nell'ambito di un procedimento per il reato di cui all'art. 171 c. 1 lett. A *bis)* L. Aut., il caso traeva nuovamente origine dalla richiesta di sequestro di un sito internet che permetteva ai propri utenti, fornendo il necessario link a server cinesi e il software per lo streaming, di vedere le partite del campionato di calcio italiano, coperte da esclusiva Sky, grazie alla diffusione in internet compiuta dalla tv cinese che aveva acquistato la licenza per la diffusione locale.
Atteso che il Giudice per le indagini preliminari non convalidava il sequestro, il Pubblico Ministero proponeva appello, anch'esso respinto dal Tribunale del Riesame. A sostegno delle proprie conclusioni, il Tribunale riteneva insussistente il *fumus* del delitto contestato in quanto accertava che, mediante una normale connessione via internet un numero imprecisato di utenti riuscisse a vedere le partite trasmessa da Sky non grazie all'elusione delle misure tecnologiche predisposte dalla società, ma perchè le partite erano immesse in rete da alcune emittenti cinesi che avevano acquistato dalla stessa Sky il diritto di trasmetterle localmente. Gli indagati italiani avevano facilitato l'accesso a tale prodotto con la sola diffusione di informazioni e la predisposizione di un link che permetteva il collegamento diretto ai server cinesi. Tale condotta, a parere del Tribunale, non era in grado di ricondursi al contestato illecito, in quanto la modalità con la quale deve avvenire la diffusione dell'opera, affinchè potesse ritenersi integrato il reato di cui all'art. 171 *ter* c. 1 lett. A *bis)* L. Aut., consiste nella immissione in rete con una connessione di qualsiasi genere: nel caso in esame, gli indagati si erano limitati a diffondere in via telematica un prodotto che già altri avevano immesso e la condotta di agevolazione alla consultazione dei siti avveniva in un momento successivo al perfezionamento del reato.

[64] Cfr. Cass. pen., Sez. III, n. 33945 del 04/07/2006, con nota di SCOPINARO L., *Rilevanza penale della divulgazione via web di programmi TV – commento,* in Diritto Penale e Processo*,* 5/2007, 651 ss.

Senonché, in accoglimento del ricorso proposto dal Pubblico Ministero, la Suprema Corte ribaltava la prospettiva adottata dai giudici del merito, ammettendo la configurabilità di un concorso attivo dei gestori del sito web italiano che avevano messo a disposizione degli utenti le informazioni ed i mezzi tecnici attraverso i quali era possibile installare sul proprio dispositivo i software necessari alla visione delle partite di calcio sulle quali Sky vantava un diritto di esclusiva.

A fondamento della propria statuizione, la Corte rilevava che "*è innegabile che gli attuali indagati hanno agevolato, attraverso un sistema di guida on line, la connessione e facilitato la sincronizzazione con l'evento sportivo; senza la attività degli indagati, non ci sarebbe stata, o si sarebbe verificata in misura minore, la diffusione delle opere tutelate. Le informazioni sul link e sulle modalità per la visione delle partite in Italia, per raggiungere il loro obiettivo, devono essere state inoltrate agli utenti in epoca antecedente alla immissione delle trasmissioni in via telematica; tale rilievo, se puntuale in fatto, comporta come conseguenza che, in base alle generali norme sul concorso nel reato, gli indagati, pur non avendo compiuto l'azione tipica, hanno posto in essere una condotta consapevole avente efficienza causale sulla lesione del bene tutelato*"[65].

La pronuncia in commento, a parere di chi scrive, fornisce uno spunto per una breve riflessione conclusiva in merito alla configurabilità della responsabilità concorsuale *ex* art. 110 c.p. dell'*hosting provider* e alle criticità del tema.

I delitti in materia di diritto d'autore sono, per la maggior parte, reati di mera a condotta a consumazione istantanea che si configurano con condotte quali la diffusione, l'immissione in reti telematiche e la trasmissione al pubblico di opere protette, sicchè, una volta realizzato il fatto tipico, qualsiasi cooperazione successiva nel reato da parte dell'ISP dovrebbe risolversi in un *post factum* irrilevante ai fini del concorso nel reato a monte, ferme restando le specifiche ipotesi di reato in cui può sussumersi detta cooperazione posteriore.

Ciò premesso, se nella sentenza "*Pirate Bay*" la responsabilità *ex* art. 110 c.p. del gestore del sito è stata correttamente fondata sulla partecipazione attiva del medesimo agli illeciti realizzati dagli utenti della rete *peer-to-peer*, manifestatasi mediante l'indicizzazione delle opere caricate dai medesimi

[65] Tale contributo, secondo i giudici di legittimità, risulta infatti sufficiente a corrispondere gli estremi del concorso *ex* art. 110 c.p., in quanto "*l'attività costitutiva del concorso può essere individuata in qualsiasi comportamento che fornisca un apprezzabile contributo alla ideazione, organizzazione ed esecuzione del reato; non è necessario un previo accordo diretto alla causazione dell'evento, ben potendo il concorso esplicarsi in una condotta estemporanea, sopravvenuta a sostegno della azione di terzi anche alla insaputa degli altri agenti*".

contestualmente al loro *upload,* nella pronuncia appena esaminata la Suprema Corte ha di fatto esteso la responsabilità per concorso dei gestori del sito per fatti cronologicamente successivi alla diffusione, da parte dei server cinesi, delle partite di calcio.
È evidente che tale approccio presta il fianco a critiche: il fatto di avvisare gli utenti della rete che in futuro verrà messa a disposizione da altri soggetti un'opera dell'ingegno protetta, indicandone le modalità di fruizione, non contribuisce in alcun modo all'immissione in rete della stessa, potendo al più, come già rilevato, agevolarne l'accesso.
Ed invero, i gestori del sito non incidevano sull'immissione in rete delle partite di calcio, che avveniva per opera del sito cinese, ma si limitavano, *ex post,* ad agevolarne la visione agli utenti che, indipendentemente dal contributo prestato degli indagati, avrebbero potuto comunque accedere ai server cinesi.[66]
In tal caso, è pacifico che, se un reato vi era, questo si era già consumato con la diffusione dell'opera televisiva su internet prima ancora che i gestori del sito italiano intervenissero con la pubblicizzazione di link diretti a fornire un collegamento con l'opera stessa.[67]
La sentenza *de quo* dimostra, pertanto, quanto alti siano i rischi di interpretazioni erronee nell'*iter* di accertamento della responsabilità per concorso attivo dell'*Internet Provider,* anche in circostanze assai frequenti nella fruizione di opere dell'ingegno in formato digitale, e quanto le esigenze punitive di tali soggetti, ancorché giustificate, possano adombrare una distorsione dei principi generali del diritto penale.

---

[66] Sulla base di tale assunto, nel caso di specie non si sarebbe neppure potuto contestare agli indagati il reato di cui alla lett. F-*bis*) dell'art. 171 *ter* L. Aut., che punisce "*chiunque fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102 quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure*". Ed invero, atteso che gli utenti avrebbero potuto in ogni caso lecitamente accedere alle opere televisive diffuse dai server cinesi, non v'era alcuna misura di protezione che i link diffusi dagli indagati avrebbe potuto aggirare.
[67] Critico verso la decisione della Corte è INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?,* il quale osserva che per l'affermazione della penale rilevanza della condotta dei gestori del sito italiano, nel caso di specie, si dovrebbe ipotizzare una fattispecie di parte speciale che incrimini la pubblicizzazione (ed in tal caso l'ISP sarebbe autore diretto del reato) ovvero il godimento senza titolo dell'opera coperta dal diritto d'autore, per cui il *provider* concorrerebbe nell'illecito penale dell'utente che accede al sito.

4.3. L'ISP "controllore": il concorso per omissione e la posizione di garanzia dell'*Internet Provider*

Il secondo paradigma possibile di criminalizzazione dell'ISP, ed in particolare del *provider* c.d. "passivo", trova il suo nucleo fondante nell'individuazione di una posizione di garanzia in capo al medesimo, volta ad impedire i reati realizzati dagli utenti della rete.

In tal senso, il *provider* dovrà ritenersi responsabile penalmente per il venir meno agli obblighi connessi a detta posizione di garanzia e per non aver impedito l'illecita diffusione e trasmissione di opere dell'ingegno negli ambienti di rete da lui amministrati. Si comprende facilmente, pertanto, come l'"evento" che il *provider* sarebbe chiamato ad impedire corrisponda al delitto commesso dall'*uploader* del contenuto protetto: del resto, atteso che i reati in materia di diritto d'autore si manifestano come fattispecie di mera condotta, non sarebbe ravvisabile già a monte un dovere di impedire un evento che, ai fini della configurazione del reato, non è neppure richiesto.

Stante l'assenza nel panorama normativo in materia di diritto d'autore di una fattispecie tipica di reato omissivo, tale aspetto dovrà essere analizzato esclusivamente sotto il profilo dei reati omissivi impropri e della generale clausola di equivalenza di cui all'art. 40 c. 2 c.p.

Ed invero, sembra ormai assodata la non estendibilità all'ISP della disciplina prevista dagli artt. 57 e 57 *bis* c.p. per le ipotesi di responsabilità del direttore e del vicedirettore concernenti la carta stampata, cui non fanno eccezione le sparute pronunce giurisprudenziali che hanno riconosciuto la responsabilità penale in capo al direttore della (sola) testata giornalistica *online*[68], attesa la sostanziale diversità intercorrente tra questo soggetto e l'intermediario che mette a disposizione le risorse informatiche, telematiche e di rete per la diffusione del periodico in formato digitale.[69]

Archiviata la percorribilità di un'incriminazione ex art. 57 c.p., quanto ancora resta da riverificare è quindi l'opzione ermeneutica che vorrebbe addebitare

---

[68] Cfr. Cass. Pen. Sez. V, n. 1275 del 23/10/2018, con nota di MAURI R., *Applicabile l'art. 57 c.p. al direttore del quotidiano online: un revirement giurisprudenziale della Cassazione, di problematica compatibilità con il divieto di analogia,* in Diritto Penale Contemporaneo, 28 febbraio 2019.

[69] Si v. in particolare BARTOLI R., *Brevi considerazioni sulla responsabilità penale dell'Internet Service Provider,* 602; FLOR R., *La tutela penale dei diritti d'autore e connessi,* 1160; INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?;* MANNA A., DI FLORIO M., *Riservatezza e diritto alla privacy: in particolare, la responsabilità per omissionem dell'Internet Provider,* 910 ss. Sul versante giurisprudenziale si possono richiamare le sentenze Cass. pen., sez. V, n. 35511 del 16/07/2010 e la successiva Cass. Pen. Sez. V, n. 44126 del 28/10/2011, che hanno escluso l'applicazione analogica dell'art. 57 c.p. non solo ai direttori dei periodici *on line*, ma anche agli *access provider*, ai *service provider*, agli *hosting provider* e ai coordinatori di *blog* e *forum*.

