Dipartimento di Giurisprudenza
Cattedra di Diritto Penale 2

PROFILI PENALISTICI DELLA RESPONSABILITÀ DEL *PROVIDER*

RELATORE
Chiar.mo Prof.
Antonino Gullo

CANDIDATA
Gaia Berlese – Matr. 190993

CORRELATORE
Chiar.mo Prof.
Enrico Gallucci

ANNO ACCADEMICO 2024/2025

INDICE

INTRODUZIONE

Internet ha assunto e continua ad assumere un ruolo fondamentale nel mondo moderno e, in tale contesto, gli *Internet Service Provider* rappresentano una figura indefettibile, poiché necessari per l'accesso alla rete e ai servizi a essa connessi.

Il presente elaborato si incentra sull'analisi dei profili penalistici della responsabilità degli ISP ed è volto ad offrire un quadro sistematico e comparato attraverso l'analisi normativa e giurisprudenziale sviluppatasi sul tema in ambito nazionale, europeo e internazionale, con particolare riguardo all'ordinamento statunitense.

Il lavoro si articola in tre capitoli. Nel primo capitolo viene proposta una panoramica generale relativa alla figura dei *provider*, in cui viene delineato il contesto operativo di questi intermediari e il quadro normativo di riferimento.

In particolare, dopo aver ricostruito l'evoluzione storica e sociale di Internet nonché i rischi connessi al suo utilizzo, viene delineato il ruolo degli ISP e le diverse tipologie di operatori individuati dalla normativa vigente a livello nazionale e internazionale. Segue l'analisi del progressivo cambiamento del ruolo dell'ISP, che da mero intermediario tecnico si è trasformato in attore centrale, non solo nel controllo del flusso e dell'accesso all'informazione, ma anche nella prevenzione e nella gestione dei rischi cibernetici. Si analizza altresì il contesto operativo degli ISP, sottolineando le caratteristiche peculiari della rete in cui operano e i possibili profili di responsabilità.

Successivamente, si prende in esame il quadro normativo di riferimento, ricostruito su più livelli. Sul piano internazionale, assumono particolare rilievo l'Unione internazionale delle telecomunicazioni e la Convenzione di Budapest del 2001, considerato il primo strumento giuridico di contrasto alla criminalità informatica. A livello europeo, invece, si evidenzia come la normativa di riferimento si sia stratificata nel tempo: partendo dalla Direttiva sul commercio elettronico del 2000, che ha introdotto un regime di responsabilità condizionata per i *provider*, passando per la Direttiva del 2011 sull'abuso sessuale e la pedopornografia *online*, per la Direttiva 790/2019 sul diritto d'autore nel mercato

unico digitale e per il Regolamento 2021/784 relativo al contrasto della diffusione di contenuti terroristici *online*, fino ad arrivare alla più recente disciplina contenuta nel *Digital Services Act*.

Infine, l'analisi si concentra sulla normativa nazionale vigente: l'ordinamento italiano, originariamente, si è limitato a recepire formalmente la citata Direttiva *e-commerce* mediante la legge delega n. 39/2002 e il d.lgs. n. 70/2003, senza introdurre sanzioni penali per i *provider*, ma privilegiando strumenti di tutela civile e alcune sanzioni amministrative.

Con l'entrata in vigore del *Digital Services Act* (DSA), la normativa nazionale è chiamata ad adeguarsi a un quadro europeo più vincolante. L'art. 49 del DSA impone agli Stati membri di designare una o più autorità competenti per garantire l'attuazione del Regolamento, nonché un coordinatore dei servizi digitali dotato di poteri di indagine, esecuzione e sanzione. In Italia, tale compito è stato affidato all'AGCOM. Il coordinatore è chiamato ad agire in piena indipendenza e nel rispetto dei diritti fondamentali, adottando misure efficaci e proporzionate, comprese sanzioni pecuniarie, ordini ingiuntivi e, nei casi più gravi, la temporanea restrizione dell'accesso ai servizi.

Il secondo capitolo è dedicato all'analisi dei profili penalistici della responsabilità degli *Internet Service Provider*.

Dapprima viene esaminato il quadro normativo europeo e nazionale, sottolineando il ruolo centrale assunto dal menzionato d.lgs. n. 70/2003, che ha introdotto un regime di responsabilità condizionata per gli ISP in attuazione degli obblighi europei. Sul punto, si è affrontato il tema degli obblighi informativi a carico dei fornitori di servizi *online*, mettendo altresì in luce come, nei suoi sviluppi normativi più recenti recati dal *Digital Services Act*, il legislatore eurounitario abbia rafforzato gli obblighi di trasparenza e diligenza, pur ponendosi – in relazione alla responsabilità del *provider* – in sostanziale continuità con la normativa precedente. L'attenzione si concentra poi sulla definizione degli ambiti di responsabilità delle diverse tipologie di prestatori, approfondendo il tema della responsabilità penale degli ISP con riguardo ai possibili paradigmi di imputazione in tale contesto – ovverosia responsabilità omissiva, monosoggettiva autonoma e concorsuale – e, sul piano settoriale, guardando alle ipotesi di diffamazione *online* e pedopornografia.

Nel prosieguo del lavoro viene esaminata la controversa questione dell'elemento soggettivo del reato: sul punto, si considera la posizione del *provider* tra dolo e colpa, nonché il rapporto con il principio costituzionale della personalità della responsabilità penale sancito dall'art. 27 Cost..

Inoltre, si analizzano gli obblighi di segnalazione e rimozione dei contenuti illeciti propri del meccanismo di *notice and action* introdotto dal più volte evocato Regolamento europeo sui servizi digitali, volto a rafforzare i meccanismi di moderazione e trasparenza delle piattaforme digitali.

L'elaborato esamina anche due significativi casi giurisprudenziali in materia di dati personali, che permettono di mettere in luce come il tema della responsabilità degli ISP si sia rivelato complesso e spesso soggetto a interpretazioni contrastanti: le vicende *Google vs ViviDown*, decisa dalla Corte di Cassazione, *Google vs Spain*, giunto all'attenzione della Corte di Giustizia dell'Unione europea, pervenuti a conclusioni opposte, offrono un esempio di tale contrasto.

A conclusione dell'elaborato, nel terzo capitolo, è dedicato ampio spazio all'analisi della disciplina statunitense in materia di responsabilità degli ISP, con l'obiettivo di ricostruire il quadro normativo e giurisprudenziale di riferimento.

In particolare, si prendono le mosse dalla descrizione delle principali forme di responsabilità riconosciute negli Stati Uniti – *direct liability*, *contributory liability* e *vicarious liability* – evidenziando come l'approccio americano, a differenza del modello europeo che appare più garantista e attento ai diritti fondamentali, si caratterizzi per un'impostazione liberista, improntata a una maggiore tutela della libertà di espressione.

In seguito, l'analisi si concentra sul *Communications Decency Act* del 1996, con particolare attenzione alla Sezione 230, quale norma che ha introdotto un ampio regime di immunità per i *provider*, e sul *Digital Millenium Copyright Act* del 1998, volto a rafforzare la tutela del diritto d'autore nell'era digitale. Quest'ultimo ha introdotto i c.d. *safe harbors* – che limitano la responsabilità civile degli ISP – e la procedura di *notice and action*, oggetto di confronto con la disciplina europea, contenuta nella Direttiva *e-commerce* prima e nel *Digital Services Act* poi.

Infine, viene analizzata la principale giurisprudenza delle Corti statunitensi, e si dedica attenzione in particolare a quattro casi emblematici – *Cubby v.*

Compuserve Inc. (1991), *Stratton Oakmont Inc. v. Prodigy Services Co.* (1995), *Zeran v. American On Line* (1997) e *Force v. Facebook* (2019).

L'analisi dei primi due casi consente di comprendere le premesse storico-normative che hanno portato all'introduzione della *Section 230* del CDA, mentre il terzo caso ne rappresenta la prima applicazione pratica. La quarta pronuncia, più recente, consente di evidenziare come la dottrina inaugurata con la sentenza *Zeran v. AOL* – che ha escluso la responsabilità dei *provider* per i contenuti generati da terzi, anche quando siano stati informati della loro natura illecita – sia stata estesa anche a contesti più gravi, come quelli legati al terrorismo, mettendo in luce le possibili conseguenze penali derivanti dall'ampia immunità garantita dalla *Section* 230.

CAPITOLO I

GLI *INTERNET SERVICE PROVIDER*

1.1. Evoluzione storico-normativa della rete *Internet*

La rete Internet viene considerata una delle innovazioni più rivoluzionarie e, ad oggi, si è affermata come il principale mezzo di comunicazione di massa, un mezzo ormai imprescindibile. È evidente che Internet e, in generale, gli strumenti tecnologici e informatici, rivestano un ruolo sempre più crescente nella vita quotidiana.

La nascita di Internet si riconduce al periodo della guerra fredda, quando il Dipartimento di Difesa statunitense, per rispondere al lancio del primo satellite artificiale russo costruito dall'uomo, avviava il progetto ARPA (*Advanced Research Project Agency*), che si prefiggeva l'obiettivo di stimolare il progresso in ambito militare, attraverso progetti strategici di grande rilevanza.

In particolare, era stata posta molta attenzione allo sviluppo di sistemi per l'interconnessione tra computer, un'idea che in quegli anni stava iniziando a diventare tecnicamente possibile[1].

Nel 1969, infatti, nasceva ARPANET (*Advanced Research Projects Agency NETwork*), che è stata la prima rete operativa basata sulla tecnologia della commutazione di pacchetto, e ad oggi adottata da tutte le reti di trasmissione dati e voce[2].

La rete informatica aveva iniziato ad espandersi connettendo nuovi nodi, principalmente università e aziende coinvolte in progetti militari. Tanto che, nel 1972 ARPA ha cambiato nome in DARPA (*Defense Advanced Research Projects Agency*) per riaffermare la sua funzione difensiva originaria.

Una delle prime iniziative della nuova DARPA era stata quella di estendere la tecnologia della commutazione di pacchetto alle reti *wireless*, riconoscendone il potenziale strategico in ambito militare[3].

---

[1] Così BOLISANI, GOTTARDI, *Nascita ed evoluzione di* Internet, in GARRONE, MARIOTTI (a cura di), *L'economia digitale*, Bologna, 2001, 4 ss.
[2] Cfr. SIGNORE, *Origini, motivazioni e regole di evoluzione del* World Wide Web, relazione presentata al convegno di *Storia dell'informatica*, Pisa, 4 maggio 2009, W3C Italia – CNR.
[3] Sul punto BOLISANI, GOTTARDI, *Nascita ed evoluzione di* Internet, cit. 6.

A seguito di continui sviluppi, nel 1973 Robert E. Kahn e Vinton Gray Cerf[4], avevano lavorato insieme per sviluppare un protocollo universale che permetteva l'interconnessione tra reti eterogenee.

Infatti, la proposta da loro strutturata prevedeva di attribuire la responsabilità della trasmissione dei dati, non più alla Rete, ma agli *host*. Le sperimentazioni che seguirono portarono poi al perfezionamento della transizione di ARPANET al Protocollo TCP/IP.

Intorno al 1980 anche nel CERN (*European Organization for Nucelar Research*) iniziava a diffondersi sempre più insistentemente l'uso della tecnologia delle reti e, nel 1989, con la nascita del collegamento ufficiale a Internet, il CERN è diventato il principale polo informatico europeo[5].

Tutto ciò ha posto le basi per la realizzazione del *World Wide Web*.In particolare, Tim Berners-Lee[6], aveva l'idea di rendere il computer più intuitivo, permettendogli di realizzare connessioni tra più informazioni in modo simile alla mente umana.

Nel 1989 aveva proposto un nuovo sistema di condivisione di informazioni, segnando la nascita di HTML. Parallelamente, nacque un nuovo *personal computer*, denominato NeXT, che si prestava ad essere idoneo per questo progetto, grazie alle sue caratteristiche.

Così Berners-Lee lo aveva utilizzato per realizzare il suo progetto. Il primo *browser* che venne realizzato, in linea con l'idea che il *Web* dovesse favorire la collaborazione, consentiva la visualizzazione e l'aggiornamento dei contenuti. Fino a che, nell'ottobre del 1994, con la collaborazione del CERN e il supporto di DARPA e della Commissione Europea, Tim Berners-Lee fonda il *World Wide Web Consortium* (W3C).

---

[4] Robert E. Kahn e Vinton Gray sono stati una figura chiave nello sviluppo di Internet. Entrambi informatici di origine statunitense, hanno collaborato negli anni '70 per lo sviluppo del protocollo TCP/IP, elemento fondamentale per l'interconnessione tra reti.

[5] In tal senso SIGNORE, *Origini, motivazioni e regole di evoluzione del* World Wide Web, cit., 3 ss.

[6] Tim Berners-Lee, fisico e informatico britannico nato nel 1955, è noto come l'inventore del *World Wide Web*. Nel 1989, mentre lavorava al CERN, ideò con Robert Cailliau un progetto per la condivisione globale dell'informazione via Internet. Realizzò il primo *server web*, il primo *browser/editor* e contribuì alla creazione di tecnologie fondamentali come HTML, URL e HTTP. Nel 1994 fondò il World Wide Web Consortium (W3C) al MIT, che definisce gli standard del *web*.

Il W3C è un consorzio che riunisce più organizzazioni internazionali, che stabilendo protocolli comuni che stimolino l'evoluzione e garantiscano l'interoperabilità del *Web*, con l'obiettivo di svilupparlo al massimo delle sue potenzialità[7].

Il *Web* si è evoluto nel tempo e continua ad evolversi costantemente. Infatti, gli utenti hanno acquisito un ruolo attivo: contribuiscono alla creazione e aggiungono contenuti, non limitandosi più a fruire passivamente delle informazioni.

Si è passati così al *Web 2.0*[8], che poggia su tre fondamenti: interazione, condivisione e partecipazione. Difatti, con il *Web 2.0* si assiste alla nascita e allo sviluppo di una società partecipativa in Rete, grazie anche alla diffusione di *social network*.

Sin dalla prima comparizione di Internet, la letteratura scientifica si è occupata delle sue implicazioni giuridiche, in particolare dei problemi legati allo spazio giuridico creato dal cyberspazio. L'aspetto centrale è però capire se il diritto dell'Internet consiste in un'estensione e adattamento del preesistente diritto nazionale, comunitario e internazionale, oppure, se è necessario elaborare un nuovo sistema giuridico che sia in grado di rispondere alle esigenze introdotte dalle innovazioni tecnologiche[9].

Le caratteristiche peculiari di Internet, quali l'istantaneità, l'immediatezza e la natura interattiva, rendono complessa la sua regolamentazione[10].

Il mondo digitale non è stato concepito come un mondo dotato di regolamentazione giuridica, bensì basato su un'autoregolamentazione tecnica. Da un lato, questo modello aspirava a superare i limiti territoriali su cui si basano i governi tradizionali e, dall'altro, era volto a garantire la libertà degli utenti.

---

[7] V. SIGNORE, *Origini, motivazioni e regole di evoluzione del* World Wide Web, cit., 4 ss.
[8] Termine coniato da Tim O'Reilly.
[9] Sul punto FROSINI, *L'orizzonte giuridico dell'*Internet, in *Dir. inf.*., 2000, 2, 279.
[10] Cfr. ALÙ, *I problemi giuridici di* Internet*: il dibattito sul diritto all'uguaglianza digitale*, in *Agenda Digitale*, 2015, 5.

Tutto ciò ha portato alla teorizzazione della *Lex Informatica*[11], quell'insieme di regole predisposte dalla tecnologia per la gestione delle reti di comunicazione e i flussi informatici, che concorrono parallelamente alle norme giuridiche[12].

Successivamente, tuttavia, la struttura così pensata, a causa dell'insistenza delle *tech companies*[13], è divenuta più complessa portando a una modificazione delle modalità di accesso e di utilizzo della Rete.

La sua regolamentazione, di conseguenza, non è più avvenuta solo con leggi dirette, ma sempre più tramite il codice. Il diritto, in Internet, viene trasmesso attraverso il codice e, per questo motivo, che diversi autori hanno teorizzato il passaggio dalla *Rule of Law* alla *Rule of Code*.

In particolare, Lawrence Lessig è partito dal presupposto per il quale «Life in cyberspace is regulated primarily through the code of cyberspace»[14]. Ciò significa che è il codice a disciplinare il *cyberspace*, prima ancora delle norme giuridiche, proprio perché è sul codice che esso si fonda.

Tuttavia, questo non impedirebbe agli Stati di regolare il cyberspazio, ma essi dovrebbero prima intervenire sul codice: sarebbe molto più efficace trovare un espediente tecnologico piuttosto che un espediente giuridico, poiché il diritto potrebbe non essere in grado di intervenire in modo efficace e tempestivo[15].

Tutte le piattaforme digitali si sono dotate di un sistema di moderazione dei contenuti che si basa tanto su regole implicite quanto su regole esplicite: le regole implicite si riferiscono al codice, quindi alla struttura logica della piattaforma; a contrario, le regole esplicite sono le regole che definiscono ciò che è consentito e ciò che è vietato fare, contenute nei documenti ufficiali.

---

[11] V. REIDENBERG, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, in *Texas Law Review*, 1998, 568: «Lex Informatica, however, allows for automated and self-executing rule enforcement. Technological standards may be designed to prevent actions from taking place without the proper permissions or authority»

[12] In argomento, MAESTRI, Lex Informatica*. Diritto, persona e potere nell'età del cyberspazio*, in ESI, Napoli, 2015.

[13] Una *tech company* è un'azienda il cui modello di business dipende in modo imprescindibile dall'uso della tecnologia. Può trattarsi di imprese che sviluppano direttamente soluzioni tecnologiche – come *software*, dispositivi digitali o infrastrutture –oppure di aziende che impiegano la tecnologia come risorsa centrale per offrire i propri prodotti o servizi. Non è sufficiente possedere una presenza *online* per essere considerati *tech*: ciò che distingue una vera *tech company* è l'impossibilità di operare senza l'innovazione tecnologica su cui si basa.

[14] V. LESSIG, *Code. Version 2.0*, New York, 2006.

[15] In tal senso BETZU, *Poteri pubblici e poteri privati nel mondo digitale*, in *Riv. GdP*, 2021, 2, 166 ss.

Grazie a queste regole, le piattaforme digitali hanno dato vita a un ordinamento para-giuridico, che definisce i divieti, configura la responsabilità degli utenti e ne sancisce diritti. Per quanto riguarda i meccanismi di moderazione, si distingue un'attività *ex ante* e un'attività *ex post*.

Attraverso la moderazione *ex ante* si effettua un controllo prima che il contenuto venga pubblicato, mediante sistemi di filtraggio dei contenuti basati su algoritmi capaci di riconoscere le attività qualificate come vietate.

Con la moderazione *ex post* si effettua, invece, un controllo dopo che il contenuto è stato pubblicato. Una prima tipologia di moderazione *ex post* è compiuta direttamente dalle piattaforme ed è finalizzata all'individuazione di contenuti ritenuti pericolosi. Una seconda tipologia è volta ad esaminare se i contenuti sono conformi alle linee guida della piattaforma, sulla base di segnalazione da parte degli utenti[16].

La diffusione globale della Rete ha reso alquanto controversa la sua regolamentazione, poiché Internet non è solo un'infrastruttura tecnologica, ma ha profonde conseguenze anche sugli aspetti economici, politici e sociali[17].

Bisogna considerare che Internet evolve in continuazione e, per gli ordinamenti giuridici, un adattamento immediato è quasi impossibile, proprio perché richiede del tempo: per questo motivo, vi è il rischio che la normativa diventi obsoleta già al momento della sua entrata in vigore.

Pur costituendo un nuovo mezzo di comunicazione e di portata innovativa, la Rete viene considerata giuridicamente regolabile. Tuttavia, è fondamentale coordinare le norme tra i vari ordinamenti statali. Tale armonizzazione dovrebbe avvenire attraverso il diritto internazionale, stabilendo regole generali comuni e, in questo modo, si può consentire ad ogni Stato di adottare leggi di dettaglio che si inseriscano all'interno di un quadro condiviso[18].

Pertanto, è evidente che regolamentare Internet sia indispensabile per arginare la possibilità che il suo utilizzo possa ledere diritti e interessi altrui.

---

[16] Cfr. BETZU, *Poteri pubblici e poteri privati nel mondo digitale*, cit., 174 ss.
[17] Così ALÙ, *La* Governance *di* Internet *oltre gli Stati? Gli inediti tratti del futuro ecosistema digitale*, in *RIID*, 2022, 251 ss.
[18] V. RUOTOLO*, Le fonti dell'ordinamento internazionale e la disciplina della Rete*, in *DPCE online*, 2021, 705.

1.1.1. I rischi connessi all'uso di *Internet*

Nonostante questi strumenti informatici rappresentino delle opportunità per il progresso in generale, talvolta l'utilizzo degli stessi può essere rischioso e, conseguentemente, possono essere considerati anche come una minaccia[19].

Originariamente non si era presa in considerazione la duplice funzione che lo strumento di Internet avrebbe potuto avere: da un lato, utile a promuovere e stimolare la libera circolazione delle informazioni e delle idee; dall'altro, quale strumento per contribuire all'amplificazione di fenomeni tutt'altro che positivi[20].

Ad oggi, le nuove tecnologie vengono comunemente definite *Dual Use Technologies*, poiché il loro impiego non solo può offrire delle opportunità di progresso per la società ma, al contempo, possono essere sfruttate dalla criminalità per finalità illecite.

In quest'ottica, quindi, i reati informatici rappresentano l'aspetto negativo della digitalizzazione. Per questo, è centrale il ruolo che il diritto penale assume nella regolamentazione di Internet.

Lo spazio virtuale e gli illeciti commessi in rete hanno infatti delle caratteristiche peculiari, che possono mettere a repentaglio l'efficacia general-preventiva e la deterrenza tipiche della sanzione penale[21]. È proprio in virtù di questa consapevolezza che si è avvertita l'esigenza di introdurre delle fattispecie *ad hoc* volte a contrastare tali fenomeni criminosi.