al provider una responsabilità per omesso impedimento dell'evento *ex* art. 40 c. 2 c.p.
Il tema è stato più volte affrontato, ancor prima che dalla giurisprudenza, da autorevole dottrina, la quale, pressoché all'unanimità, ha escluso la configurabilità tanto di una posizione di garanzia o di protezione in capo all'ISP quanto di un qualche obbligo giuridico di impedire la commissione dei reati da parte degli utenti della rete.
Le ragioni che osterebbero a giustificare un rimprovero per omesso impedimento di illeciti commessi da terzi nei confronti del fornitore di servizi internet, ben rappresentate dal concetto di "fuoco di sbarramento"[70], sono molteplici, e attengono sia a motivi di diritto che di fatto.
Quanto ai profili giuridici, è di immediata percezione come il legislatore non soltanto non si sia preoccupato di prevedere una norma che fondi un generale obbligo di impedimento dei reati degli utenti contro la proprietà intellettuale, ma abbia altresì espressamente sancito, proprio nella disciplina normativa sulla responsabilità dei *providers,* l'assenza di qualunque obbligo di controllo preventivo rispetto ai contenuti immessi online dai fruitori dei servizi di rete: ed invero, a mente dell'art. 17 del D.Lgs. 70/2003 "*il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, nè ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite*"; di analogo tenore appare l'art. 17 della Direttiva 790 ed il corrispondente art. 102 *septies* L. Aut. introdotto con il D.Lgs. 177/2021, che sanciscono l'insussistenza di un obbligo generale di sorveglianza in capo al prestatore di servizi di condivisione online.
Inoltre, è stato rilevato che un obbligo di impedimento non potrebbe essere ricavato neppure dagli obblighi di rimozione degli effetti derivanti da reati già realizzati previsti dagli artt. 14 c. 3, 15 c. 2 e 16 c. 3 d.lgs 70/2003, né dagli obblighi di segnalazione di illeciti sanciti dall'art. 17 c. 2 del citato decreto: ed infatti, questi ultimi hanno finalità diverse, orientate alla collaborazione con le autorità, e presuppongono, in ogni caso, attività illecite già verificatesi.[71] In merito a tale considerazione, tuttavia, non manca chi ammette la configurabilità di una responsabilità omissiva del *provider* fondata sull'omessa rimozione, a seguito di segnalazione dell'autorità competente, dei contenuti caricati senza autorizzazione dei titolari dei diritti di proprietà intellettuale sui medesimi, in quanto i relativi obblighi fanno riferimento a "violazioni" ed "attività illecite" e non già a reati consumati. Di conseguenza,

[70] Il termine è di INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?*
[71] V. BARTOLI R., *Brevi considerazioni sulla responsabilità penale dell'Internet Service Provider,* 603; INGRASSIA A., *Responsabilità penale degli internet service provider: attualità e prospettiva,* Diritto Penale e Processo, 12/2017, 1626 ss.

le suddette norme che regolano la procedura di *notice and take down* che l'ISP deve attivare su ordine dell'autorità individuano semplici situazioni di rischio che possono anche avere rilevanza penale, e quindi dare origine ad una posizione di garanzia *ex lege* se non affrontate, ma che non necessariamente costituiscono un delitto già perfezionatosi.[72]

Senonché, a sfavore del riconoscimento di una posizione di garanzia per come, seppur autorevolmente, prospettato poc'anzi, giocherebbe altresì la circostanza per cui questo impatterebbe anche sul difetto di un nesso di causalità tra omissione ed evento. La gran parte degli illeciti commessi su internet, ed in particolar modo i delitti contro il diritto d'autore, risulta infatti riconducibile alla *species* dei reati a consumazione istantanea: di conseguenza, non potendo rispondere, almeno in astratto, a titolo di responsabilità omissiva per non aver impedito il protrarsi degli effetti del reato[73], l'inottemperanza ad un obbligo di intervento del *provider* non avrebbe in ogni caso alcuna efficacia causale, atteso che il reato si è già consumato nel momento stesso in cui la situazione tipizzata dalla fattispecie penale si manifesta facendo sorgere per l'ISP l'obbligo di attivarsi; obbligo la cui violazione potrà eventualmente dar luogo ad ipotesi di reato autonome e non ascrivili a titolo di responsabilità omissiva.[74]

Oltre alla mancanza *ex lege* di una posizione di garanzia, in capo al *provider* difetterebbero, dal punto di vista giuridico ancor prima che tecnico, anche i concreti poteri impeditivi degli eventi[75], *rectius* dei reati commessi in rete,

---

[72] La tesi in esame è stata elaborata da FLOR R., *La tutela penale dei diritti d'autore e connessi,* 1162.

[73] Sul punto deve tuttavia richiamarsi la sentenza Cass. Pen. Sez. V, n. 59496 del 27/12/2016, che, con un'interpretazione innovativa, ha ritenuto responsabile *ex* art. 40 c. 2 c.p. un *Internet Provider* che aveva omesso di rimuovere un contenuto diffamatorio pubblicato sulla *community* del sito da lui gestito sul presupposto delll'asserita omissione dell'obbligo di impedire non tanto il reato a monte, quanto il protrarsi dei suoi effetti. È evidente che la S.C. abbia, nel caso di specie, configurato una responsabilità dell'ISP per omissione argomentando che gli illeciti che avvengono su internet sono illeciti permanente, e connotati dalla permanente ritrasmissione del dato, senza la possibilità del danneggiato di impedirlo. Sul punto, MANNA A., DI FLORIO M., *Riservatezza e diritto alla privacy: in particolare, la responsabilità per omissionem dell'Internet Provider,* osservano che siffatta elaborazione, per quanto originale, non chiarisce, tuttavia, da dove derivi tale obbligo di impedire gli effetti del reato; tale indeterminatezza della fonte giuridica costituisce quindi un limite, a fronte del prevalentemente orientamento per cui le fonti della posizione di garanzia sono esclusivamente la legge, il contratto e la precedente attività pericolosa.

[74] V. STEA G., *La responsabilità penale dell'Internet Provider,* 4 ss.; INGRASSIA A., *Responsabilità penale degli internet service provider: attualità e prospettiva,* 1627.

[75] Così INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?;* BARTOLI R., *Brevi considerazioni sulla responsabilità penale dell'Internet*

requisito indispensabile per poter fondare ogni rimprovero basato sull'applicazione dell'art. 40 c. 2 c.p.: il quadro normativo di cui agli articoli 14 ss., D.Lgs. n. 70 del 2003, consente, infatti all'ISP di impedire l'accesso ai dati da altri immessi e di rimuoverli solo a seguito di richiesta dell'autorità od ove tale materiale risulta manifestamente illecito.
Né parrebbe idonea a fondare responsabilità *ex* art. 40 c.2 c.p. nei confronti dell'ISP la tesi di una responsabilità nascente da obblighi di impedimento riconducibili a precedente attività pericolosa. È stato infatti osservato da attenta dottrina che non potrebbe definirsi tale l'usuale predisposizione di un accesso ad Internet, né l'offerta di spazi su supporti collegati in rete o di servizi in detto ambito.
Ed invero, l'astratta possibilità che si commettano reati online non può rendere, per ciò solo, pericolosa la fondamentale attività di concessione di servizi agli utenti, che necessitano di accedere alle informazioni circolanti in rete non tanto per porre in essere condotte illecite, ma per soddisfare importanti interessi della propria vita sociale, professionale e privata.[76]
Maggiori aperture sono invece state manifestate da voci isolate, seppur autorevoli, rispetto ad una posizione di garanzia nascente dal contratto tra l'ISP e i titolari di diritti d'autore, quale ad esempio quello relativo all'esclusiva di distribuzione online di specifiche opere dell'ingegno: tale accordo, infatti, nella misura in cui preveda la tutela di determinati interessi che possono essere minacciati attraverso l'uso della rete o delle strutture tecniche ed organizzative dell'ISP, può assumere rilievo ai fini della configurabilità posizione di garanzia di fonte contrattuale in capo al *provider,* qualora contenga una specifica individuazione del bene giuridico da proteggere e l'assunzione consapevole da parte dell'ISP della funzione di protezione e di controllo sulle condotte illecite degli utenti.[77] È tuttavia evidente che, in simili

Service Provider, 603, , secondo cui l'impossibilità di configurare una responsabilità dell'ISP per omesso impedimento *ex ante* del reato non è una questione soltanto tecnica (impossibilità di controllo o eccessiva dispendiosità di tale controllo), ma sostanziale, nel senso che il *provider* non ha alcuna relazione con la fonte del pericolo, ossia con l'utente, né sono individuabili beni da proteggere particolarmente vulnerabili, così come non esistono in capo allo stesso veri e propri poteri giuridici di interferenza o inibizione rispetto alla condotta dell'autore del reato.

[76] Si v. sul punto PICOTTI L., *Fondamento e limiti della responsabilità penale dei service-provider in internet,* 381 ss; INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?;* FLOR R., *La tutela penale dei diritti d'autore e connessi,* 1160; MANNA A., DI FLORIO M., *Riservatezza e diritto alla privacy: in particolare, la responsabilità per omissionem dell'Internet Provider,* 912 ss., secondo cui la "*precedente attività pericolosa non pu essere considerata quella svolta dal gestore del sito che, al contrario, costituisce espressione della libertà di manifestazione del pensiero (ex art. 21 Cost.)*".

[77] Si v. sul punto FLOR R., *La tutela penale dei diritti d'autore e connessi,* 1162.

ipotesi, non potendo trarre un principio generalmente valido per tutte le relazioni contrattuali tra ISP e titolare dei diritti sulle opere dell'ingegno, occorrerà procedere ad una disamina, caso per caso, delle clausole di ogni singolo accordo.
Oltre ai limiti giuridici, sono stati evidenziati anche i limiti tecnici e "di fatto" che precluderebbero la sussistenza di una posizione di garanzia in capo all'ISP. Mancherebbe, infatti, in capo al *provider,* la concreta possibilità di esercitare un efficace controllo generale sul traffico telematico e del suo contenuto. Le attività svolte in rete e la mole di informazioni trasmesse nel ciberspazio non rientrerebbero nel normale potere di organizzazione e disposizione del gestore del *network* senza ammettere un'ingerenza di quest'ultimo nella sfera riservata e personale degli utenti.[78]
La mancanza in concreto del potere di controllare le attività degli utenti *ex ante* si potrebbe dedurre inoltre dall'enorme flusso di "*dati che transitano sul o sui servers gestiti da ciascun Provider, essendo oltretutto sempre possibile che la trasmissione di o l'accesso a determinati dati avvengano anche per selezione (automatica o meno) di collegamenti alternativi, in conformità con la struttura aperta (od "anarchica", come è stato detto) di Internet, che non rappresenta alcun unitario sistema centralizzato, ma una possibilità di molteplici connessioni, fra reti e computer diversi, "semplicemente" in grado di scambiarsi dati utilizzando protocolli di trasmissione comuni*".[79]
Peraltro, per quanto autorevole, quest'ultima tesi potrebbe, ad oggi, stridere con lo sviluppo e con l'enorme afflusso di potere acquisito delle grandi piattaforme online e delle c.d. *big tech,* le quali, come testimonia anche il bisogno di intervento espresso dal legislatore europeo con il Digital Service Act, paiono attualmente possedere tutti gli strumenti tecnici ed economici per esercitare un controllo costante e generale sul comportamento tenuto dagli utenti della rete e sull'eventuale materiale non autorizzato da loro caricato negli ambienti telematici.