La locuzione "reati informatici" può essere interpretata in due modi. Da un lato, si indicano reati informatici in senso ampio ovverosia tutti i reati già previsti dall'ordinamento, ma che possono essere commessi anche con modalità informatiche. Dall'altro, per reati informatici in senso stretto si fa riferimento a tutte quelle condotte in cui l'utilizzo del mezzo tecnologico è un elemento costitutivo

[19] Sul punto CAMISA, SIMONCINI, *Il fattore umano e la regolazione della* cybersecurity, in *Mondo Digitale*, 2024, 2.
[20] Cfr. MATTARELLA, *La futura Convenzione ONU sul* cybercrime *e il contrasto alle nuove forme di criminalità informatica*, in *Sist. pen.*, 2022, 3, 44.
[21] Così GARGANI, *Tra sanzioni amministrative e nuovi paradigmi punitivi: la legge delega di 'riforma della disciplina sanzionatoria' (art. 2 l. 28.4. 2014 n. 67)*, in *Leg. pen*., 2015, 14.

della fattispecie, a prescindere dal fatto che sia lo strumento attraverso cui si commette il reato o l'oggetto materiale del reato[22].

Fino agli inizi degli anni Novanta, l'ordinamento italiano non prevedeva una disciplina specifica per i crimini informatici.

Tuttavia, il legislatore italiano è stato tra i primi legislatori europei ad occuparsi di criminalità informatica, introducendo la l. 547/1993[23]. L'adozione di questa legge è stata incentivata dalla Raccomandazione del Consiglio d'Europa del 1989 sulla criminalità informatica, in cui erano menzionate le condotte illecite che potevano realizzarsi nel mondo informatico e che si auspicava fossero oggetto di introduzione da parte dei diversi Stati membri.

Nello specifico, tale raccomandazione conteneva una lista essenziale di tutte le fattispecie che dovevano necessariamente previste dall'ordinamento e una lista facoltativa di ulteriori fattispecie, la cui introduzione, si fondava su una scelta discrezionale degli Stati.

In questo senso, la raccomandazione assolveva a un duplice obiettivo: in primo luogo, colmare le lacune normative esistenti; in secondo luogo, elaborare una strategia uniforme di contrasto a questi fenomeni[24].

L'analisi dei reati cibernetici offre degli spunti di riflessione di teoria generale del reato. Gli istituti fondamentali del diritto penale, quali azione, evento, nesso di causalità, sono stati concepiti dal legislatore con riferimento ad attività che si svolgono nella realtà materiale.

Pertanto, questi istituti fondamentali si sono dovuti reinterpretare in virtù dei cambiamenti introdotti dal progresso tecnologico. Proprio perché, come si è visto, tali reati si consumano nella realtà cibernetica attraverso impulsi elettronici.

Un aspetto preoccupante riguarda anche l'a-territorialità degli illeciti commessi tramite Internet: la rete è ovunque, ma allo stesso tempo in nessun luogo. Non ci sono confini statali e, spesso, il reato informatico è commesso a distanza.

---

[22] Sul punto MONACO, *Prolegomena alla riforma del diritto penale dell'informatica nell'ordinamento giuridico della repubblica di San Marino*, in *Studi Urb., A - Sci. Giur. Pol. Econ.*, 2016, 3-4, 339.

[23] In argomento BLENGINO, *I reati della rete e la costruzione dei rischi nello spazio digitale*, in *Antigone*, 2008, 3, 111.

[24] Cfr. LARINNI, *Garantismo europeista: un ossimoro? A proposito dell'accesso abusivo ad un sistema informatico o telematico (615-ter c.p.)*, in *Criminalia*, 2019, 309 ss.

Tale aspetto si riflette sul piano penalistico, rendendo difficile capire chi è l'autore del reato e il luogo in cui questo è stato commesso[25].

La nascita del mondo digitale ha fatto venire meno i confini spazio-temporali. Il *cyberspace*, infatti, è un luogo infinito e senza tempo, che prescinde da qualsiasi interazione fisica.

Le modalità di relazione sociale sono cambiate in maniera significativa, facendo sì che le forme di comunicazione siano necessariamente mediate dagli *Internet Service Provider*.

La mancanza di vincoli e confini consente di operare sul *Web* in modo continuo e trasversale, alimentando al contempo l'illusione di poter agire in modo del tutto anonimo. Ed invero, poiché non è sempre possibile individuare l'autore di una condotta antigiuridica, è necessario indentificare in ogni caso un soggetto da ritenere responsabile della violazione[26].

In tale contesto, emerge dunque la necessità di delineare i profili di responsabilità degli ISP, rispetto a tutti gli illeciti che possono essere compiuti sul *Web*, senza però inibire lo sviluppo della rete[27].

La crescita di fenomeni, quali la diffusione di contenuti illeciti e la criminalità informatica, ha infatti portato all'intensificazione del dibattito normativo in materia di responsabilità penale dei *provider.*

1.2. Gli *Internet Service Provider*

L'art. 2, lett. b), della direttiva 2000/31/CE (c.d. *direttiva e-commerce*) definisce l'*Internet Service Provider* come «la persona fisica o giuridica che presta un servizio della società dell'informazione»[28].

Dunque, *provider* sono tutti coloro che offrono un servizio accessibile tramite *Internet*. Tale servizio viene definito "della società dell'informazione", vale

[25] V. PICOTTI, *Reati informatici, riservatezza, identità digitale*, in *AIPDP*, s.d., 1 ss.
[26] Cfr. TAVERNITI, *Profili di responsabilità dell'*internet service provider *tra disciplina vigente e nuove esigenze di tutela*, in*. Camm. dir.*, 2022, 2.
[27] Cfr. IMPERADORI, *La responsabilità dell'*Internet Service Provider *per violazione del diritto d'autore: un'analisi comparata*, in *Lawtech*, 2014, 3.
[28] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (Direttiva sul commercio elettronico).

a dire «qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi»[29].

Da queste premesse si può, quindi, desumere che i *provider* sono una figura indefettibile: senza di essi non sarebbe possibile utilizzare la rete nelle modalità in cui è attualmente utilizzata.

La figura degli *Internet Service Provider* è stata riconosciuta negli anni'90: gli stessi venivano considerati dei semplici operatori capaci di fornire accesso alla rete *online*.

Tuttavia, a fronte della diffusione esponenziale di Internet, i *provider* hanno assunto dei ruoli sempre più centrali, diventando protagonisti non solo per l'accesso alla rete, ma anche per i servizi ad essa collegati[30].

Fondamentale è stato il ruolo delle università e dei centri di ricerca che tra il 1980 e il 1990 hanno favorito l'ingresso di Internet in Italia. Altrettanto fondamentale sul tema è stato il ruolo assunto dal Consiglio Nazionale della Ricerca (CNR) e la rete GARR[31] (Gruppo di Armonizzazione delle Reti della Ricerca).

In poco tempo anche aziende ed enti no-profit iniziarono a collegarsi a *Internet* tramite IUNet, che oltre a consentirgli di accedere alla rete gli ha permesso di comunicare verso l'estero, in particolare con gli Stati Uniti.

Tuttavia, i privati che si collegavano a IUNet erano pochi. La diffusione del primo *browser Web*, c.d. *Mosaic*, e l'inclusione del *software* TCP/IP in un sistema operativo *Microsoft Windows* rappresentano due dei principali eventi che hanno consentito lo sviluppo dell'accesso a Internet da parte degli utenti privati, entrambi avvenuti nel 1993. Ed è proprio in quell'anno che nacque il primo ISP chiamato *Video On Line* (VOL), progettato proprio per l'accesso dei privati. VOL si distingueva per il fatto di offrire l'accessibilità alla Rete in modo totalmente

[29] Art. 1, paragrafo 1, lettera b), Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (codificazione) (Testo rilevante ai fini del SEE).
[30] In tal senso MOLINARI, *Nascita, evoluzione e funzionamento della rete*, in *Filodiritto*, 2008, 4 ss.
[31] "*GARR è la rete nazionale ad altissima capacità dedicata alla comunità dell'istruzione, della ricerca e della cultura. Il suo principale obiettivo è quello di fornire connettività ad alte prestazioni e di sviluppare servizi innovativi per le attività quotidiane di docenti, ricercatori e studenti e per la collaborazione a livello internazionale*".

gratuito, sebbene, per poter usufruire di questo servizio, gli utenti dovevano fornire numerosi dati personali.

Ma, la gratuità del servizio offerto ha reso VOL il più grande ISP italiano. Durante quel periodo, oltre a colossi come *Italia On Line* e *Telecom Online*, si affermarono anche ISP locali di dimensioni ridotte[32].

Senza gli ISP gli utenti non potrebbero connettersi direttamente alla rete Internet, in quanto essa è accessibile solo tramite di essi. Nello specifico, il *provider* fornisce agli utenti un *Internet Protocol* (IP) affinché possano comunicare con altri dispositivi connessi alla rete. Infatti, l'indirizzo IP immette e favorisce lo scambio di informazioni, permettendo ai dispositivi degli utenti di interagire con gli altri terminali sulla rete.

In via generale, una distinzione basata sulla funzionalità è tra *Internet access provider* (IAP) e *Internet content provider* (ICP). Per poter accedere alla rete e godere dei vari beni e servizi da essa offerti è necessario stipulare un contratto con l'IAP, in base al quale egli fornirà le credenziali di accesso, quali password, nome utente e *browser*[33], affinché gli utenti possano navigare nel Web. L'IAP, a tal proposito, si appoggia a fornitori e gestori di infrastrutture e affitta una linea che conduce gli utenti dal punto di accesso (POP – *point of presence*) alle dorsali di telecomunicazioni (*backbone*). Diversamente, l'ICP non si limita a fornire l'accesso alla Rete, ma provvede alla creazione e alla diffusione di contenuti online, fornendo, inoltre, ulteriori servizi[34].

1.2.1. Le tipologie di ISP: *Mere Conduit Provider*, *Caching Provider* e *Hosting Provider*

[32] Così AJMONE MARSAN, GUADAGNI, LENZINI, *Le reti a pacchetto*, CANTONI, FALCIASECCA, PELOSI (a cura di), in *Storia delle telecomunicazioni I*, Firenze, 2011, 271 s.
[33] V. definizione fornita da Enciclopedia Treccani in cui browser è definito come l'"*Applicazione software che consente a un utente di visualizzare una pagina web (presente in una rete locale o su Internet) e gestire in modo interattivo le sue funzionalità testuali, iconiche, visuali o musicali*"
[34] Cfr. IASELLI, Internet Service Provider*. Guida all'ISP: cos'è, regime e tipologie di responsabilità*, in *Altalex*, 2019,, 1.

Il D.lgs. 9 aprile 2003 n. 70, che ha dato attuazione alla direttiva 2000/31/CE, distingue tre tipologie di ISP, classificandoli in *Mere Conduit Provider*, *Caching Provider* e *Hosting Provider*[35].

Queste due tipologie, pur avendo ciascuno le proprie caratteristiche specifiche, sono spesso coinvolti in attività illecite svolte da terzi, cioè gli utenti dei loro servizi[36].

L'articolo 14 del D.lgs. 70/2003 si occupa dei *Mere Conduit Provider*, i quali erogano servizi di mero trasporto di dati.

Nello specifico, si limitano a trasmettere dati da un mittente a un destinatario, senza elaborarli o modificarli. Il loro compito principale è quello di fornire l'accesso a una rete di comunicazione principale, consentendo così uno scambio di informazioni. Fastweb o Vodafone ne sono un esempio.

Queste attività «includono 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»[37].

Ciò significa che l'archiviazione di informazioni è funzionale esclusivamente alla loro trasmissione, pertanto, non appena verrà raggiunto questo scopo, le stesse dovranno essere eliminate.