4.4. *Segue:* Le linee guida dettate dalla sentenza "*Google c. Vividown*"

Le ferree conclusioni dottrinali, ispirate dalla stessa disciplina normativa in vigore, in relazione all'opportunità di configurare una responsabilità penale omissiva del *service provider* sono state ampiamente condivise anche dalla giurisprudenza di legittimità che, con la sentenza nota come "*Google – Vivi Down"*,[80] ha dettato i fondamenti dell'insussistenza, in capo all'*hosting*

[78] Sostiene questa tesi *Ibidem,* 1160.
[79] In questi termini PICOTTI L., *Fondamento e limiti della responsabilità penale dei service-provider in internet,* 380.
[80] Il riferimento è a Cass. Pen. Sez. III, n. 5107 del 17/12/2013, commentata da numerosi autori. Si v. in particolare MANNA A., DI FLORIO M., *Riservatezza e diritto alla privacy: in particolare, la responsabilità per omissionem dell'Internet Provider,* 901 ss.;

provider, in particolare quello c.d. "attivo", di qualsivoglia posizione di garanzia rispetto all'attività in linea degli utenti.
Seppur inerente ad un caso di trattamento illecito di dati personali e non già alla materia del diritto d'autore, a parere di chi scrive la pronuncia in esame, data la sua natura di vero e proprio *leading case* nella disciplina della responsabilità dell'ISP, merita uno sguardo più approfondito.
Come noto, il processo traeva origine dalla pubblicazione, sulla piattaforma *Google-Videos,* di un filmato nel quale uno studente disabile era insultato e maltrattato da tre compagni, mentre un quarto studente riprendeva la scena con il proprio cellulare. Inoltre, nel filmato si faceva riferimento, in maniera diffamatoria, all'associazione "*Vivi Down"*. Dalla diffusione del video, riprodotto e scaricato da un elevato numero di utenti, derivava l'insorgere del procedimento penale nei confronti di alcuni dirigenti della filiale Google Italia per il reato di diffamazione di cui all'art. 595 c.p., contestato ai sensi dell'art. 40 c. 2 c.p., e per il reato di trattamento illecito di dati personali attinenti alla salute del ragazzo ripreso, punito dall'art. 167 D.Lgs. 196/2003.
Nel contesto di tale procedimento si inseriva, in primo grado, la sentenza del Tribunale di Milano del 24 febbraio 2010, che, in primo luogo, escludeva il concorso omissivo nel delitto di diffamazione degli imputati, affermando, già in sede di merito, l'esclusione in capo all'*hosting provider* di un obbligo di impedire reati commessi dagli utenti; tale esclusione, per riprendere quanto illustrato poc'anzi*,* era motivata sia da ragioni giuridiche, in quanto la normativa sul commercio elettronico esclude un obbligo di vigilanza sul contenuto dei materiali diffusi dagli utenti, sia da considerazioni di tipo fattuale, ossia l'impossibilità in concreto di filtrare *ex ante* i contenuti degli *uploaders*.
Per contro, il giudice di prima istanza affermava invece la responsabilità omissiva dell'*Internet Provider* per la violazione dell'art. 167 cod. privacy, fondata non tanto sul mero omesso impedimento, mediante l'uso di strumenti tecnici e di filtraggio, del reato commesso da terzi, bensì sull'omissione di una corretta e puntuale informazione circa il rispetto delle prescrizioni normative concernenti il trattamento dei dati.
Il processo di merito procedeva in appello. In tale sede, con sentenza del 22 dicembre 2012, la Corte confermava l'assenza di una posizione di garanzia in capo all'*hosting provider* e annullava la condanna anche in relazione all'illecito trattamento dei dati personali**.** In particolare, il Giudice di seconde cure qualificava la piattaforma *Google video* come *hosting provider* attivo, ossia

---

INGRASSIA A., *La sentenza della Cassazione sul caso Google,* in Diritto Penale Contemporaneo, 6 febbraio 2014; MACRILLO' A., *Punti fermi della Cassazione sulla responsabilità dell'Internet Provider per il reato ex art. 167, D.Lgs. n. 196/03,* in Giurisprudenza Italiana, n. 8-9, 1agosto 2014.

come fornitore di servizi di rete che, oltre alla memorizzazione delle informazioni degli utenti svolge anche un'attività non neutra, connotata altresì da un possibile finanziamento economico attraverso le inserzioni. Senonchè, anche da tale qualità non discenderebbe, secondo la Corte, alcun obbligo di controllo preventivo in capo al *provider*. Inoltre, il Giudice del gravame rilevava altresì, al fine di escludere la posizione di garanzia nei confronti di Google, che un eventuale obbligo, penalmente sanzionato, di impedire i reati degli utenti non può in ogni caso dedursi dal dovere, in capo all'intermediario, di informare gli *uploader* sui corretti comportamenti da tenere durante l'utilizzo dei servizi di rete: in tal senso, l'unico soggetto responsabile dell'illecito commesso tramite *la piattaforma online* resta, in via autonoma, soltanto l'utente che procede al caricamento del materiale *contra jus*.

I principi affermati dalla Corte d'Appello di Milano venivano integralmente fatti propri e confermati dalla Corte di Cassazione successivamente adita dal Procuratore Generale, nell'ambito di una più ampia attività di coordinamento tra la disciplina sul commercio elettronico e la normativa sulla tutela dei dati personali, per la cui disamina si rinvia a sedi più opportune.[81]

Per quel che qui interessa, può osservarsi che, nel rigettare l'impugnazione, la Cassazione confermava l'assenza di una posizione di garanzia e di obblighi di sorveglianza in capo agli ISP, giacché nessuna disposizione "*prevede che vi sia in capo al provider, sia esso anche un hosting provider*, *un obbligo generale di sorveglianza dei dati immessi da terzi sul sito da lui gestito*"; parimenti, secondo l'interpretazione della Corte, nessuna norma incriminatrice punisce un ipotetico obbligo dei *provider* di ricordare agli utenti di rispettare la legge.

In particolare, il caso esaminato sarebbe ricaduto nella sfera applicativa delle limitazioni di responsabilità dell'*hosting provider* previste dagli artt. 16 e 17 D.Lgs. 70/2003, atteso che l'ISP si era limitato a memorizzare e trasmettere i video inseriti dagli utenti, senza apportare alcun contributo alla determinazione del contenuto del video e alla sua diffusione.[82]

---

[81] V. MACRILLO' A., *Punti fermi della Cassazione sulla responsabilità dell'Internet Provider per il reato ex art. 167, D.Lgs. n. 196/03*

[82] Sul punto, osserva la Corte, "c*irca i responsabili della violazione, deve però ribadirsi che, contrariamente a quanto sostenuto dal ricorrente, questi sono da identificarsi con gli utenti che hanno caricato il video sulla piattaforma Google video e non con i soggetti responsabili per la gestione di tale piattaforma, trattandosi, come già ampiamente visto, di un mero servizio di hosting. Ed è proprio la natura del servizio reso ad escludere anche la fondatezza del secondo dei rilievi svolti dal Procuratore generale nell'ambito del primo motivo di ricorso, non essendo configurabile alcun obbligo generale di controllo in capo ai rappresentanti di Google Italy s.r.l., gestore del servizio stesso*"

Inoltre, in anticipazione del discorso che verrà affrontato nel paragrafo successivo, con la sentenza "*Google – Vivi Down*" la giurisprudenza di legittimità ha avuto modo di soffermarsi direttamente sulla conoscenza che, necessariamente, il *provider* deve possedere rispetto al materiale illecito trasmesso o memorizzato sui propri server, presupposto imprescindibile nell'accertamento di un'eventuale responsabilità penale del fornitore di servizi internet.
Ed invero, oltre a non prevedere espressamente una posizione di garanzia in capo all'ISP rispetto alla prevenzione degli illeciti perpetrati dagli utenti della rete, la normativa sull'*e-commerce* limita ulteriormente la responsabilità del *provider* laddove questi non sia effettivamente a conoscenza del fatto che l'attività o l'informazione proveniente dal *content provider* è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione, ovvero, non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso. Così disponendo, secondo la Corte, il legislatore ha inteso porre quali presupposti della responsabilità del provider proprio la sua effettiva conoscenza dei dati immessi dall'utente e l'eventuale inerzia nella rimozione delle informazioni da lui conosciute come illecite.
Da ciò, pertanto, può dedursi che il legislatore ha inteso far coincidere il potere decisionale sui contenuti provenienti dai singoli fruitori della rete, ivi comprese le opere dell'ingegno digitali, con la capacità di incidere concretamente su tali contenuti, il che non può prescindere dalla conoscenza degli stessi. In altri termini, finchè il materiale illecito è sconosciuto al service provider, questo non può essere chiamato a rispondere della sua illiceità, perchè privo di qualsivoglia potere decisionale sul materiale stesso.
In via generale, sono, dunque gli utenti ad essere responsabili in via principale dell'attività di *uploading* nei servizi di *hosting* e non i gestori che si limitano a fornire tali servizi.
Richiamando le osservazioni dottrinali[83], le statuizioni della Suprema Corte possono sintetizzarsi in tre principi: in primo luogo, non è possibile attribuire all'*hosting provider,* anche se attivo, un generale obbligo di impedire i reati commessi dagli utenti, mancando una norma che fondi l'obbligo giuridico; inoltre, le attività compiute dall'*hosting provider* sui materiali caricati dagli utenti, che non importino un intervento sul contenuto degli stessi o la loro conoscenza, non fanno venir meno le limitazioni di responsabilità previste dagli artt. 16 e 17 D.Lgs. 70/2003; infine, solo dal momento della conoscenza dell'illiceità dei contenuti

[83] Così MANNA A., DI FLORIO M., *Riservatezza e diritto alla privacy: in particolare, la responsabilità per omissionem dell'Internet Provider,* 908 ss.; INGRASSIA A., *La sentenza della Cassazione sul caso Google.*

pubblicati dagli utenti può ipotizzarsi una responsabilità del *provider* connessa ai reati posti in essere dagli utenti, che tuttavia, come meglio si vedrà *infra,* non potrebbe in ogni caso dar luogo ad una contestazione per concorso omissivo *ex* art. 40 c. 2 c.p., essendosi il reato ormai realizzato, bensì a contestazioni aventi ad oggetto fattispecie commissive autonome da individuarsi caso per caso.

4.5. *Actual knowledge* ed elemento soggettivo nell'accertamento della responsabilità penale dell'*Internet Provider.*

Esaminati i requisiti "oggettivi" per la configurabilità, o non configurabilità, di una responsabilità penale *ex* art. 110 c.p. o per omissione dell'ISP, la lettura dell'importante sentenza "*Google – Vivi Down"* pone le premesse per una breve dissertazione relativa all'elemento soggettivo che, tenuto conto della normativa sull'*e-commerce,* dei principi regolanti la materia del dolo di concorso e delle peculiarità tecniche di internet e delle funzioni svolte dai *providers,* appare imprescindibile per una completa trattazione dello statuto penale dei fornitori di servizi di rete per i reati contro la proprietà intellettuale. Come noto, il sistema a tutela del diritto d'autore previsto dalla L. 633/1941, ed in particolar modo quello relativo ai reati di c.d. "pirateria" digitale, è costituito in prevalenza[84] da fattispecie che, fra i loro elementi essenziali, prevedono i requisiti dello scopo di lucro o dell'ingiusto profitto in capo all'autore materiale del reato. In alcune fattispecie, questi ultimi vanno implicitamente ricondotti alla stessa natura commerciale delle condotte previste, quali ad esempio la "diffusione", "vendita" o "messa in commercio" di cui all'articolo 171, c. 1, lett. a) ovvero l'esercizio in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore di cui all'art. 171 *ter* c. 2 lett. b).[85]

---

[84] Tra le ipotesi di reato per le quali non è richiesto il dolo specifico possono richiamarsi le fattispecie "base" meno gravi previste dall'art. 171 L. Aut.; in particolare, potrebbe intraversi un concorso dell'ISP nel caso previsto dalla lett. a) *bis* del primo comma, che punisce chi mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa; tale reato, peraltro, pur configurandosi come delitto è suscettibile di una speciale procedura di oblazione che ne consente l'estinzione dietro pagamento di una somma corrispondente alla metà del massimo della pena stabilita per il reato, sicché nella maggioranza dei casi può ben ritenersi che un eventuale procedimento penale nei confronti dell'ISP sia destinato a concludersi su questa strada e non già con una sentenza di merito.

[85] Curiosamente, non è invece previsto il dolo specifico per il reato di cui all'art. 171 *ter* c. 2 lett. a) che punisce chi "*riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti*

In altri casi, invece, tali elementi vanno a costituire l'elemento soggettivo del dolo specifico, come nel caso dello "scopo di lucro", di cui all'articolo 171-*ter*, c. 1 e c. 2 lett. a) *bis* e del "fine di trarne profitto" di cui all'art. 171 *bis*: in tali casi, la condotta dell'autore è inscindibilmente legata allo scopo cui è tesa, senza che la concreta realizzazione di quest'ultima sia peraltro necessaria al fine della consumazione.
Quale che sia il fine perseguito dall'autore di reati di pirateria online, non può farsi a meno di rilevare, in ossequio al granitico indirizzo giurisprudenziale in merito[86], l'irrilevanza del suddetto fine in capo all'ISP che, attivamente o mediante omissione, fornisce un contributo causale all'attività illecita degli utenti sul web.
In altre parole, nei confronti del *provider* concorrente, ed in specie quello *ex* art. 110 c.p., dovrà accertarsi quantomeno un atteggiamento psicologico verso il fatto di reato qualificabile come dolo generico, ossia, da un lato, come rappresentazione (e volontà) di offrire il proprio contributo all'illecito posto in essere dall'*intraneus* e, dall'altro, come consapevolezza dello scopo mirato da quest'ultimo.
Tale assunto deve leggersi necessariamente in combinato con la normativa sul commercio elettronico (artt. 16 e 17 D.Lgs. 70/2003), che, come più volte anticipato nel corso della presente trattazione, postula, a monte di qualsiasi ricognizione di responsabilità dell'ISP, l'effettiva conoscenza da parte di quest'ultimo dell'illiceità dell'attività compiuta dagli utenti sui suoi server e all'interno delle proprie reti.
La necessità di tale effettiva conoscenza presenta importanti ricadute sia in ambito di responsabilità concorsuale attiva che in materia di concorso *ex* art. 40 c. 2 c.p.
Quanto al concorso *ex* art. 110 c.p., dal quadro normativo tratteggiato dal D.Lgs. 70/2003 può ricavarsi il corollario dell'esclusione di qualsivoglia forma di responsabilità concorsuale dell'ISP ove il suo contributo quale partecipe o coautore non sia sorretto almeno dal dolo diretto.[87]

---

connessi". Ad avviso di chi scrive, premesso che dal tenore letterale del comma sembra essersi in presenza di un reato autonomo e non già di una circostanza aggravante della fattispecie base di cui al primo comma, la differenza in termini di elemento soggettivo richiesto ai fini della configurazione di quest'ultima rispetto all'ipotesi di cui al comma secondo parrebbe ricondursi, alternativamente, da una svista del legislatore ovvero, più verosimilmente, alla volontà di sanzionare penalmente violazioni sistematiche e su larga scala del diritto d'autore anche senza la necessità di uno specifico fine lucrativo.

[86] Cfr. *ex multis* Cass. Pen. Sez. III, n. 19213 del 07/05/2019; Cass. Pen. Sez. V, n. 27141 del 27/03/2018.

[87] Sul punto v. INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?;* di orientamento contrario in merito alla necessaria qualifica

Ed invero, come desumibile dagli artt. 16 e 17 del D.Lgs. 70/2003, il legislatore ha escluso la rilevanza, anche penale, dei contributi offerti dall'ISP, ed in particolare dall'*hosting provider*, alla realizzazione del fatto tipico qualora i medesimi non siano almeno accompagnati, al momento della trasmissione o della memorizzazione dei dati, da una "effettiva conoscenza" del contenuto illecito degli stessi o di fatti e di circostanze che rendono manifesta l'illiceità delle attività compiute dagli utenti.

La nozione di "effettiva conoscenza" presenta alcune incertezze.

Il termine adoperato prima dal legislatore europeo nella Direttiva 31/2000/CE[88] e poi tradotto dai differenti legislatori nazionali parrebbe rimandare all'espressione "*actual knowledge*" contenuta nel §512 del *Digital Millennium Copyright Act* statunitense[89], e che nel nostro ordinamento rimarca, esclusivamente, che non può trattarsi di mera conoscibilità: non sarà, quindi, sufficiente dimostrare che il provider avrebbe potuto conoscere del compimento di attività penalmente rilevanti da parte dei fruitori dei propri servizi utilizzando un certo grado di diligenza, essendo invece necessario che sia fornita la dimostrazione di una concreta e, appunto, effettiva conoscenza.[90]

Tale impostazione parrebbe del resto confermata anche dalla terminologia utilizzata dalle altre versioni della Direttiva CE 31/2000, quali, ad esempio, quella tedesca, che utilizza il termine analogo "*tatsächliche Kenntnis*".[91]

È evidente che dalla necessaria sussistenza di tale "effettiva conoscenza" in capo al *provider* discende inevitabilmente il corollario per cui, quand'anche il

---

dell'elemento soggettivo in termini di dolo diretto BARTOLI R., *Brevi considerazioni sulla responsabilità penale dell'Internet Service Provider,* 605.

[88] V. art. 14 Direttiva 31/2000: "*Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:*
a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent.

[89] Ed infatti, ai sensi del D.M.C.A., "*Under the knowledge standard, a service provider is eligible for the limitation on liability only if it does not have actual knowledge of the infringement, is not aware of facts or circumstances from which infringing activity is apparent, or upon gaining such knowledge or awareness, responds expeditiously to take the material down or block access to it".*

[90] Sul punto si v. STEA G., *La responsabilità penale dell'Internet Provider*, 4.

[91] La direttiva 31/2000 è stata recepita in Germania con la Legge sulle condizioni generali delle transazioni commerciali elettroniche del 14 dicembre 2001 (*Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr - (Elektronischer Geschäftsverkehr-Gesetz*), la cui disciplina sulla responsabilità dei *providers* ("*Dienstanbieter"*) è contenuta negli articoli 8 e seguenti della norma.

provider ponga in essere, consapevolmente, attività e prestazioni causalmente adeguati a contribuire, in maniera attiva, alla commissione di reati da parte dei membri della comunità di *users* di internet (mediante, ad esempio, l'indicizzazione di opere dell'ingegno diffuse illecitamente, come ben illustrato dalla sentenza "*Pirate Bay"*), la penale rilevanza di tali attività e prestazioni ai fini del concorso *ex* art. 110 c.p. del *provider* sarà in ogni caso subordinato al duplice accertamento della concreta consapevolezza dell'illegalità della condotta del singolo e dell'adesione psicologica alla medesima. In caso contrario, infatti, si finirebbe per riconoscere un *dolus in re ipsa* in capo al *provider* per il solo fatto di aver messo a disposizione strumenti che, sul piano oggettivo, hanno agevolato la commissione di reati da parte degli utenti del web.

Tale considerazione preclude, di conseguenza, la configurabilità di ipotesi di partecipazione nel reato non soltanto di natura colposa (comunque non conciliabile con i reati in materia di diritto d'autore, e più in generale con i reati informatici, tutti puniti esclusivamente a titolo di dolo), bensì anche in termini di dolo eventuale, atteso che è la stessa norma fondante la responsabilità del *provider* a non ritenere sufficiente la mera prospettazione ed accettazione del rischio di contribuire ad un'attività illecita.[92]

Parimenti, deve altresì escludersi che il *provider* possa rispondere, ai sensi dell'art. 116 c.p., per un reato diverso da quello voluto realizzato da un altro compartecipe nonché, laddove si voglia comunque ritenere ammissibile l'istituto[93], a titolo di concorso colposo nel reato doloso.

Presentato in questi termini, pertanto, l'elemento soggettivo in capo all'*Internet Provider* per le ipotesi di concorso attivo in reati commessi *una tantum* da parte degli utenti della rete risulta, innegabilmente, di ardua dimostrazione; sicché, in concreto, la ricostruzione del dolo di concorso dell'ISP dovrà passare dall'accertamento di elementi sintomatici di un'adesione psicologica *ex ante* ai delitti dei singoli, quali l'esistenza di accordi preesistenti con chi materialmente abbia diffuso contenuti illeciti sui server amministrati dal *provider*[94] ovvero la continua prestazione di servizi

[92] Sull'impossibilità di configurare l'elemento soggettivo in termini di dolo eventuale si sono espressi INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine;* MANNA A., DI FLORIO M., *Riservatezza e diritto alla privacy: in particolare, la responsabilità per omissionem dell'Internet Provider,* 916; ERCOLANI S., *Il diritto d'autore e i diritti connessi. La legge n. 633/1941 dopo l'attuazione della direttiva n. 2001/29/CE,* 2004, 376 ss.

[93] L'ammissibilità del concorso colposo nel delitto doloso, originariamente riconosciuta da un indirizzo giurisprudenziale in seno alla C.S., esplicato, tra le altre, nella sentenza Cass. Pen. Sez. IV, n. 4107 del 12/11/2008, è stata recentemente esclusa dalla sentenza Cass. Pen. Sez. IV, n. 7032 del 14/02/2019.

[94] Secondo MANNA A., DI FLORIO M., *Riservatezza e diritto alla privacy: in particolare, la responsabilità per omissionem dell'Internet Provider,* 902, tale modello, anche se più

che agevolino l'*upload,* la trasmissione e la diffusione di materiale illecito nonostante, in base a precedenti segnalazioni, ad autonome iniziative o a ordini di rimozione provenienti dall'autorità, ovvero ancora nel caso in cui il contenuto caricato dall'utente sia immediatamente riconoscibile come antigiuridico e non presenti margini di discrezionalità nella valutazione della sua illiceità, al fornitore sia noto che sulle proprie piattaforme online vengano commessi reati in maniera sistematica.

Non meno problematica si presenta la configurabilità dell'elemento soggettivo in capo al *provider,* ed in particolare in capo a quello che non interviene direttamente sulla circolazione dei contenuti nel ciberspazio, per le ipotesi in cui gli si voglia riconoscere una posizione di garanzia e, dunque, una sua responsabilità omissiva per i delitti commessi dalle persone fisiche sulla rete internet.

Come noto, ai fini della sussistenza dell'elemento soggettivo doloso nei reati omissivi impropri è necessario, cumulativamente, che il garante abbia consapevolezza della posizione di garanzia, che si sia rappresentato l'evento nella sua portata illecita[95] e che infine l'omissione della condotta doverosa sia cosciente e volontaria.

Sulla base di quanto illustrato sin qui, è evidente che, in relazione all'ISP, le criticità nell'accertamento del dolo emergono, in particolare, con riferimento ai primi due profili di consapevolezza, da un lato, della propria posizione di garanzia (e quindi degli obblighi giuridici di impedire i reati degli utenti) e della rappresentazione, dall'altro, dell'antigiuridicità dell'attività compiuta dai singoli sulla rete.

Ed invero, l'assenza di una legge che preveda espressamente una posizione di garanzia in capo all'intermediario di servizi della società dell'informazione contrasta, già di per sé, con la pretesa di un'inequivocabile cognizione della titolarità di obblighi penalmente sanzionati di vigilanza ed interposizione rispetto ai delitti commessi online dalle persone fisiche.

Se a tale premessa si aggiungono le difficoltà, anche di natura tecnica, di vagliare ogni singolo contenuto trasmesso e memorizzato sulla rete da parte dell'ISP, tanto più nei casi in cui, ai fini della fruizione delle prestazioni, il *provider* stesso abbia predisposto dispositivi la cui operatività, pur agevolando e migliorando la trasmissione delle informazioni, si basa su meccanismi predefiniti rispetto all'attività dell'utente, appare di immediata percezione che assai di rado potrà contestarsi all'*Internet Provider* l'attuale conoscenza delle condotte criminose realizzate tramite i servizi da lui forniti.

---

garantista, comporta una notevole difficoltà probatoria connessa alla problematica dimostrazione dell'accordo tra gestore di rete e soggetto che ha immesso in rete il materiale penalmente rilevante.

[95] Cfr. *ex multis* Cass. Pen. Sez. IV, n. 45011 del 26/10/2016.