Sebbene, l'espressione utilizzata dal legislatore – "tempo ragionevolmente necessario" – è generica, spetterà alla tecnologia stabilire il tempo e definire il confine tra il ruolo di neutralità del fornitore di servizi e una possibile interferenza nella trasmissione di informazioni[38].

Inoltre, la norma stabilisce che il prestatore non sarebbe responsabile delle informazioni che trasmette, a meno che «non dia origine alla trasmissione», «non

---

[35] In tal senso D'ALTERIO, *ISP: la responsabilità per le pubblicazioni degli utenti. I criteri di imputazione delle responsabilità civile e penale a carico degli* Internet Service Provider *in base al d.lgs. n. 70/2003*, in *Altalex*, 2021, 1.

[36] V. LAVAGNINI, *La responsabilità degli* Internet Service Provider *e la nuova figura dei prestatori di servizi di condivisione* online *(art. 17)*, in LAVAGNINI (a cura di), *Il diritto d'autore nel mercato unico digitale: direttiva (UE) 2019/790 e d. lgs. n. 177/2021 di recepimento*, Torino, 2022, 210 s.

[37] Art. 14 Decreto legislativo 9 aprile 2003, n. 70.

[38] In argomento MARSICO, *La responsabilità civile dell'*internet service provider*: sulla dibattuta* species *del contratto di accesso*, in *Dir. amm*., 2022, 8.

selezioni il destinatario della trasmissione» e «non selezioni né modifichi le informazioni trasmesse».

Quindi, il *mere conduit provider*, limitandosi a compiere esclusivamente un'attività di trasmissione, non incorrerebbe in nessuna responsabilità[39].

I *Caching Provider*, a differenza dei primi, sono previsti dall'articolo 15 del D.lgs. menzionato e prestano un servizio di archiviazione temporanea di informazioni al solo scopo di rendere più efficace la trasmissione delle informazioni da parte e su richiesta di altri destinatari del servizio. Rientrano in questa tipologia i motori di ricerca, come *Google search*[40].

L'attività di "caching" si concretizza nell'analizzare le pagine Web disponibili in rete attraverso un *software* automatico. Una volta individuata una determinata pagina analizza il contenuto, scansiona e ne memorizza i codici HTML che la compongono[41]. In questo caso, il prestatore non andrebbe esente da responsabilità se interferisse con i dati memorizzati o qualora non procedesse alla rimozione delle informazioni memorizzate «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»[42].

Infine, l'articolo 16 del medesimo Decreto è dedicato all'*Hosting Provider*. Quest'ultima tipologia di *provider* ospita i contenuti, gli immagazzina e gli archivia in modo stabile.

Pertanto, in questo caso, non si tratta solo di trasmissione o memorizzazione temporanea di informazioni, ma di archiviazione di dati al fine di renderli disponibili a utenti remoti[43]. In altre parole, la sua funzione è quella di rendere reperibili i dati forniti da un destinatario del servizio conservandoli stabilmente.

---

[39] Si veda CEDROLA, *La responsabilità penale dell'*Internet Service Provider *(ISP)*, in *Ius in Itinere*, 2018, 4.
[40] Cfr. LAVAGNINI, *La responsabilità degli* Internet Service Provider *e la nuova figura dei prestatori di servizi di condivisione* online *(art. 17),* , cit., 211.
[41] V. D'ALTERIO, *ISP: la responsabilità per le pubblicazioni degli utenti. I criteri di imputazione delle responsabilità civile e penale a carico degli* Internet Service Provider *in base al d.lgs. n. 70/2003*, cit. 1.
[42] Così CEDROLA, *La responsabilità penale dell'*Internet Service Provider *(ISP)*, cit., 4.
[43] Cfr. LAVAGNINI, *La responsabilità degli* Internet Service Provider *e la nuova figura dei prestatori di servizi di condivisione* online *(art. 17),* , cit., 211.

L'*hosting provider*, ai sensi della norma citata, potrebbe beneficiare dell'esenzione da responsabilità a condizione che «non sia effettivamente a conoscenza» dell'attività illecita e qualora agisca prontamente alla rimozione del contenuto illecito, o alla disabilitazione dell'accesso, non appena riceva una segnalazione[44].

La distinzione delle funzioni svolte dai *provider* è stata introdotta dal legislatore per classificare in modo chiaro le diverse tipologie di servizi che questi soggetti possono offrire. Nella pratica, uno stesso *provider* può ricoprire contemporaneamente tutti e tre i ruoli – *mere conduit*, *caching* e *hosting* – e questa suddivisione si è rivelata utile anche per individuare i relativi regimi di responsabilità.

Tuttavia, con l'adozione del recente *Digital Services Act* (DSA)[45], recepito nell'ordinamento italiano attraverso il D.lgs. 25 marzo 2024, n. 50, sono stati abrogati gli artt. 14, 15, 16 e 17 del D.lgs. 70/2003, corrispondenti agli artt. 12, 13, 14 e 15 della Direttiva *E-commerce*. Ciononostante, i principi ispiratori di quella normativa continuano a mantenere la loro rilevanza, poiché il DSA ha introdotto una disciplina europea più uniforme e dettagliata.

È importante sottolineare che la tradizionale tripartizione dei servizi non risulta più sufficiente per descrivere le funzioni attuali svolte dai *provider*, profondamente trasformate con l'avvento del c.d. *Web 2.0*. I fornitori di servizi digitali, infatti, non si limitano più a trasportare o archiviare i contenuti: l'evoluzione tecnologica e la diffusione di dispositivi mobili, come *smartphone* e *tablet*, hanno determinato un cambiamento radicale del contesto economico e sociale, rendendo ormai superata l'impostazione originaria della Direttiva[46].

1.2.2. Il ruolo attivo e passivo del *Hosting Provider*

In base alle operazioni che realizza, il *provider* che fornisce servizi di *hosting* può essere classificato come attivo o passivo.

---

[44] V. CEDROLA, *La responsabilità penale dell'*Internet Service Provider *(ISP)*, cit., 4 s.
[45] Regolamento UE 2022/2065.
[46] In tal senso BRASCHI, Social media *e responsabilità penale dell'*Internet Service Provider, in *MediaLaws*, 2020, 3, 159.

Come meglio si vedrà nel prossimo capitolo, l'articolo 17 del d.lgs. 70/2003 sancisce un'assenza generale di obblighi di controllo dei contenuti o di ricerca proattiva degli illeciti.

Tuttavia, il secondo comma della medesima norma riconosce un obbligo di collaborazione *ex post* con la pubblica autorità, imponendo all'ISP di fornire le informazioni in suo possesso per prevenire e individuare attività illecite.

Tale regime si fonda sul c.d. "principio di neutralità della rete", in base al quale «i fornitori di servizi *Internet* (ISP) trattano l'intero traffico online in modo equo e aperto, senza discriminazioni, blocchi, limitazioni o priorità»[47].

Il *provider*, quindi, non dovrebbe operare nessun filtraggio dei contenuti caricati dagli utenti.

Tuttavia, l'*hosting provider*, per come delineato dall'art. 16 d.lgs. 70/2003, col tempo ha iniziato ad intervenire attivamente sui contenuti, non limitandosi più al puro e semplice *storage*[48].

Infatti, sebbene la Direttiva sia stata concepita immaginando un *hosting provider* che si limitasse esclusivamente a fornire la piattaforma in modo passivo, gli sviluppi tecnologici hanno delineato un nuovo tipo di *hosting provider*, che si caratterizza per un'interazione attiva con i contenuti[49].

A riguardo è necessario avere presente quanto disposto dal Considerando n. 42 della Direttiva 2000/31/CE[50]: l'ISP può beneficiare dell'esenzione di responsabilità unicamente se l'attività svolta sia di ordine «meramente tecnico, automatico e passivo».

Pertanto, se il fornitore del servizio si limita a mettere a disposizione uno spazio di archiviazione a richiesta del destinatario, non ha né conoscenza né

---

[47] Cfr. EUR-Lex, *Internet aperta e neutralità della rete.*

[48] Così ACCINNI, *Profili di responsabilità penale dell'*hosting provider *"attivo"*, in *Arch. Pen.*, 2017, 2, 8 s.

[49] In argomento TORMEN, *La linea dura della Cassazione in materia di responsabilità dell'*hosting provider *(attivo e passivo)*, in *NGCC*, 2019, 2, 1046.

[50] Considerando n. 42 della Direttiva 2000/31/CE "*Le deroghe alla responsabilità stabilita 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*".

controllo delle informazioni trasmesse o memorizzate e non partecipa alla loro diffusione potrà beneficiare del regime di *favor*[51].

Viceversa, la definizione di *hosting* attivo è di derivazione giurisprudenziale. Il Tribunale di Milano, nella sentenza Mediaset-RTI c. Yahoo[52], è stato uno dei primi organi giudiziari nazionali a delineare la figura dell'*hosting provider* attivo.

Successivamente, la Suprema Corte[53] ha sancito una definizione di tale soggetto.

Nello specifico, l'*hosting provider* attivo è stato definito come «il prestatore dei servizi della società dell'informazione che svolge un'attività che esula da un servizio di ordine meramente tecnico, automatico e passivo, e pone invece in essere una condotta attiva concorrendo nella commissione dell'altrui illecito, onde resta sottratto al regime di esenzione previsto all'art. 16 d.lgs. n. 70/2003»[54].

Da questa definizione si evince quindi che l'*hosting* attivo è tale quando pone in essere un'attività che in qualche modo determina una manipolazione dei dati. Le attività di filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione o promozione dei contenuti rientrano tra gli indici semplificativi indicati dalla Cassazione[55].

Ne consegue che l'ISP riveste un ruolo attivo quando non si limita a compiere un'attività meramente tecnica, ma interviene nell'organizzazione, selezione o promozione dei contenuti caricati dagli utenti. Realizzando così una condotta attiva e concorrendo, insieme ad altri soggetti, alla realizzazione di un illecito.

Al contrario, si considera passivo il fornitore che si limita a offrire un servizio neutro, caratterizzato da un trattamento tecnico e automatico dei dati forniti dagli utenti[56].

---

[51] In tal senso COSTA, *La responsabilità dell'*Internet Service Provider *per i reati in materia di diritto d'autore*, in *Giur. pen*., 2022, 2, 17.
[52] V. Trib. Milano, Sez. Spec. Propr. Ind. e Intellettuale, 9 settembre 2011, n. 10893.
[53] Cfr. Cass. Civ. sez. I, 19/03/2019, n.7708.
[54] V. RUSSO, *La responsabilità dei* providers, in *SalvisJuribus*, 2022, 1s.
[55] Cfr. COSTA, *La responsabilità dell'*Internet Service Provider, cit., 18 s.
[56] In argomento SPINOGLIO, *Contenuti illeciti e responsabilità degli ISP: tutto quello che c'è da sapere*, in *Agenda Digitale.*, 2019, 7.

Tuttavia, secondo un orientamento giurisprudenziale minoritario[57] la figura dell'*hosting provider* attivo, nel nostro ordinamento, non ha nessuna rilevanza giuridica per tre ordini di ragioni. In primo luogo, perché non vi è nessuna norma che lo preveda in maniera espressa. In secondo luogo, il regime di esenzione di responsabilità è stato previsto dalla Direttiva proprio per favorire il progresso tecnologico e, pertanto, sarebbe contradditorio sostenere che, raggiunto un certo livello di sviluppo, l'*hosting* non benefici più del regime di esenzione. Infine, i sostenitori di questo orientamento giurisprudenziale ritengono che la Corte di Giustizia dell'Ue non abbia mai introdotto esplicitamente la figura dell'*hosting provider* attivo.