Per le ragioni suesposte, non sembra potersi neppure applicare al fornitore di servizi di rete l'orientamento giurisprudenziale che ammette la sussistenza della responsabilità omissiva intesa, sotto il profilo soggettivo, nella prospettazione dell'evento come evenienza solo eventuale.[96]
Tale assunto stride, infatti, con le peculiarità dell'ISP e con la specifica disciplina legislativa, che parla espressamente di "conoscenza" dell'illecito e non di mera conoscibilità o accettazione del rischio che si verifichino fatti illeciti sulla rete, sicché non saranno sufficienti a fondare un rimprovero penale né la mancata reazione dinanzi ai c.d. "segnali d'allarme" né, a maggior ragione, la presunzione per cui il *provider* "non poteva non sapere" dei delitti realizzati all'interno delle reti cibernetiche riconducibili ai propri server.[97] Aderendo alla già richiamata dottrina maggioritaria sul tema, deve peraltro precisarsi che la suddetta conoscenza, laddove acquisita *ex post,* non fa comunque sorgere alcun sintomo di colpevolezza, ma costituisce piuttosto il punto di partenza per l'irradiarsi di una serie di obblighi di cooperazione e di intervento successivo nei confronti del *provider* (c.d. "*notice and take down"*), non punibili a titolo di omesso impedimento del reato altrui.
Come più volte ribadito, infatti, anche volendo ammettere una posizione di garanzia del *provider,* una volta acquisita la conoscenza dell'illiceità, questi non potrà rispondere per concorso, non essendo ipotizzabile una responsabilità concorsuale sorta *ex post* rispetto al momento di consumazione del reato, momento nel quale mancava altresì l'elemento soggettivo in capo al *provider*.
Tuttavia, come anticipato in precedenza, tale argomentazione potrebbe vacillare difronte alla novellata disciplina introdotta dal D.Lgs. 177/2021 all'interno della L. Aut., in particolare con il nuovo art. 102 *septies,* per la quale la limitazione di responsabilità data dalla necessità dell'"effettiva conoscenza" non troverebbe applicazione per gli *hosting provider* di piattaforme di condivisione di contenuti online che non abbiano ottenuto l'autorizzazione per la comunicazione al pubblico delle opere caricate sulle piattaforme medesima.

---

[96] Cfr. Cass. Pen. Sez. III, n. 28701 del 12/05/2010, per la quale "*la responsabilità penale per omesso impedimento dell'evento può qualificarsi anche per il solo dolo eventuale, a condizione che sussista, e sia percepibile dal soggetto, la presenza di segnali perspicui e peculiari dell'evento illecito caratterizzati da un elevato grado di anormalità"*.

[97] Sul punto si v. MANNA A., DI FLORIO M., *Riservatezza e diritto alla privacy: in particolare, la responsabilità per omissionem dell'Internet Provider,* 916, per cui, ai fini della configurabilità di una responsabilità omissiva impropria rimane comunque necessario, sul piano soggettivo, accertare l'intensità del dolo non soltanto potenziale ma effettiva, pena il rischio di integrare un *dolus in re ipsa* in contrasto col principio della personalità della responsabilità penale.

Per concludere, fatte salve le future applicazioni pratiche dell'art. 102 *septies* L. 633/1941, ricollegandosi a quanto detto parlando del concorso *ex* art. 110 c.p., ad oggi pare opportuno limitare, sotto il profilo della colpevolezza, la responsabilità *ex* art. 40 c. 2 c.p. dell'ISP ai soli casi in cui, dopo aver ricevuto segnalazioni relative a reati già commessi sulle proprie reti, ometta consapevolmente di adottare misure di controllo e di filtraggio imposte dall'autorità al fine di prevenire la reiterazione di reati futuri per i quali, a questo punto, potrà rispondere per omissione.

4.6. Le conseguenze penalmente rilevanti dell'inerzia dell'ISP dopo la commissione del reato.

Sin qui s'è parlato della responsabilità penale dell'*Internet Provider,* e delle relative criticità, in termini di concorso, attivo ed omissivo, nelle condotte antigiuridiche poste in essere dagli utenti, ossia i *content providers,* della rete.
Senonchè, come già anticipato in precedenza, può individuarsi un terzo modello di *accountability* del fornitore di servizi digitali che prescinde da un suo eventuale contributo nell'illecito dei singoli, ma si fonda invece sull'accertamento dell'esistenza di obblighi giuridici penalmente sanzionati insorgenti in capo all'ISP solo dopo, e non già *ante,* la commissione di reati.
Sotto questo profilo vengono in gioco tutte quelle disposizioni che impongono di rimuovere dal server
il materiale illecito memorizzato o di inibire l'accesso a siti contenenti tali informazioni.
A ben vedere, gli agganci normativi sono molteplici, e possono rinvenirsi tanto nella disciplina regolante l'*e-commerce* quanto, per quel che interessa in questa sede, nella legislazione sul diritto d'autore.
In particolare, come già evidenziato, gli artt. 14, 15 e 16 prevedono, nei confronti rispettivamente del *mere conduit, caching* e *hosting provider,* la facoltà per l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza di esigere che il prestatore, nell'esercizio delle sue attività, impedisca o ponga fine alle violazioni commesse.
Come regola generale, inoltre, l'art. 17 impone all'ISP un duplice obbligo informativo, avente ad oggetto sia la comunicazione delle attività e delle informazioni illecite riguardanti un destinatario del servizio sia, se richiesto dall'autorità, la fornitura di dati che consentano l'identificazione del destinatario che abbia tenuto condotte antigiuridiche mediante i servizi digitali prestati dal *provider*.
Si rammenti inoltre la clausola di responsabilità civile prevista dall'ultimo comma dell'art. 17 per il caso in cui l'ISP, richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non abbia agito prontamente per impedire l'accesso al detto contenuto illecito, ovvero se, avendo avuto conoscenza del carattere antigiuridico pregiudizievole per un terzo del

contenuto di un servizio al quale assicura l'accesso, non ha provveduto ad informarne l'autorità competente.
Accanto alla normativa sul commercio elettronico, vi sono ulteriori disposizioni che regolano i contenuti di siffatti obblighi di cooperazione e rimozione dei contenuti illeciti, riassumibile nel concetto di fonte statunitense, più volte ripetuto nelle pagine precedenti, di "*notice and take down*".
Per quel che inerisce alla materia che qui interessa, ossia il diritto d'autore, sono plurime le norme che, in tale ambito, prescrivono determinati adempimenti agli ISP in caso di violazioni delle privative di proprietà intellettuale sulle opere dell'ingegno digitali.
Tra queste, possono richiamarsi le procedure di inibitoria giudiziale attivabili da coloro che hanno subito violazioni di diritti di utilizzazione economica su opere dell'ingegno previsti dai già citati art. 156 e 163 L. Aut., traducibili, anche in via indiretta, in ordini di rimozione dei contenuti illeciti rivolti all'intermediario i cui servizi sono utilizzati per tali violazioni.
Al di fuori della Legge 633/1941 si rinvengono, sul tema, altre fonti da cui trarsi l'obbligo di adottare la procedura di *notice and take down* in materia di illeciti contro la proprietà intellettuale. Emblematico è l'art. 1 del D.L. 72 del 22 marzo 2004, convertito dalla L. 128 del 21 maggio 2015, i cui commi 5 e 6 prevedono rispettivamente che "*a seguito di provvedimento dell'autorità giudiziaria, i prestatori di servizi della società dell'informazione, di cui al D.Lgs. 9 aprile 2003, n. 70, comunicano alle autorità di polizia le informazioni in proprio possesso utili all'individuazione dei gestori dei siti e degli autori delle condotte segnalate*" e "*a seguito di provvedimento dell'autorità giudiziaria, per le violazioni commesse per via telematica di cui al presente decreto, i prestatori di servizi della società dell'informazione, ad eccezione dei fornitori di connettività alle reti* (c.d. *access providers* n.d.r.) *pongono in essere tutte le misure dirette ad impedire l'accesso ai contenuti dei siti ovvero a rimuovere i contenuti medesimi*".
Dalla suesposta elencazione di norme può ricavarsi una bipartizione di doveri che incombono sull'ISP a seguito della notizia della realizzazione di delitti sulle reti da lui gestite, ricomprendenti, da un lato, l'obbligo di denuncia all'autorità competente dell'illecito e delle informazioni utili all'identificazione degli autori e, dall'altro, l'obbligo di rimozione del materiale antigiuridico memorizzato sui propri server o di inibizione all'accesso, sempre su richiesta dell'autorità competente.
Entrambe le categorie di oneri ricadenti sul *provider* appaiono comunque riconducibili ad un minimo comun denominatore di non scarsa rilevanza, ossia il presupposto per cui l'obbligo di notifica e di rimozione sorge, soltanto, a seguito dell'intervento dell'autorità pubblica competente, giudiziaria e non, laddove segnalazioni o intimazioni di privati risultano, se ci si attiene alla lettera delle norme, prive di vincoli giuridici per l'ISP. Sulla

scorta di tale considerazione, pertanto, la dottrina è univoca nell'orientarsi, anche in materia penale, verso la necessità di quella "conoscenza qualificata" già menzionata nelle pagine precedenti.
Ad ogni modo, in mancanza di una specifica fattispecie penale volta a tutelare l'osservanza di detti obblighi, che risultano puniti, quando previsto, soltanto in via amministrativa o civile[98], occorre individuare ipotesi di reato di parte speciale nel quale sussumere l'inerzia del *provider* nell'adozione dei comportamenti esigibili in caso di reati commessi online.
In via preliminare, si può ricordare che, come già anticipato sopra, una parte minoritaria della dottrina ha osservato che l'inadempimento degli obblighi di *notice and take down* da parte dell'ISP, benché apparentemente successivo ad un reato già consumatosi, potrebbe fondare una responsabilità penale per omesso impedimento dei reati sulla rete; le attività antigiuridiche commesse online, secondo tale indirizzo, si svolgono pur sempre sotto l'autorità o il controllo del *provider,* rispetto alle quali questi è dotato di un effettivo potere e dovere di interferenza e rimozione che deve esercitare ricevuta la notizia del provvedimento ingiunzionale dell'autorità giudiziaria.[99] Questa soluzione ermeneutica, se consente indubbiamente di trovare un equilibrio fra le interpretazioni che potrebbero comportare il rischio di deriva vero forme di "responsabilità da posizione" dell'ISP con le posizioni tradizionali orientate verso la non prospettabilità di una posizione di garanzia in capo al fornitore

[98] Ed invero, come noto l'art. 17 prevede esclusivamente la responsabilità civile dell'ISP rimasto "inerte" nell'attivazione della procedura di *notice and take down;* gli artt. 156 e 163 L. Aut. prevedono la possibilità per il giudice di fissare una somma dovuta, a titolo chiaramente civilistico, per ogni violazione o inosservanza successivamente constatata o per ogni ritardo nell'esecuzione del provvedimento; infine, il comma 7 dell'art. 1 del D.L. 72/2004 prevede una sanzione amministrativa pecuniaria da 50.000 a 250.000 euro per la violazione degli obblighi di cui ai commi 5 e 6 del medesimo articolo.