Le sentenze della Corte si limitano a ribadire la distinzione tra chi svolge un'attività di mera memorizzazione – esente da responsabilità – e chi invece pone in essere una manipolazione dei dati – a cui non si applica l'esenzione[58].

1.2.3. Il *Provider* come *gatekeeper* della Rete

Gli Stati fondatori della Comunità economica europea (CEE) hanno deciso di escludere il settore delle telecomunicazioni dall'ambito di competenza della nascente Comunità, pienamente consapevoli della sua rilevanza strategica.

Sul punto, il Trattato di Roma del 1957 non faceva alcuna menzione a tale settore ma, successivamente, la disciplina europea sulle telecomunicazioni ha subito un progressivo cambiamento, passando da un sistema monopolistico gestito da ciascuno Stato membro ad un sistema gestito a livello comunitario[59].

In questo contesto, infatti, si inserisce il tema della c.d. *net-neutrality* già accennato nel paragrafo precedente.

Il concetto di *net-neutraliy* presenta numerose sfaccettature e nel tempo è stato oggetto di diversi tentativi definitori da parte di molti autori.

---

[57] Cfr. App. Milano, 7 gennaio 2015, n. 29.
[58] Così. TORMEN, *La linea dura della Cassazione in materia di responsabilità dell'*hosting provider *(attivo e passivo)*, cit., 1046 s.
[59] V. OROFINO, *La politica europea delle telecomunicazioni (comunicazioni elettroniche): la nuova sfida della* net-neutrality, in *Eurojus*, 2017, 1 ss.

In questa prospettiva, appare significativo il tentativo compiuto nello Studio della Commissione per il mercato interno e la protezione dei consumatori (IMCO)[60] circa la possibilità di sistematizzare le varie declinazioni del concetto di neutralità della Rete attraverso una tripartizione.

In primo luogo, la neutralità della rete viene interpretata come la possibilità per tutti gli utenti di accedere a contenuti o applicazioni sulla base di una loro libera scelta. In secondo luogo, essa consiste nella garanzia che tutto il traffico di *Internet* venga trattato in modo uguale, senza alcuna distinzione basata sulla fonte, sul contenuto o sulla destinazione. Infine, la neutralità della Rete viene intesa come il divieto per gli operatori di adottare comportamenti discriminatori nella trasmissione del traffico *Internet*[61].

La *net-neutrality* rappresenta quindi un principio cardine nello sviluppo di *Internet*, volto a prevenire discriminazioni dannose o pratiche anti-competitive da parte dei gestori della Rete e dei *provider* di servizi digitali[62]. Con il Regolamento (UE) 2015/2120 l'Unione europea, oltre ad aver eliminato i sovrapprezzi di traffico al dettaglio, favorendo la creazione di un mercato europeo dei servizi di telefonia mobile, ha anche introdotto delle norme comuni a tutela della neutralità della Rete[63].

In altri termini, il Regolamento ha stabilito delle regole uniformi volte a prevenire trattamenti discriminatori nella gestione del traffico e nei servizi di accesso a *Internet*. L'obbiettivo principale è quello di tutelare i diritti degli utenti finali, tra i quali rientrano il diritto di accedere a informazioni e contenuti, il diritto di utilizzare e fornire servizi, contenuti e applicazioni, nonché il diritto di scegliere liberamente le apparecchiature terminali da utilizzare.

---

[60] La Commissione per il mercato interno e la protezione dei consumatori (IMCO) riveste un ruolo fondamentale nel coordinamento delle normative nazionali che regolano il mercato unico e l'unione doganale a livello dell'UE. Si occupa principalmente «della libera circolazione di merci e professionisti, dell'armonizzazione delle norme tecniche, della promozione del diritto di stabilimento e della libera prestazione dei servizi, fatta eccezione per i settori finanziario e postale». Inoltre, le è affidato il compito di rilevare e rimuovere gli ostacoli che possono compromettere il buon funzionamento del mercato interno, tutelando al contempo gli interessi economici dei consumatori europei. Cfr. Gruppo PPE, Mercato interno e protezione dei consumatori.

[61] In tal senso BIASIN, *La neutralità della rete*, in *LawTech*, 2016, 48.

[62] Cfr. MARTANI, *La* net neutrality *alla luce del Regolamento UE n. 2120/2015 e delle Linee Guida BEREC*, in *Cibersp. dir.*, 2017, 3 s.

[63] In tal senso OROFINO, *La politica europea delle telecomunicazioni (comunicazioni elettroniche)*, cit., 7.

In tal senso, l'art. 3, par.1, delinea un generale diritto di accesso a Internet, sancendo la libertà di circolazione delle informazioni, anche al fine di utilizzarle e diffonderle indipendentemente dalla loro origine, dal loro contenuto o dalla loro destinazione.

Invece, il par. 2 introduce una garanzia riguardante le condizioni contrattuali tra utenti e ISP, stabilendo in particolare che questi ultimi non possano legittimare trattamenti iniqui del traffico, non avendo nessuna rilevanza l'esplicita manifestazione del consenso.

Il par. 3 infine, stabilisce un obbligo in capo ai *provider* di trattare in modo equo e non discriminatorio il traffico dei dati.

Dall'art. 3, par. 3, del Regolamento (UE) 2015/2120, considerato da molti autori come una definizione normativa di neutralità della rete, si ricavano due obblighi distinti: il primo dispone di trattare il «traffico allo stesso modo, senza discriminazioni, restrizioni o interferenze, e a prescindere dalla fonte e dalla destinazione, dai contenuti cui si è avuto accesso o che sono stati diffusi, dalle applicazioni o dai servizi utilizzati o forniti, o dalle apparecchiature terminali utilizzate »[64]; il secondo impone che i fornitori «non bloccano, rallentano, alterano, limitano, interferiscono con, degradano o discriminano tra specifici contenuti, applicazioni o servizi, o loro specifiche categorie, salvo ove necessario e solo per il tempo necessario »[65].

In questa prospettiva, il principio di *net-neutrality* si propone di tutelare i diritti degli utenti, evitando ingiustificate interferenze da parte dei gestori della Rete. Dunque, fa sì che i *provider* trattino tutti i dati aventi le medesime caratteristiche in maniera equa e senza alcuna discriminazione per finalità di profitto[66].

Ed infatti, proprio grazie alla sua struttura neutrale *Internet* si è affermato come un ambiente competitivo e favorevole, in cui l'innovazione ha trovato terreno fertile per lo sviluppo di innumerevoli servizi.

---

[64] Reg. (UE) 2015/2120, art. 3, par. 3.
[65] Reg. (UE) 2015/2120, art. 3, par. 3, part. 3, Regolamento (UE) 2015/2120.
[66] V. POMA, *L'interpretazione del regolamento 2015/2120 tra principio di neutralità della rete, principio di non discriminazione e* Internet *aperta*, in *MediaLaws*, 2021, 3, 228 s. e 234.

Tuttavia, il rapido incremento delle informazioni trasmesse in rete ha messo in luce i limiti della neutralità, portando così gli ISP ad applicare dei trattamenti differenziati in base al contenuto e alla provenienza dei dati.

Infatti, i fornitori si sono sempre di più avvalsi di pratiche di *network management*, attraverso le quali la trasmissione dei dati viene reindirizzata, rallentata o velocizzata, minando così il carattere di neutralità della rete.

Queste pratiche di gestione del traffico però, per essere considerate ragionevoli, devono essere trasparenti, non discriminatorie, proporzionate e motivate esclusivamente da caratteristiche di ordine tecnico del servizio, non dovendo rilevare le motivazioni di ordine commerciale[67].

Tra le pratiche di gestione del traffico particolarmente rilevante è la categoria nominata *zero-rating*. Attraverso questa pratica i fornitori di accesso a *Internet* mettono a disposizione degli utenti specifici servizi o applicazioni, il cui utilizzo non comporta costi aggiuntivi o non viene conteggiato nel consumo del traffico dati previsto dal piano dell'utente. Ciò consente a milioni di persone, che altrimenti rimarrebbero escluse, di accedere ad Internet[68].

Gli ISP, dal canto loro, in qualità di fornitori dell'accesso alla rete, hanno finito per essere denominati *gatekeeper*, cioè dei guardiani che controllano l'accesso delle informazioni nell'ecosistema digitale, decidendo cosa possa passare e cosa no, influenzando l'esperienza di navigazione.

Si è presentata allora la necessità di evitare la nascita di posizioni dominanti che consentano ai *provider* di mettere a repentaglio il pluralismo e la libertà di espressione degli utenti. In particolare, destano una certa preoccupazione le c.d. *Internet Company*, tra le quali rientrano ad esempio Microsoft, Apple, Google, Amazon, ecc. che hanno assunto una notevole forza di mercato[69].

In questa prospettiva, è proprio il *Digital Markets Act* (DMA) – il regolamento europeo approvato dal Parlamento UE il 5 luglio 2022 – a stabilire insieme al *Digital Services Act* (DSA), gli obblighi di condotta delle imprese prima che si realizzi un abuso di posizione dominante. Entrambi i regolamenti

---

[67] Si veda PAMPANIN, *I nuovi protagonisti del mondo digitale tra neutralità della Rete e accesso all'informazione*, in *Inf.dir.*, 2017, 1-2, 238 ss.
[68] Ivi, 247 ss.
[69] Ivi, 252 ss.

compongono il c.d. *Digital Services Package*, volto a garantire un ecosistema digitale più equo e competitivo. Infatti, tra i diversi obbiettivi perseguiti, il DMA mira a contrastare l'abuso di posizione dominante da parte delle grandi piattaforme digitali, contribuendo a garantire una maggiore libertà di scelta agli utenti[70].

La nozione di *gatekeeper* risale al 1947, quando Kurt Lewin[71] elaborò una teoria secondo la quale vi sono dei soggetti che, come dei guardiani, esercitano un controllo sui flussi di comunicazione tra due determinate aree, decidendo cosa può attraversare il *gate*.

Questa concezione si è poi adattata al contesto digitale. I *gatekeeper* hanno la capacità di controllare il flusso e l'accesso alle informazioni.

Sul punto, il DMA ha adottato positivizzato la nozione di *gatekeeper*: al combinato disposto degli articoli 2 e 3 del regolamento sopra citato si comprende come tali vengano qualificate quelle imprese che offrono servizi definiti di "piattaforma di base" e che vengono designate come tali dalla Commissione europea se hanno «un impatto significativo sul mercato interno»[72], forniscono "«un servizio di piattaforma di base che costituisce un punto di accesso (gateway) importante affinché gli utenti commerciali raggiungano gli utenti finali»[73] e detengono "«una posizione consolidata e duratura, nell'ambito delle proprie attività, o è prevedibile che acquisisca siffatta posizione nel prossimo futuro»[74][75].

Da questa panoramica, emerge chiaramente come, per la loro posizione centrale nell'ambiente digitale, i *provider* non hanno un ruolo centrale solo in termini di accesso e controllo dell'informazione, ma anche nella prevenzione e gestione dei rischi cibernetici. Dunque, questi soggetti, da meri intermediari tecnici

---

[70] In tal senso MARTORANA, Digital Markets Act *(DMA), la Commissione individua i 6 gatekeeper*, in *Altalex*, 2023, 1.