[99] Sostiene questa tesi FLOR R., *La tutela penale dei diritti d'autore e connessi,* 1162 ss.; secondo l'autore, l'interpretazione sistematica delle disposizioni di cui agli artt. 14 ss. del D.Lgs. 70/2003 "*non esclude la possibilità di configurare una responsabilità penale del provider per omesso impedimento di taluni reati in materia di diritto d'autore, in particolar modo a titolo di concorso tramite omissione e nell'ambito di attività che si svolgano sotto la sua autorità o controllo, essendo rinvenibile un modello ingiunzionale e una procedura, al cui esito è emesso un provvedimento amministrativo o giurisdizionale che impone l'inibitoria o il blocco di una webpage o ad un website o a determinati materiali. Il provider, dunque, non solo viene cos' a conoscenza dell'illecito o messo concretamente in grado di riconoscerlo, se il citato provvedimento è preciso, ma è altresì dotato di effettivi poteri di interdizione, impeditivi o direttamente legati ai processi da cui derivano i rischi, se non preventivi".* Contrari sul punto BARTOLI R., *Brevi considerazioni sulla responsabilità penale dell'Internet Service Provider,* 604; INGRASSIA A., *Responsabilità penale degli internet service provider: attualità e prospettiva,* Diritto Penale e Processo, 1626 ss.

di servizi, presenta il limite, già evidenziato *supra,* di estendere la responsabilità penale per concorso di un soggetto a reati che, di fatto, si sono consumati in precedenza e in un momento nel quale il *provider* non risultava (ancora) titolare di alcun obbligo di controllo e impedimento. Letta in questo modo, infatti, tale tesi porterebbe il *provider* a rispondere *ex* art. 40 c. 2 c.p. non già per non aver impedito un reato, ma per non aver rimosso gli effetti pregiudizievoli di un reato già manifestatosi in tutti i suoi elementi costitutivi.
Abbandonando ora il discorso sulla responsabilità concorsuale dell'ISP e concentrandosi esclusivamente sul disvalore intrinseco dell'inottemperanza ai doveri di comunicazione e di rimozione previsti dalle differenti disposizioni extrapenali di riferimento, può affermarsi che le fattispecie tipiche riconducibili a detta inottemperanza non manchino e, anzi, siano molteplici.
Premessa, per ovvie ragioni, l'impossibilità di rendere l'ISP destinatario dei precetti di cui ai reati di omessa denuncia di reati all'autorità di cui agli artt. 361 e 364 c.p.[100], le prime ipotesi delittuose di parte speciale, astrattamente riferibili al *provider,* che saltano all'occhio sono indubbiamente quelle di favoreggiamento personale e reale previste dagli artt. 378 e 379 c.p.
Quanto al favoreggiamento personale, aderendo all'insegnamento ormai consolidato della giurisprudenza di legittimità fermo nell'ammettere la possibilità di realizzare il reato anche mediante un *non facere* antidoveroso nei casi in cui vi sia un obbligo di cooperazione con l'autorità[101], è di immediata percezione che la, dolosa, mancata segnalazione alle autorità giudiziarie, a seguito di provvedimento delle medesime, delle informazioni utili all'individuazione degli autori delle condotte lesive del diritto d'autore commesse su internet imposta agli ISP dagli artt. 17 c. 2 lett. b) D.Lgs. 70/2003 e 1 c. 5 D.L. 72/2004 potrà essere facilmente interpretata come quell'aiuto diretto a eludere le indagini o a sottrarsi alle ricerche dell'autorità che integra il fatto tipico del reato di cui all'art. 378 c.p.
Va tuttavia segnalata l'opinione di chi, in letteratura, ha ritenuto che la specifica previsione di una sanzione amministrativa per la mancata collaborazione con l'autorità, previste dal D.L. 72/2004, sembra escludere, in virtù del principio di specialità e di sussidiarietà dello strumento penale, che il mero omesso adempimento di questi obblighi da parte dell'ISP possa integrare il delitto di favoreggiamento: se, infatti, la mancata comunicazione integrasse già la fattispecie delittuosa, il portato dell'illecito amministrativo,

[100] Come noto, infatti, l'art. 361 c.p. è norma rivolta ai soli pubblici ufficiali, qualifica difficilmente attribuibile ad un Internet Provider; l'art. 364, che punisce il cittadino che ometta di denunciare un reato contro la personalità dello Stato punibile con l'ergastolo, è invece, evidentemente, del tutto inapplicabile rispetto ai reati in materia di diritto d'autore.
[101] Cfr. *ex multis* Cass. Pen. Sez. VI, n. 37757 del 07/10/2010.

a fronte di una formulazione assai ampia, sarebbe piuttosto esiguo, limitandosi alle violazioni di carattere colposo.
In tale ottica, la possibilità di ascrivere un'imputazione a titolo di favoreggiamento verso l'ISP parrebbe limitarsi ad ipotesi in cui la condotta del medesimo si colori di un *quid pluris* rispetto alla semplice omissione, come nel caso di comunicazione di informazioni false o difformi sulle imprese o soggetti che diffondono o commercializzano opere dell'ingegno in rete senza licenza.[102]
Se si ammette in ogni caso la configurabilità del reato di favoreggiamento personale verso l'ISP, non sembrano porsi ostacoli all'applicazione, anche, della fattispecie di favoreggiamento reale: quest'ultima pare infatti configurabile non soltanto nei casi di omessa segnalazione degli autori dei reati, ma anche in caso di omessa rimozione del contenuto illecito, condotte ben sintomatiche di un'intenzione di assicurare al colpevole il profitto dei reati contro la proprietà intellettuale commessi in rete, il cui fine lucrativo è, del resto, elemento costitutivo della struttura del fatto.
Con specifico riferimento all'inadempimento degli obblighi di adozione delle misure dirette ad impedire l'accesso ai contenuti dei siti e a rimuovere i contenuti medesimi previsto dagli artt. 17 c. 3 D.Lgs. 70/2003 e 1 c. 6 D.L. 72/2004 ordinate dall'autorità, nonché all'inottemperanza degli ordini inibitori emessi ai sensi degli artt. 156 e 163 L. Aut., le fattispecie immaginabili sono essenzialmente due: la prima, delittuosa, di mancata esecuzione dolosa di un provvedimento del giudice *ex* art. 388 c.p.; la seconda, contravvenzionale, consistente nell'inosservanza di provvedimenti dell'autorità di cui all'art. 650 c.p.
Quanto al reato di cui all'art. 388 c.p., l'ipotesi di riferimento potrebbe individuarsi, oltre che nella generale commissione di atti fraudolenti al fine di sottrarsi all'adempimento di obblighi nascenti dal provvedimento del giudice, nella fattispecie di cui al comma terzo, che prevede la pena della reclusione fino a tre anni verso chi elude l'esecuzione di un provvedimento del giudice che prescrive misure inibitorie a tutela di diritti di proprietà industriale. L'applicazione di tale comma, tuttavia, sembra richiedere una contorta estensione del concetto di proprietà industriale alla nozione di proprietà intellettuale, della quale, come noto, la proprietà industriale costituisce una *species*.
Benchè certamente non escludibile a priori, l'applicabilità in concreto dell'art. 388 c.p. alla condotta inerte dell'ISP sembra incontrare un limite nella parte in cui subordina l'integrazione del delitto alla realizzazione di atti fraudolenti

[102] Così INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine*.

diretti ad eludere gli obblighi di esecuzione del provvedimento giudiziale.[103]
Di conseguenza, sembrerebbe escluso dalla sfera applicativa della norma l'ipotesi, certamente più frequente, di mera inosservanza dell'ordine inibitorio o di altro provvedimento giudiziale che imponga il blocco dell'accesso al materiale illecito non accompagnata da comportamenti elusivi e fraudolenti del *provider*.
Tali ragioni hanno portato la dottrina a ritenere più corretto il richiamo all'ipotesi meno grave di cui all'art. 650 c.p., la quale, trattandosi di contravvenzione, è idonea ad applicarsi anche ai casi in cui il mancato filtraggio dei siti web e l'omessa rimozione del materiale lesivo dei diritti di proprietà intellettuale siano imputabili ad un'inerzia del *provider* di natura colposa.
Seppur di più immediata applicazione, è tuttavia pacifico che il ricorso alla fattispecie *ex* art. 650 c.p. nei confronti del fornitore di servizi di rete presenta un limite attinente alla scarsissima deterrenza verso gli ISP rispetto all'osservanza dei doveri di cooperazione con l'autorità.
Il reato è infatti una contravvenzione punita con pena alternativa, e pertanto suscettibile di estinzione mediante oblazione ai sensi dell'art. 162 *bis* c.p. dietro il pagamento di una somma pari alla metà del massimo dell'ammenda prevista, che l'art. 650 c.p. fissa in 206 euro.
Sembra inutile dilungarsi su quanta poca efficacia dissuasiva presenta la minaccia del versamento di 103 euro per soggetti, quali i prestatori di servizi internet, il cui fatturato annuo, in alcuni casi, raggiunge importi calcolabili in scala di miliardi di euro.
Sulla base di tali considerazioni, è evidente che, il rimprovero penale per l'omesso adempimento dell'ordine di "*take down*" proveniente dall'autorità giudiziaria sia, di fatto, destinato a lasciare spazio al più immediato nonché, paradossalmente, più severo e inibitorio regime sanzionatorio di carattere amministrativo e civile previsto dalla normativa di settore.
Di conseguenza, tenuto conto delle inevitabili difficoltà applicative dei suddetti reati di cui agli artt. 378, 379, 388 e 650 c.p. verso l'ISP che non dia seguito ai provvedimenti autoritativi di segnalazione e rimozione degli effetti

[103] Ciò è del resto avallato dalla Cassazione nella sua più alta composizione, che con sentenza Cass. Pen. SS. UU., n. 12213 del 21/12/2017 ha statuito che "*ai fini della configurabilità del reato di mancata esecuzione dolosa di un provvedimento del giudice di cui all'art. 388, comma primo, cod. pen. non è sufficiente che gli atti dispositivi compiuti dall'obbligato sui propri o altrui beni siano oggettivamente finalizzati a consentirgli di sottrarsi agli adempimenti indicati nel provvedimento, rendendo così inefficaci gli obblighi da esso derivanti, ma è necessario che tali atti abbiano natura simulata o fraudolenta, siano cioè connotati da una componente di artificio, inganno o menzogna concretamente idonea a vulnerare le legittime pretese del creditore*".

delle attività illecite commesse tramite i servizi forniti sulla rete, la suesposta modalità di allocazione della risposta penale a seguito della commissione di un reato pare poter superare i tre fondamentali problemi posti dalla qualificazione della responsabilità penale dell'ISP in termini di concorso, attivo ed omissivo, nei reati degli utenti, ossia il fondamento giuridico della posizione di garanzia, l'esistenza di poteri giuridici
impeditivi dell'evento e la sussistenza del dolo, in relazione alla conoscenza del reato da altri realizzato.[104]
Una nuova prospettiva di responsabilizzazione del *provider* per l'omessa rimozione di contenuti contrastanti con il diritto d'autore si è aperta, peraltro, con l'introduzione del nuovo art. 102 *decies* nella L. 633/1941 ad opera del D.Lgs. 177/2020; come anticipato *supra,* infatti, la norma attribuisce ai titolari dei diritti di utilizzazione economica sulle opere digitali di chiedere al prestatore di servizi di condivisione di contenuti online di disabilitare l'accesso a loro specifiche opere o ad altri materiali o di rimuoverli.
Ed invero, se è evidente che l'inerzia del *provider* di fronte a tali richieste non potrà certamente configurare le suesposte ipotesi di reato di cui agli artt. 388 e 650 c.p., considerato che l'ordine di rimozione non proviene da una fonte "pubblicistica" bensì da un privato, la stessa inerzia potrebbe tradursi nella commissione, in via autonoma, di una delle fattispecie di cui agli artt. 171 ss. L. Aut.: non ottemperare alla richiesta di rimozione proveniente dal titolare del diritto d'autore, infatti, equivale alla diffusione e messa a disposizione di un'opera dell'ingegno senza l'autorizzazione dell'autore, sicché, se compiuta a scopo di lucro, tale condotta rientrerebbe pacificamente nella categoria dei delitti di pirateria digitale previsti dal testo legislativo. Tuttavia, occorre precisare che tale considerazione, data l'assenza di interventi giurisprudenziali e dottrinali sull'art. 102 *decies* L. Aut., rimane una mera tesi interpretativa ancora priva di riscontri applicativi ed ermeneutici.
In ogni caso, in una prospettiva *de jure condendo,* qualora si ritenga necessaria un'effettiva tutela penale della corretta esecuzione della procedura di *notice and take down* da parte dei *providers* può dirsi auspicabile un intervento ordinatore del legislatore che vada a tipizzare una fattispecie specificamente diretta a reprimere l'omesso adeguamento dei fornitori dei servizi internet agli obblighi loro imposti dopo la commissione di delitti da parte dei fruitori del ciberspazio.

[104] Secondo INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine,* il paradigma del *provider* "tutore dell'ordine" si fonda infatti su previsioni che tipizzano obblighi di condotta specifici, non correlati all'impedimento di un evento e che scaturiscono da un provvedimento dell'autorità in cui è già indicato il reato commesso di cui si devono interdire gli effetti o la continuazione.

4.7. La responsabilità amministrativa *ex* D.Lgs. 231/2001 dell'*Internet Provider*.

Sin qui si è trattato dei possibili modelli di *accountability* penale degli ISP intendendo, implicitamente, come destinatari del rimprovero e della sanzione le persone fisiche che agiscono all'interno della loro organizzazione aziendale a cui può direttamente e personalmente addebitarsi un'eventuale condotta illecita, attiva od omissiva che dir si voglia.

Pertanto, ancor prima di individuare il paradigma di responsabilità e la fattispecie concretamente applicabile al *provider,* occorre procedere nel tentativo, tutt'altro che semplice, di risalire al soggetto, apicale o subordinato, all'interno della struttura organizzativa della società "fornitore di servizi internet" a cui può ascriversi la violazione.

Ben diversa è la situazione in cui si voglia responsabilizzare il *provider* inteso come ente o società organizzata economicamente ed esercente un'attività d'impresa. Non va infatti dimenticato che i fornitori di servizi di rete sono organizzazioni imprenditoriali ramificate spesso a livello globale, come le grandi piattaforme di *hosting online* a noi ben note, o comunque nazionale, che rilasciano le loro prestazioni dietro corrispettivo.

In altre parole, si tratta di realtà economiche che, laddove coinvolte nella commissione di reati consumati o tentati, sono a pieno titolo destinatarie della disciplina della responsabilità amministrativa delle persone giuridiche contenuta nel D.Lgs. 231/2001, che negli ultimi anni si è rivelata particolarmente severa, per lo meno nelle intenzioni, nel responsabilizzare le società per i reati realizzati nel contesto dello sviluppo
tecnologico e della società dell'informazione.[105]

Rinviando a sedi più opportune per una trattazione più approfondita di un argomento estremamente vasto,[106] ci si limiterà qui ad esaminare i profili di intersezione di maggiore interesse tra il Decreto 231 e lo statuto penale degli *Internet Providers,* per come fin qui ricostruito, in relazione ai reati in materia di diritto d'autore.

---

[105] In particolare, l'art 24 *bis* del Decreto 231 introdotto dalla L. 92/2008 pone a fondamento della responsabilità dell'ente quasi tutti i reati informatici "in senso stretto", ad accezione del delitto di frode informatica di cui all'art. 640 *ter* c.p. e delle fattispecie di illecito trattamento dei dati personali, curiosamente indicati nella rubrica dell'articolo ma non contemplati nel catalogo dei reati presupposto.

[106] La bibliografia è amplissima. Per una visione d'insieme si rinvia in ogni caso a VINCIGUERRA S., ROSSI A., CERESA GASTALDO M., *La responsabilità dell'ente per il reato commesso nel suo interesse (D.Lgs. n. 231/2001),* CEDAM, 2004; in relazione alla responsabilità degli enti per i reati informatici si v. la brillante disamina di FONDAROLI D., *La responsabilità di persone giuridiche ed enti per i reati informatici ex D.Lgs. n. 231/2001,* in CADOPPI A., CANESTRARI S., MANNA A., PAPA M., *Cybercrime,* 2019, Utet Giuridica, 193 ss.

Come noto, la Legge 23 luglio 2009, n. 99 ha esteso la responsabilità amministrativa degli enti ai reati in materia di proprietà intellettuale, introducendo all'art. 25 *novies* del Decreto, tra i reati presupposto, una serie di delitti in materia di violazione del diritto di autore previsti dalla L. 633/1941, e più precisamente di quelli di cui agli artt. 171, comma 1, lett. a-*bis*), e comma 3, 171 *bis*, 171 *ter*, 171 *septies* e 171 *octies* del testo legislativo, prevedendo in relazione ai medesimi la sanzione pecuniaria applicabile fino a cinquecento quote e quelle interdittive *ex* art. 9 c. 2[107] del Decreto per la durata non superiore ad un anno, la cui afflittività può risultare, soprattutto per società quali quelle che prestano servizi della società dell'informazione, ancor maggiore rispetto alla sola sanzione pecuniaria.
Il comma 2 dell'articolo in commento prevede, inoltre, l'applicazione anche nel procedimento a carico dell'ente delle disposizioni di cui all'art. 174 *quinquies* L. Aut., che impone al pubblico ministero, al momento dell'esercizio dell'azione penale, di informare il questore qualora l'illecito sia stato commesso nell'ambito di un esercizio commerciale o di un'attività soggetta ad autorizzazione al fine dell'adozione dei provvedimenti amministrativi di sospensione dell'esercizio o dell'attività, nonché la sanzione amministrativa accessoria della cessazione temporanea dell'esercizio o dell'attività per un periodo da tre mesi ad un anno.
Nell'estendere la responsabilità amministrativa da reato degli enti anche ai delitti in materia di diritto d'autore, la legge mira a garantire un'efficace tutela contro la contraffazione e al fine di ostacolare energicamente il rischio che attraverso la sistematica violazione delle norme di proprietà intellettuale e di comportamenti commerciali in frode ai consumatori vengano realizzate vere e proprie politiche aziendali "criminose" in grado di alterare la concorrenza tra imprese e di ledere l'economia nazionale.[108]
È tuttavia importante effettuare una duplice puntualizzazione: in primo luogo, è fuori dubbio che la disciplina troverà applicazione solo nei casi di responsabilità concorsuale dell'ente negli illeciti, consumati o tentati, commessi dagli utenti della rete, e non anche in caso di inottemperanza ai successivi doveri di notificazione, rimozione e blocco dell'accesso, i quali,

[107] Tra queste si possono richiamare l'interdizione dall'esercizio dell'attività, la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito, il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio, l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi ed infine il divieto di pubblicizzare beni o servizi.
[108] Così MARENGHI I., *Le nuove norme in materia di proprietà industriale. Brevi note a margine della riforma del diritto penale industriale,* in Il Diritto Industriale, n. 5/2009, 468 ss.

come osservato, sono riconducibili a fattispecie estranee all'elenco dei reati presupposto indicato dal Decreto 231.
Inoltre, quando si parla di responsabilità *ex* D.Lgs. 231/2001 dell'ISP, non si intende il caso del dipendente della società, attiva in un qualsiasi settore merceologico, che nell'interesse o a vantaggio della stessa pone in essere condotte penalmente rilevanti ai sensi della L. 633/1941 utilizzando i servizi e le strutture messe a disposizione dal *provider* nel proprio contesto aziendale (si pensi al dipendente esperto di informatica che, scaricati abusivamente un *software* o una banca dati utili per l'esercizio dell'attività lavorativa, li duplichi e li condivida con i colleghi garantendo all'azienda un risparmio sulle *royalties*), bensì dell'*intraneus* all'organizzazione dell'ISP stesso che, in una delle forme di partecipazione concorsuale al reato sopra analizzate, cooperando attivamente od omissivamente, offra un contributo eziologicamente funzionale alla commissione del reato presupposto da parte dell'utente della rete.
Poste le dovute premesse, occorre evidenziare innanzitutto che la circostanza per cui, non di rado, i fornitori di servizi di rete siano costituiti da una società madre situata all'estero che consta di una rete estesissima di filiali e *subsidiaries* non osta all'applicazione, anche nei confronti di ISP aventi sede al di fuori del territorio nazionale, delle norme del Decreto. Ed invero, è ormai principio assodato quello per cui la persona giuridica, ancorché avente sede all'estero, è chiamata a rispondere dell'illecito amministrativo derivante da un reato presupposto per il quale sussista la giurisdizione nazionale commesso dai propri legali rappresentanti o soggetti sottoposti all'altrui direzione o vigilanza. Ed infatti, l'ente è soggetto all'obbligo di osservare la legge italiana e, in particolare, quella penale, a prescindere dalla sua nazionalità o dal luogo ove esso abbia la propria sede legale ed indipendentemente dall'esistenza o meno nel Paese di appartenenza di norme che disciplino in modo analogo la medesima materia.[109]
Allo stesso modo, in ossequio all'art. 4 del Decreto, anche i grandi *players* del mercato dei servizi digitali aventi sede in Italia potranno rispondere per i reati commessi all'estero ai sensi del Decreto 231.
In ogni caso, anche per fondare la responsabilità dei *providers* sarà necessario accertare la sussistenza dei presupposti di cui all'art. 5 del D.Lgs. 231: occorre, in altre parole, che il reato presupposto sia stato commesso da soggetti apicali o subordinati, operanti all'interno dell'organigramma della società, nell'interesse o a vantaggio dell'ente stesso, con esclusione dunque delle ipotesi in cui l'illecito sia stato realizzato esclusivamente nell'interesse proprio della persona fisica.
La corretta individuazione dell'autore del reato entro la compagine societaria, come noto, è dirimente ai fini della prova della responsabilità dell'ente, atteso

[109] Cfr. da ultimo Cass. Pen. Sez. VI, n. 11626 del 07/04/2020.

che laddove l'illecito sia stato posto in essere da un soggetto esercente la gestione o il controllo il relativo onere è rimesso all'ente con modalità tali da farlo apparire alla stregua di una *probatio diabolica*.[110]
E tuttavia, sono evidenti le criticità che tale accertamento presenta nel contesto organizzativo di enti quali gli *Internet Providers,* i quali, come anticipato, sono spesso costituiti da complessissime e multiformi realtà imprenditoriali articolate su scala globale le cui procedure decisionali coinvolgono un numero estesissimo di soggetti, di diverse nazionalità e sottoposti ad ordinamenti giuridici diversi: ed invero, già prima di soffermarsi sulla qualificazione aziendale attribuibile al responsabile del concorso dell'ISP nel reato presupposto, sarà necessario determinare se il contributo causale prestato dall'ente rispetto alle condotte antigiuridiche dei fruitori dei servizi dell'ISP possa ascriversi ad una "falla" incidentale nella direzione della vigilanza sull'operato dei dipendenti in un contesto nel quale sono state comunque adottate appositi presidi cautelari volti a ridurre le possibilità di commissione di (o il concorso in) reati-presupposto, ovvero ad una prassi imposta "dall'alto" in virtù della quale, per volontà dei vertici dell'*Internet Provider,* quest'ultimo omette volontariamente di adottare misure di controllo, di filtraggio o di rimozione dei contenuti trasmessi e memorizzati sulle proprie
piattaforme di rete.

[110] Ed invero, ai sensi dell'art. 6 c. 1 esonera l'ente da responsabilità per il reato commesso dai vertici aziendali soltanto se l'ente stesso prova che l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi, che il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo, che le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione e che non vi è stata omessa o insufficiente vigilanza da parte dell'OdV.
Meno rigida è invece la disciplina nell'ipotesi in cui il reato presupposto sia stato commesso dal soggetto sottoposto a direzione o vigilanza: in questo caso, l'art. 7 prevede che l'ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza, la quale è in ogni caso esclusa se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.
Sul punto, è stato evidenziato in dottrina che la previsione di cui all'art. 6 determinerebbe di fatto un'inversione dell'onere della prova, che celerebbe la presunzione di colpevolezza dell'ente che non provi la propria innocenza; si v. FONDAROLI D., *La responsabilità di persone giuridiche ed enti per i reati informatici ex D.Lgs. n. 231/2001*, 197.