[71] Psicologo statunitense di origine tedesco-polacca è considerato uno dei padri della psicologia sociale contemporanea. La sua teoria si accentra sul concetto di "ambiente comportamentalistico", vale a dire l'ambiente comportamentale che plasma l'individuo attraverso l'interazione sociale. Secondo Lewin, il comportamento umano è determinato da una continua interazione tra individuo e ambiente, all'interno di un contesto sociale complesso e dinamico. Si veda BERNARDINI, voce *Lewin Kurt*, in Enc. Treccani.

[72] Reg. (UE) 2022/1925, art. 3.

[73] Reg. (UE) 2022/1925, art. 3.

[74] Reg. (UE) 2022/1925, art. 3.

[75] Sul punto PELLIZZONI, Gatekeeper*: vecchie idee o nuove soluzioni?*, in *CERIDAP,* 2024, 1, 219 s.

sono divenuti attori principali, responsabili e destinatari di obblighi di sicurezza da attuare mediante l'adozione di regole tecnologiche e organizzative[76].

1.3. Il contesto operativo degli *Internet Service Provider*

L'*Internet service provider*, come già osservato, fornisce agli utenti tutti quei servizi indispensabili per il funzionamento e l'utilizzo di *Internet*, imponendo di confrontarsi con le caratteristiche principali delle forme di manifestazione del reato calate in un contesto digitale.

Si tratta di condotte che si inseriscono in un "non luogo", spesso realizzate da un soggetto non fisico e che richiedono un attento bilanciamento dei diritti fondamentali.

In questo senso, la responsabilità dell'ISP si colloca nel *cyberspace*. All'interno di questo contesto, i concetti tradizionali di azione ed evento mutano inevitabilmente e, di conseguenza, anche le forme di aggressione, oltre che i beni stessi, subiscono un'evoluzione[77]. Il termine *cyberspace* era stato utilizzato per la prima volta in un romanzo, appartenente al genere letterario *cyberpunk*[78], che si era diffuso intorno agli anni '80. Nel lavoro di William Gibson, intitolato Neuromancer, veniva descritta una realtà futuristica e distopica, in cui i personaggi vivevano esperienze alternative in uno spazio digitale ove era possibile archiviare, scambiare e sottrarre dati e informazioni. Progressivamente, il termine iniziò ad essere utilizzato anche in ambiti diversi da quello letterario, soprattutto in ambito politico e nel settore militare.

---

[76] In argomento FIORINELLI, *L'attuale ruolo del* provider *nella società digitale: modelli di responsabilità penale*, in *Leg. pen.*, 2022, 32.

[77] Rileva INGRASSIA, *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine*, in LUPÁRIA (a cura di), Internet Provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012, 1 ss.

[78] «Genere narrativo in cui temi legati alla realtà delle società postindustriali (cibernetica, robotica, telematica, realtà virtuale, biotecnologie, clonazione) vengono elaborati fantasticamente nel segno di un'ideologia contestataria, di ribellione e critica sociale, analoga a quella del movimento punk o della musica punk rock. Originale sintesi di suggestioni tecnologiche e cultura underground (➔), il c. si è affermato negli Stati Uniti nel corso degli anni 1980 grazie soprattutto al romanzo Neuromancer (1984) di William Gibson e a un'antologia di racconti di autori vari pubblicata da B. Sterling nel 1986, Mirrorshades. Adottando modalità narrative proprie della fantascienza, il c. si è poi aperto alla contaminazione con altri generi, particolarmente il noir, avendo tra i propri antecedenti il romanzo hard-boiled e tra i modelli più vicini autori come l'inglese J.G. Ballard o lo statunitense Philip K. Dick, autore di Do androids dream of electric sheep? (1968), da cui R. Scott trasse ispirazione per il film Blade runner (1982), uno dei sicuri punti di riferimento dell'immaginario cyberpunk».

A partire dal 1998, a livello politico, le Nazioni Unite riconobbero, in differenti risoluzioni, l'esistenza di questo nuovo ambiente; senza però darne una definizione, ma limitandosi a stabilire i comportamenti che gli Stati dovevano tenere.

Diversamente, a livello militare, vennero fornite molteplici definizioni di cyberspazio che, nella maggior parte dei casi, lo descrivevano come uno spazio fisico, inteso come "luogo" o come "dominio".

A partire dalla seconda metà degli anni 2000, gli studiosi hanno riconosciuto il *cyberspace* come un ambiente che può essere suddiviso in tre macro-livelli: il livello umano comprende gli utenti dell'informatizzazione; il livello logico riguarda il *software* e i *bit*, i quali rappresentano informazioni, istruzioni e risorse dello spazio cibernetico; infine, il livello fisico in cui sono incluse le componenti materiali della Rete.

Tuttavia, questa concezione è stata criticata da studi più recenti, in quanto considerata troppo statica. Infatti, oggi si preferisce una visione più dinamica del *cyberspace*, caratterizzata dalla velocità di propagazione e l'abbattimento dei confini[79]. Lo spazio cibernetico si affianca ai quattro domini tradizionali, quali terra, mare, aria e spazio. Nel linguaggio contemporaneo, infatti, viene qualificato come "quinto dominio" poiché manca di una vera e propria fisicità[80] e presenta delle caratteristiche proprie e del tutto peculiari.

Per prima cosa, è importante sottolineare che il *cyberspace* sia un'invenzione dell'uomo ed è passibile di continue evoluzioni, strutturali e funzionali che potrebbero causarne anche la chiusura. Questo implica che ogni area e ogni attività in esso compiute sono esposte a un rischio costante. Non bisogna neppure trascurare il fatto che, al suo interno, agiscono soggetti talvolta difficilmente identificabili.

Gli utenti, inoltre, sono portatori di interessi diversi e le possibili tensioni che possono sorgere tra loro presentano dinamiche uniche, non comparabili con quelle che possono verificarsi negli altri domini.

---

[79] Sul punto SERINI, *La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana*, in *RIID*, 2023, 2, 42 ss.

[80] Cfr. MERCURIO, *Il* cyberspace*: la sovranità nel quinto dominio*, in *Camm. dir.*, 2024, 4.

Due ulteriori aspetti critici che rendono complessa la regolazione e la gestione del cyberspazio sono l'ubiquità informatica e l'assenza di confini territoriali. Il fatto che, da un lato, le azioni compiute in questo ambiente e i loro effetti possano verificarsi contemporaneamente in luoghi diversi del mondo fisico e, dall'altro, la mancanza di una ripartizione spaziale in diversi "settori", lascia dubbi su quale autorità debba intervenire e dove debba farlo, complicandone una risposta tempestiva ed efficace[81]. Tecnicamente, il *cyberspace* è una rete globale che, grazie a Internet e a reti private, consente la connessione e l'interazione tra utenti, dati e applicazioni[82].

Dunque, è proprio grazie ad Internet che i contenuti circolano nello spazio cibernetico[83]. L'intera discussione che si è avuta sulla responsabilità del *provider* trae le fila da una questione teorica di principio, ossia se Internet sia uno spazio libero o controllato[84].

Nel 1996, John Perry Barlow ha redatto la Dichiarazione d'indipendenza del Cyberspazio, in cui manifestava la percezione di un mondo libertario fino all'anarchia. L'incipit di tale documento manifestava a pieno questa impostazione sostenendo che «Governi del mondo industriale, stanchi giganti di carne e di sangue, io vengo dal Cyberspazio, la nuova dimora della mente. In nome del futuro, invito voi, che venite dal passato, a lasciarci in pace. Non siete benvenuti tra noi. Non avete sovranità sui luoghi dove ci incontriamo»[85]. *Internet* era quindi visto come un luogo completamente libero e privo di controlli, ideato per garantire una comunicazione che nessuno potesse bloccare o controllare. Tuttavia, questa visione idealistica è stata messa progressivamente alla prova, dovendosi confrontare con una storia in costante sviluppo[86].

Infatti, nell'evoluzione della regolazione del *cyberspace* si possono distinguere due momenti. I primi dieci anni dalla nascita di Internet si sono caratterizzati per la totale assenza di vincoli statali. I governi hanno accettato il

---

[81] In argomento MIRTI, *La disciplina giuridica del* cyberspace*. Una panoramica sulle problematiche attuali e le principali linee evolutive*, in *Riv. Op. Juris.*, 2016, 3, 2.
[82] V. RUGOLO, *Cos'è il* cyberspace, in *Difesa Online*, 2024, 1.
[83] Così FROSINI, *L'orizzonte giuridico dell'*Internet, cit., 278.
[84] In questo senso GIRARDI, *Libertà e limiti della comunicazione nello spazio pubblico digitale*, in *Federalismi.it*, 2024, 17, 153.
[85] V. BARLOW, *Una dichiarazione di indipendenza del Cyberspazio*, 1996.
[86] Si veda RODOTÀ, *Una Costituzione per* Internet*?*, in *Pol. dir.*, 2010, 3, 338.

modello della *self-regulation*, più flessibile e favorevole all'innovazione, che ha permesso l'utilizzo commerciale di Internet, ma al contempo ha determinato il fallimento del movimento liberatorio della rete, sottratto all'autorità dei governi.

Negli ultimi vent'anni, i poteri pubblici hanno maturato la consapevolezza dei rischi connessi alla Rete ponendo un'accurata attenzione allo spazio cibernetico e dimostrando di poterlo regolamentare, anche in maniera rigida ed eccessiva[87].

Sulla scia di questa evoluzione storica, si sono sviluppati due modi di intendere il diritto in rete. Secondo l'approccio giuspositivistico[88], tutte le attività online devono essere disciplinate da norme tecniche.

Al contrario, secondo la concezione giusnaturalistica[89] rivendica la natura libertaria dello spazio virtuale, esonerato da ogni tipo di regolamentazione[90]. La crescente affermazione del ruolo degli intermediari, e in particolare dei prestatori di servizi della società dell'informazione, ha segnato il superamento dell'idea iniziale che la rete fosse un luogo di libertà assoluta, immune da governi e poteri economici[91].

Alle molteplici innovazioni corrispondono diverse direttrici globali volte a regolare in modo più efficace il *cyberspace*. Vi è anzitutto un tentativo di ri-territorializzare la giurisdizione, attraverso il riconoscimento in capo ai fornitori di nominare un rappresentante legale incaricato di ricevere le richieste e di garantire il rispetto della normativa vigente. Vi è anche una tendenza alla disintermediazione con il progressivo superamento della logica centralizzata, basata sul necessario coinvolgimento tra le autorità di due Stati coinvolti, in favore del crescente ruolo assunto dalle società private nella tutela dei diritti fondamentali.

Dunque, un orientamento condiviso, avviato prima dagli Stati Uniti e progressivamente accolto dalla comunità internazionale e dall'Unione Europea, è quello di cercare una collaborazione diretta con gli ISP[92].

---

[87] Così SERINI, *La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana*, cit., 46 ss.
[88] Tra gli esponenti della concezione giuspositivistica si può citare Lawrence Lessig.
[89] John Perry Barlow è tra gli esponenti dell'approccio giusnaturalistico.
[90] In argomento FEROLETO, *I diritti umani dal giusnaturalismo alla nuova era digitale: i processi di tutela dei soggetti socialmente vulnerabili nel cyberspazio e la responsabilità* dell'internet service provider, in *TIGOR*, 2024, 1, 97.
[91] Cfr. BASSINI, *Libertà di espressione e* social network*, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione*, in *Riv.it. inf. dir.*, 2021, 2, 45.
[92] In tal senso FRAGASSO, *La regolamentazione europea sulla* Mutual Legal Assistance *(MLA)*

1.4. Il quadro normativo di riferimento

Risulta estremamente complesso configurare una responsabilità in capo all'ISP, tanto per la mancanza di una disciplina aggiornata in grado di far fronte alle nuove esigenze poste dalla realtà digitale, quanto per le profonde divergenze tra le posizioni dottrinali e giurisprudenziali nell'ambito dell'ordinamento europeo.

Infatti, il tema della responsabilità si inserisce nel quadro più ampio relativo al rapporto tra diritto penale e Internet.

Tuttavia, di fronte all'inerzia del legislatore, che spesso non interviene in modo tempestivo, vi è il rischio di superare le garanzie proprie del diritto penale, primo tra tutti il principio di legalità[93]. Il punto di partenza per la riflessione sulla responsabilità degli ISP è rappresentato dalla Direttiva E-Commerce, la quale ha previsto un regime di esenzione da responsabilità per i prestatori a condizione che l'attività da essi svolta sia di natura puramente tecnica, automatizzata e passiva. Tale impostazione risponde all'esigenza di evitare che le piattaforme online siano gravate da un obbligo di sorveglianza preventiva, che implicherebbe un monitoraggio sistematico dei materiali caricati dagli utenti. Diversamente, l'obbligo di responsabilità si applica ai soggetti che producono e diffondono direttamente contenuti, in quanto esercitano un controllo diretto sulle informazioni trasmesse.

Tuttavia, la Direttiva introduce un regime di responsabilità analogo a quello previsto per i fornitori di contenuti nel caso in cui il prestatore di servizi venga a conoscenza effettiva di comportamenti o contenuti illeciti da parte degli utenti. In tali circostanze, il prestatore non potrà più avvalersi dell'esenzione prevista e sarà tenuto a intervenire prontamente, rimuovendo il contenuto incriminato per evitare di incorrere in responsabilità legale.

Il quadro normativo evidenzia chiaramente la volontà del legislatore europeo di tutelare i *provider* che non esercitano alcun controllo sui contenuti

---

nel cyberspace, in FONDAZIONE OCCORSIO (a cura di), *Intelligenza artificiale e giurisdizione penale*, Roma, 2021, 22.

[93] V. TAVERNITI, *Profili di responsabilità dell'*internet service provider *tra disciplina vigente e nuove esigenze di tutela*, cit., 6 s.

generati dagli utenti, evitando che possano essere ritenuti responsabili per condotte illecite a loro non riconducibili[94].

Questo assetto normativo, si è però rivelato sempre più inadeguato di fronte all'evoluzione del panorama digitale. Infatti, il *Digital Services Act* rappresenta uno degli strumenti fondamentali con cui l'Unione europea mira a realizzare la c.d. sovranità digitale. Questa espressione riflette l'ambizione di costruire una strategia autonoma nel settore digitale, mediante l'adozione di meccanismi sia di protezione che di intervento, in risposta alla crescente influenza delle grandi piattaforme digitali, che si espande spesso al di fuori dei confini imposti dalla normativa europea e dai principi fondamentali dell'ordinamento. Guidato da tali principi, il Digital Services Act si concentra sulla regolamentazione dell'offerta dei servizi digitali, fondando la propria disciplina su tre pilastri essenziali: trasparenza, responsabilità e tutela degli utenti.

L'obiettivo è quello di creare un ambiente digitale sicuro, prevedibile e affidabile per tutti gli utenti. In questo senso, il legislatore europeo ha tradotto in norme la consapevolezza che la profonda trasformazione del ruolo dei *provider*, e in particolare dei servizi di *hosting*, rappresenta un potenziale rischio per i cittadini, aggravato dalla mancanza di un sistema amministrativo di vigilanza efficace e da una normativa frammentata.

Tutto ciò ha evidenziato la necessità di una revisione della disciplina prevista dalla Direttiva 2000/31/CE, pur conservando il principio di base di quest'ultima esso viene riformulato alla luce delle nuove sfide del mondo digitale. Il fine ultimo è quello di rafforzare, attraverso un atto giuridico vincolante, la responsabilità degli ISP rispetto a fenomeno come la violenza *online* l'*hate speech* e la disinformazione *online*[95].

I tratti peculiari delle modalità lesive di beni giuridici compiute in rete richiedono un indispensabile processo di armonizzazione dei reati a livello sovranazionale. Tale esigenza si avverte anzitutto nell'orizzonte europeo, ove il

[94] V. DE GREGORIO, *Il regime di responsabilità degli ISP alla luce della sentenza della Corte di Cassazione n. 54946/2016*, in *MediaLaws*, 2017, 1.
[95] Cfr. VASINO, *Censura "privata" e contrasto all'*hate speech *nell'era delle* Internet Platforms, in *Federalismi.it*, 2023, 4, 147 ss.

lungo ma continuo processo di integrazione ha permesso la predisposizione di rilevanti strumenti di cooperazione in materia penale.

Anche su scala globale si auspica una maggiore uniformità normativa, senza trascurare che un'intensa cooperazione tra Stati potrebbe compromettere il rispetto del principio di proporzione e delle libertà fondamentali a causa dei differenti standard di tutela delle garanzie individuali[96]. Affinché il futuro, nel metaverso, sia migliore del presente e del passato, occorre regolamentare per garantire le libertà e i beni comuni fissando dei principi generali più che norme di dettaglio. Risulta opportuno adottare una prospettiva sovranazionale piuttosto che limitarsi a quella nazionale, senza dimenticarsi di mettere l'uomo al centro.

Non bisogna avere il timore di intervenire, perché le regole, quando sono ben formulate, garantiscono le libertà. Al contrario bisogna avere il coraggio di farlo. Non esistono delle strade semplici e immediate per affrontare le sfide nella dimensione digitale. Il punto di riferimento da seguire è sicuramente uno: il rispetto dei diritti fondamentali[97].

1.4.1. La normativa internazionale

L'assenza di una disciplina internazionale in materia di cibersicurezza ha spinto la Comunità internazionale ad accogliere un duplice approccio per l'individuazione dei principi attuativi del *cyber international law*, inteso come l'insieme delle norme che regolano i rapporti tra gli utenti all'interno dello spazio digitale.

In un primo momento, il dibattito era diviso tra chi proponeva la redazione di nuovi principi e chi, invece, sosteneva applicare in via analogica i principi vigenti del diritto internazionale[98].

---

[96] Sul tema PERDONÒ, *Le responsabilità penali collegate all'uso di* internet *fra comparazione e prospettive di riforma*, in *Dir. Inf.*, 2007, 345.

[97] In tal senso SCORZA, *In principio era* Internet *e lo immaginavamo diverso*, in *Dir. Inf.*, 2022, 1, 13 ss.

[98] Tra i sostenitori della redazione di nuovi principi rientrano Russia, Iran, Siria, Cuba, Egitto e Cina. Al contrario i membri dell'Ue e gli Stati Uniti hanno sostenuto l'applicazione in via analogica dei principi del diritto internazionale già vigenti. V. rapporto del 14 luglio 2021 del *UN Group of Governmental Experts on the Development in the Field of Information and Telecommunications in the Context of International Security (UNGEE)*, *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UN Doc. 76/135, par. 6 ss*.

Oggi si preferisce quest'ultima impostazione, pur lasciando aperta la possibilità di predisporre delle nuove regole, qualora fosse necessario.

Questa impostazione è confermata sia dal progetto del codice internazionale di condotta per la sicurezza delle informazioni, sia dai rapporti redatti da due gruppi di lavoro che lavorando all'interno dell'ONU si occupano di stabilire le norme che formano il diritto internazionale applicabile al *cyberspace*[99].

A riguardo, rilevante è la recente *Declaration on a Common Understanding of International Law in Cyberspace* adottata dal Consiglio dell'Unione europea il 18 novembre 2024. Tale Dichiarazione evidenzia la complessità delle attività cibernetiche ostili, favorita anche dall'evoluzione delle tecnologie dell'informazione e della comunicazione (ICT), che giocano un ruolo sempre più centrale nei conflitti nazionali e internazionali attuali. Da qui deriva l'esigenza che gli Stati si comportino in modo responsabile nel cyberspazio, rispettando i principi sanciti dalla Carta ONU, al fine di preservare la pace, la sicurezza e la stabilità a livello internazionale.

Centrale è il richiamo della Dichiarazione a due importanti iniziative internazionali, quali l'*UN framework of responsible State behaviour in cyberspace* e il *Cyber programme of action initiative*. Entrambi questi strumenti mirano a promuovere e consolidare la cooperazione internazionale e il coinvolgimento di molteplici attori nel settore della sicurezza cibernetica.

L'ONU, da tempo, si impegna attivamente per promuovere l'adozione di un quadro normativo internazionale capace di contrastare l'uso improprio dello spazio cibernetico. In questo senso, tali iniziative si sviluppano principalmente attraverso l'Assemblea Generale e il lavoro del Gruppo di esperti governativi (GGE) sulle tecnologie ICT. In un rapporto del 2013, il GGE ha evidenziato come l'applicazione delle norme esistenti del diritto internazionale all'ambito ICT sia fondamentale per ridurre i rischi che minacciano la pace, la sicurezza e la stabilità globale. Pur riconoscendo la necessità di ulteriori approfondimenti sull'applicazione concreta di tali norme, il documento richiama esplicitamente principi come la sovranità, il

[99] In argomento SCIACOVELLI, *Attività ostili nel ciberspazio: il quadro normativo internazionale e dell'UE e l'importanza di istituire un'Unità congiunta per il ciberspazio*, in GARGIULO, INGRAVALLO (a cura di), *Osservatorio sulle attività delle organizzazioni internazionali e sovranazionali, universali e regionali*, Napoli, 2022, 10.

rispetto dei diritti fondamentali, la lotta alla criminalità e al terrorismo, e la responsabilità per comportamenti illeciti.

Nel 2015, l'Assemblea Generale ha ripreso le indicazioni del rapporto del GGE del 2013, sottolineando l'importanza dell'applicazione del diritto internazionale — in particolare della Carta delle Nazioni Unite — per garantire un ambiente ICT sicuro, stabile, aperto e pacifico. Ha inoltre valorizzato l'adozione volontaria di regole e principi non vincolanti da parte degli Stati, ritenendoli strumenti utili per ridurre i rischi legati all'uso delle tecnologie digitali. In tale contesto, il rapporto del GGE del 2015 propone undici regole volontarie per promuovere comportamenti responsabili nel cyberspazio. Infine, il rapporto del GGE 2019–2021 ha ulteriormente dettagliato queste regole, suggerendo misure concrete che gli Stati possono adottare a livello nazionale e regionale.

Il *Cyber Programme of Action Initiative*, sostenuto da cinquantaquattro Paesi, mira a promuovere progressi tangibili nel comportamento statale attraverso interventi mirati, tra cui: l'individuazione delle principali sfide e la formulazione di raccomandazioni e strategie di cooperazione per affrontarle; il supporto concreto alle attività di rafforzamento delle capacità, anche mediante la creazione di un gruppo di lavoro dedicato; e la promozione di un coinvolgimento attivo e significativo di tutti gli attori interessati[100].