Da quanto sopra esposto è fuori dubbio che, al fine di accertare a quale titolo l'ente debba eventualmente rispondere, sarà essenziale, in particolare con riferimento alle c.d. "*big tech*", accertare l'esistenza di documenti che consentano di individuare, all'interno di vastissime strutture imprenditoriali, "chi deve fare cosa", quali l'organigramma, codici etici e disciplinari, un sistema di procure e deleghe di funzione ecc.[111]
Altro presupposto imprescindibile per l'attribuzione della responsabilità in relazione ai reati-presupposto è dato dal fatto che l'ente abbia avuto un interesse o tratto un vantaggio dalla commissione del reato.
Come noto, si tratta di requisiti alternativi ed indipendenti l'uno dall'altro: il criterio dell'interesse, da un lato, esprime la valutazione teleologica del reato apprezzabile *ex ante* e secondo un metro di giudizio soggettivo in relazione all'elemento psicologico della specifica persona fisica autrice del reato; viceversa, il criterio del vantaggio ha una connotazione essenzialmente oggettiva, come tale valutabile *ex post,* sulla base degli effetti concretamente derivati dalla realizzazione dell'illecito e indipendentemente dalla finalizzazione originaria del reato.[112]
Pur in assenza di una specifica casistica giurisprudenziale, non è arduo immaginare i potenziali interessi che *l'Internet Provider* potrebbe *ex ante* avere nel - o i benefici che potrebbe *ex post* trarre dal – concorso nei reati contro la proprietà intellettuale commessi online: si pensi, ad esempio, agli eventuali introiti che una piattaforma di *hosting* potrebbe ricavare grazie alla messa a disposizione in *streaming* di opere multimediali senza autorizzazione, ovvero alla possibilità di ricavare profitti grazie ai *banners* pubblicitari ospitati sul sito dove viene diffuso il materiale illecito, ovvero, ancora, alla più semplice ipotesi di pagamenti ricevuti dai gestori di siti web in occasione di accordi finalizzati a fornire a questi ultimi i mezzi tecnici e informatici per procedere con l'*upload* di contenuti protetti o, comunque, a non interferire con tale attività.
Le procedure di *compliance* normativa volte a prevenire la commissione di reati-presupposto nel contesto della struttura organizzativa dell'ente e ad esonerare quest'ultimo da possibili responsabilità nell'eventualità in cui detti reati siano stati posti in essere si traducono nell'adozione (e nell'attuazione) di quei Modelli di Organizzazione e Gestione che il Decreto stesso individua come i presidi tesi ad escludere la colpa organizzativa dell'ente per i delitti commessi dalle persone fisiche operanti al suo interno.
Come noto, l'efficacia di tali modelli è subordinata ad una determinata struttura e ad uno specifico contenuto delineati dall'art. 6 c. 2 del D.Lgs. 231/2001, che ricomprendono la previsione di un organismo di vigilanza

[111] Sul punto v. FONDAROLI D., *La responsabilità di persone giuridiche ed enti per i reati informatici ex D.Lgs. n. 231/200,* 196.
[112] Cfr. Cass. Pen. Sez. II, n. 295 del 09/01/2018.

dotato di autonomi poteri di iniziativa e di controllo, la previsione di protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire, la specificazione delle modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di reati, la previsione di obblighi di informazione nei confronti dell'organismo di vigilanza da parte, l'introduzione di un sistema disciplinare effettivo che sanzioni il mancato rispetto delle misure indicate nel modello e l'individuazione delle attività nel cui ambito possono essere commessi reati.[113]

Pensando ai reati in materia di diritto d'autore, le aree maggiormente sensibili alla commissione di delitti da parte di soggetti interni ad organizzazioni imprenditoriali operanti in larga parte su un mercato digitale e smaterializzato saranno indubbiamente costituite da quelle riconducibili all'Information Technology, alla comunicazione esterna e ai rapporti coi media, alla diffusione di materiale promozionale online potenzialmente coperto dal diritto d'autore, ai rapporti con la clientela nella fornitura di servizi di rete ovvero, ancora, agli acquisti di beni e servizi (quali software o banche di dati soggetti a privative intellettuali) da parte di terzi.

Ad ogni modo, data la scarsità di interventi giurisprudenziali sul tema, può ritenersi che l'applicazione della disciplina sulla responsabilità degli enti nei confronti dei prestatori di servizi di rete per reati in materia di diritto d'autore rimanga ad oggi una questione di interesse più teorico che pratico.

5. Conclusioni: lo stato dell'arte e prospettive future

Nel terminare la presente disamina si può concludere affermando che, alla luce del combinato dell'attuale disciplina comunitaria e nazionale applicabile in materia, gli spazi per un riconoscimento della responsabilità penale dell'ISP per i reati contro il diritto d'autore commessi online del tutto scevro da perplessità sono ancora molto limitati.

I dubbi emergono, sostanzialmente, in relazione a tutti i differenti modelli di responsabilizzazione del *provider* esaminati nelle pagine precedenti.

[113] L'adozione di modelli 231 all'interno di società operanti prevalentemente su un fronte digitale e smaterializzato può, peraltro, ispirarsi al sistema di adempimenti volti ad adeguare il trattamento dei dati personali alla *compliance* normativa introdotta con il GDPR; è infatti ragionevole ritenere che un ISP, avente nella maggior parte dei casi la sede legale all'estero, ancor prima di dotarsi di un MOG ai sensi del D.Lgs. 231/2001 abbia attuato un c.d. "modello organizzativo *privacy*", il quale, pur tenendo conto del diverso ambito di applicazione e dei diversi fini di tutela, potrà eventualmente costituire un punto di rifermento nella successiva predisposizione del modello previsto dal Decreto. Sul punto sia consentito rinviare a COSTA D., *I modelli 231 e la compliance aziendale sulla tutela dei dati personali. Aspetti comuni e divergenze a quattro anni di distanza dall'entrata in vigore del GDPR,* in Giurisprudenza Penale, 5/2020.

Ed invero, con riferimento alla responsabilità omissiva, l'ordinamento italiano pare adottare come postulato l'esclusione *tout court* dell'attribuzione all'ISP di un ruolo di "controllore" rispetto alle condotte illecite aventi luogo nel ciberspazio, in relazione alle quali l'intero panorama legislativo interno continua a negare, in capo al *provider,* posizioni di garanzia ovvero obblighi di sorveglianza.
La linea adottata dal legislatore risulta peraltro condivisa, ad oggi, anche dalla giurisprudenza prevalente, come testimoniato dal citato caso *Google – Vivi Down*.
A ben vedere, tuttavia, allo stato attuale l'esclusione dallo statuto penale dell'ISP di una responsabilità *ex* art. 40 c. 2 c.p. non è una scelta criticabile.
La penale irrilevanza di una responsabilità concorsuale "omissiva" si presenta infatti coerente con i valori tecnico-giuridici su cui si reggono la rete internet e il diritto penale, aventi ad oggetto, rispettivamente, la neutralità della rete (in virtù della quale il web non potrebbe essere sottoposto ad alcun vaglio censorio preventivo) e il rispetto di quei principi di legalità e colpevolezza che precludono l'addebito ad un soggetto del mancato impedimento di un reato da altri realizzato in assenza di una norma che fondi tale obbligo, di un potere giuridico-tecnico idoneo a scongiurare l'illecito altrui e, infine, dell'effettiva conoscenza del compimento di reati da parte degli utenti dei propri servizi.[114]
Maggiori margini applicativi si intravedono invece in relazione al modello di *accountability* del *provider* inteso come soggetto obbligato ad attivarsi in seguito alla commissione dei reati; tuttavia, anche in questo caso, in assenza di una fattispecie che si rivolga direttamente al prestatore di servizi di rete rimasto inerte a fronte di illeciti commessi tramite i servizi da lui offerti*,* sarà comunque necessario andare ad accertare quale, tra le differenti ipotesi di reato di parte speciale, possa eventualmente applicarsi nel caso concreto.
Occorre in ogni caso tenere a mente che le conseguenza penalmente rilevanti in caso di inerzie e ritardi nell'attivazione della procedura di *notice and take down* sono limitate ai casi in cui l'ISP si interfacci con un'autorità pubblica, amministrativa o giurisdizionale che sia, e non anche alle sempre più numerose ipotesi, previste in particolar modo dalla legislazione sulla tutela del diritto d'autore, in cui l'intimazione a rimuovere i contenuti pubblicati online e a disabilitarne l'accesso provenga da un privato cittadino titolare di privative violate dai fruitori della rete.
Infine, sembra invece più agevole la responsabilizzazione dell'ISP come concorrente attivo nel reato commesso dagli utenti: ed invero, i pochi dubbi sull'ammissibilità del concorso materiale nei reati sono stati definitivamente dissipati dall'art. 102 *septies* L. Aut., introdotto dal D.Lgs. 177/2021, che

[114] V. INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine*.

esclude ogni limitazione di responsabilità per il *provider* che agevoli condotte aventi ad oggetto l'illecita condivisione di opere dell'ingegno in rete; ad ogni modo, anche la responsabilità penale *ex* art. 110 c.p. dell'ISP presenta alcune criticità con riferimento alla corretta individuazione di quelle condotte, poste in essere su un piano informatico e virtuale, che possono tradursi in un'agevolazione o in un contributo eziologico alla realizzazione dei delitti da parte dei fruitori dei servizi di rete messi a disposizione dal *provider*.

Certo è che non può negarsi l'impatto potenzialmente dirompente che presenterà l'attuazione della Direttiva Copyright 790 del 2019 tramite il D.Lgs. 177/2021, soprattutto nella parte in cui introduce l'onere per l'*hosting provider* che fornisca piattaforme di condivisione online dove gli utenti possono caricare contenuti di ottenere la licenza dai titolari dei diritti d'autore sulle opere dell'ingegno immesse nel ciberspazio.

Ed invero, nel caso in cui tale autorizzazione manchi, così come nel caso in cui l'ISP non abbia posto in essere i "massimi sforzi" per ottenerla, opererà l'esclusione dell'applicazione del regime di esonero da responsabilità previsto dal D.Lgs. 70/2003. Può dunque presumersi che non saranno rari i casi in cui le contestazioni per reati in materia di diritto d'autore saranno dirette anche verso gli ISP stessi, sia in termini di concorso attivo nelle ipotesi di vera e propria partecipazione dolosa nei reati che in termini di concorso omissivo qualora i fornitori di servizi di rete abbiano consapevolmente omesso di vigilare sulle attività di *upload* di materiale non autorizzato da parte degli utenti di internet.

Peraltro, oltreché sul piano giuridico, le criticità relative all'addebito di una penale responsabilità all'ISP si presentano anche da un punto di vista tecnico; le attività tipiche poste in essere nel ciberspazio dai fornitori di servizi digitali, infatti, spesso e volentieri sono del tutto automatizzate e, come ovvio, si manifestano sotto forma di numeri binari; le stesse, pertanto non sono direttamente e fisicamente riscontrabili nel mondo fisico, come invece potrebbe dirsi per un accesso abusivo ad un sistema informatico realizzato da una persona fisica mediante la pressione di tasti su una tastiera o per un *upload* di contenuti protetti facilmente riconducibile ad un determinato *device* tramite l'individuazione dell'indirizzo IP di riferimento.

Da ciò consegue una difficoltà di fondo nell'accertamento delle modalità di estrinsecazione della condotta ascrivibile ai *providers* e, non da ultimo, nella dimostrazione della consapevolezza dolosa, in capo all'ISP, della partecipazione attiva od omissiva in un reato commesso in rete. E' indubbia, pertanto, la necessità di un accrescimento delle competenze informatiche e digitali da parte di tutti gli operatori del diritto penale, siano essi esponenti della P.G., Pubblici Ministeri o difensori, che renda per essi più agevole tipizzare le attività dei prestatori di servizi di rete all'interno dei tradizionali istituti del diritto penale.

In ogni caso, in una prospettiva *de jure condito,* è evidente che una più chiara e uniforme disciplina sulla responsabilità penale dell'ISP per i reati informatici contro la proprietà intellettuale non potrà che passare da un riordino e da una razionalizzazione dei delitti in materia di diritto d'autore, eventualmente anche con la previsione di una fattispecie *ad hoc* rivolta proprio verso coloro che rendono possibile la circolazione e diffusione delle opere dell'ingegno nella rete delle reti.
Certo è che ogni possibile risposta penale diretta a far fronte alle esigenze di tutela rispetto alle condotte illecite poste in essere dai fornitori dei servizi della società dell'informazione non potrà esimersi dal modulare il trattamento sanzionatorio tenendo conto delle immani capacità economiche di tali soggetti e della sempre maggiore influenza esercitata dagli stessi nei confronti della politica e della società; in caso contrario, infatti, sarà inevitabile che, ancora una volta, il diritto si trovi nuovamente a rincorrere, senza speranza di raggiungere, lo sviluppo tecnologico e l'ascesa dei giganti del web.