Le regole che disciplinano il funzionamento di *Internet* sono spesso sviluppate "dal basso", attraverso strumenti chiamati *Request For Comments* (RFC). Tali documenti, redatti da esperti, studiosi e professionisti del settore, contengono informazioni e specifiche tecniche basate su pratiche che si sono dimostrate efficaci nel tempo. Gli RFC vengono messi a disposizione della comunità *online* tramite la *Internet Engineering Task Force* (IETF), che ne promuove l'adozione con l'obiettivo di trasformarli in veri e propri standard.

L'IETF è un'organizzazione internazionale non governativa che riunisce tecnici e ricercatori impegnati individualmente nello sviluppo tecnico del *Web*. Tra i suoi scopi principali vi è la standardizzazione della rete, obiettivo perseguito anche

[100] In tal senso GARGIULO, *La* Declaration on a common understanding of international law in cyberspace *del Consiglio dell'Unione europea*, in *Osservatorio sulle attività delle organizzazioni internazionali e sovranazionali, universali e regionali, sui temi di interesse della politica estera italiana*, Roma, 2025, 1 ss.

attraverso la collaborazione con altre organizzazioni, sia non governative — come il *World Wide Web Consortium* (W3C), fondato nel 1994 presso il MIT per valorizzare le potenzialità del Web — sia internazionali tradizionali, come l'*International Organization for Standardization* (ISO) e l'*International Electrotechnical Commission* (IEC), che si occupano della definizione di standard in ambito elettronico e tecnologico.

Gli standard, poiché indicano ai destinatari comportamenti da adottare, hanno sicuramente una portata normativa, pur essendo considerati semplici raccomandazioni prive di effetti giuridicamente vincolanti, la cui osservanza dipenderebbe dalla libera volontà degli operatori della rete. Tuttavia, il mancato rispetto di queste regole determina l'impossibilità di accedere o utilizzare la risorsa a cui esse si riferiscono. Pertanto, chiunque intenda avvalersi di tale risorsa è tenuto a conformarsi alle regole stabilite o, alternativamente, accettare l'esclusione dal loro utilizzo[101].

I tentativi unilaterali dei singoli Stati di regolare i contenuti illeciti in rete spesso incontrano difficoltà, soprattutto quando tali contenuti sono conservati in *server* esteri. Per affrontare efficacemente le criticità e gli ostacoli legati alla competenza giurisdizionale e all'effettività delle sanzioni comminate, sarebbe auspicabile adottare, a livello internazionale globale, un insieme di regole condivise ed uniformi, valide e applicabili in ogni Paese.

Dal momento che Internet è onnipresente e privo di confini fisici, solo attraverso un approccio giuridico condiviso si può garantire certezza del diritto e della pena nei confronti dei responsabili, indipendentemente da dove essi si trovino[102].

Le iniziative di riforma, al fine di superare le difficoltà legate alla competenza giurisdizionale e rendere più efficacie l'azione giudiziaria e repressiva contro i crimini commessi *online*, richiederebbero il coinvolgimento dell'intera comunità internazionale. Tuttavia, per affrontare in modo risolutivo tali problemi è necessario che non solo la normativa sia chiara e ben definita, ma lo devono essere anche le procedure di intervento tempestivo da parte dei gestori dei contenuti stessi.

---

[101] Così RUOTOLO *Le fonti dell'ordinamento internazionale*, cit. 703 ss.
[102] Cfr. DI TANO, *Prospettive* de iure condendo *sulla responsabilizzazione dei* content provider, *Inf. dir.*, 2017, 1-2, 113.

La legge, pur essendo essenziale, non è sufficiente, anche in un ideale panorama in cui esistano norme internazionali armonizzate e globalmente accettate.

È necessario cambiare approccio, che preveda un maggior coinvolgimento degli stessi ISP affinché siano stimolati ad applicare spontaneamente strumenti tecnologici avanzati. Tali strumenti dovrebbero essere in grado di colmare le lacune dell'intervento umano e a supportare l'attività di vigilanza svolta dagli operatori specializzati[103].

In una prospettiva *de iure condendo*, che miri alla massima armonizzazione a livello internazionale, è necessario intervenire per aggiornare la disciplina in materia di responsabilità degli ISP. Occorre, in particolare, introdurre degli obblighi specifici e tempestivi per il blocco o la rimozione di contenuti segnalati dagli utenti, come *hate speech* o molestie. Sicuramente, la strada verso tale riforma è complessa, soprattutto se si considera la diffidenza di *provider* e *stakeholder* in gioco. Gli stessi provider, infatti, pur manifestando una maggior apertura, temono di perdere la propria autonomia e indipedenza, nonché di dover sostenere costi elevati per l'implementazione di sistemi avanzati di controllo dei contenuti[104].

1.4.1.1. L'Unione internazionale delle telecomunicazioni (ITU)

L'*International Telecommunication Union* (ITU) è un'organizzazione internazionale di matrice europea, istituita nel 1865 con lo scopo di coordinare e uniformare le reti telegrafiche tra i vari Stati. Nata originariamente come un "cartello internazionale" delle agenzie telegrafiche nazionali, nel tempo ha ampliato significativamente le proprie competenze, includendo anche la telefonia, la radiocomunicazione, le tecnologie satellitari e, più recentemente, le infrastrutture digitali.

Per comprendere il ruolo dell'ITU e il modo in cui ha gestito le telecomunicazioni via cavo e le tecnologie *wireless*, sia all'interno che oltre i confini nazionali nel corso del XX secolo, è fondamentale considerare le tre principali categorie normative elaborate dai suoi organi: la Convenzione Internazionale delle Telecomunicazioni, il Regolamento Internazionale delle

[103] Ivi, 120 ss.
[104] Ivi, 118.

Telecomunicazioni e le Raccomandazioni. Inoltre, le conferenze plenipotenziarie dell'ITU, organizzate periodicamente, hanno definito i principi generali che disciplinano i servizi di telecomunicazione, tra cui il diritto del pubblico ad accedere a tali servizi, la facoltà dei governi di sospenderli o interromperli, e la tutela delle infrastrutture fisiche, tutti formalizzati all'interno della Convenzione Internazionale delle Telecomunicazioni.

Negli anni '60 e '70, l'ITU ha avuto un ruolo significativo nello sviluppo di nuovi mercati nei Paesi emergenti e in via di sviluppo, grazie alle sue missioni di assistenza tecnica e alle esposizioni internazionali dedicate alle telecomunicazioni. Con la liberalizzazione del settore nei Paesi industrializzati negli anni '80, il Segretariato dell'Unione ha assunto un ruolo centrale nell'adeguare le normative che regolano l'accesso alle reti e la loro interoperabilità. Durante gli anni '90, in un contesto dominato da un ordine economico sempre più competitivo e liberale, l'ITU ha contribuito a promuovere la coesione sociale e a gestire le disparità, favorendo un approccio neutrale alle politiche neoliberali. Inoltre, ha guidato i Paesi in via di sviluppo nel processo di riforma dei propri sistemi di telecomunicazione, incoraggiando l'adozione di normative sugli investimenti e sulla proprietà delle reti e dei servizi[105].

A distanza di quasi 150 anni dalla sua fondazione e oltre sessant'anni dopo il suo riconoscimento come agenzia specializzata delle Nazioni Unite continua a svolgere un ruolo centrale nelle questioni inerenti alle tecnologie dell'informazione e delle comunicazioni[106].

L'ambito di operatività dell'Organizzazione si sviluppa su tre settori: radiocomunicazione, per quanto riguarda l'uso globale dello spettro e delle orbite satellitari; standardizzazione, dedicandosi allo sviluppo di standard nell'ambito delle telecomunicazioni e dell'ampliamento delle sue attività relative ad Internet; sviluppo, contribuendo alla realizzazione degli obbiettivi per lo Sviluppo Sostenibile (SDGs)[107].

---

[105] Sul punto MANSOURI, *Money, magic, and machines: International Telecommunication Union and liberalisation of telecommunications networks and services (1970s–1990s)*, in *London R. of Inter. L.*, 2023, 2, 235 ss.

[106] Così SHAHIN, *The role of the International Telecommunication Union*, in *Wereldbeeld*, 2010, 154, 11.

[107] Cfr. *L'unione internazionale delle Telecomunicazioni (ITU)*.

Attraverso interventi specifici in queste tre aree, l'ITU si concentra sul suo mandato principale, ovvero "connettere il mondo".

L'Unione fornisce anche un aiuto concreto ai Paesi in via di sviluppo, contribuendo al potenziamento delle capacità e il supporto allo sviluppo delle infrastrutture.

Inoltre, promuove diversi forum mondiali su tematiche come la politica delle telecomunicazioni e lo sviluppo radiofonico. Difatti, si è fatta promotrice del Vertice mondiale sulla società dell'informazione (WSIS), continuando ad essere coinvolta nel suo proseguimento attraverso l'*Internet Governance Forum* (IGF). Le tecnologie di telecomunicazione globali hanno subito una profonda evoluzione negli ultimi anni. Pertanto, di conseguenza, le istituzioni di *governance* globale, come l'ITU, si sono confrontate con un ambiente in cui il loro mandato originario è divenuto obsoleto, e probabilmente non più necessario, a causa di nuovi attori che hanno fatto propri i loro compiti e ruoli.

Tuttavia, anche se non è più il solo attore centrale, l'ITU mantiene un ruolo strategico nel coordinare la creazione di standard tecnici internazionali. In questo senso, può essere considerata un'istituzione ibrida che da un lato assume un ruolo di legittimazione delle iniziative degli Stati membri e, dall'altro si presenta come un forum per il coordinamento degli standard, grazie all'attività dei gruppi di studio che gestisce[108].

1.4.1.2. La Convenzione sulla criminalità informatica di Budapest del 2001

Il 23 novembre 2001 il Consiglio d'Europa ha approvato la Convenzione di Budapest, il primo strumento giuridico internazionale in materia di *cybercrime*.

Per la prima volta sono state introdotte delle nozioni tecniche specifiche del campo digitale, offrendo delle definizioni dei principali termini del *Web* e del crimine informatico.

Inoltre, ha istituito un sistema di cooperazione tra Stati per combattere i reati online, che spaziano dalla violazione del copyright fino alla pornografia minorile[109].

---

[108] V. SHAHIN, *The role of the International Telecommunication Union*, cit., 12 e 13 ss.
[109] Cfr. SANTARELLI, *Lotta al* cyber *crimine, ecco il secondo protocollo addizionale alla convenzione di Budapest: le finalità*, in *Cybersecurity360*, 2023, 5 s.

Questo documento normativo offre una soluzione globale al crescente rischio di esposizione a minacce informatiche. Attraverso il suo Programma sulla criminalità informatica, il Consiglio d'Europa fornisce a tutti i Paesi del mondo una risposta concreta a tale pericolo[110].

La Convenzione, mirando a istituire un quadro giuridico penale e processuale omogeneo tra gli Stati aderenti, costituisce ancora oggi il principale strumento di contrasto alla criminalità informatica[111].

Ciò che rende questo trattato particolarmente significativo è la composizione eterogenea degli Stati firmatari: in totale hanno vi hanno aderito 68 Stati, dei quali solo 47 sono membri del Consiglio d'Europa. Questa circostanza dimostra come sia possibile ottenere dei risultati comuni tra Paesi provenienti da tradizioni giuridiche diverse[112].

Nondimeno, l'impatto della Convenzione non è limitato ai soli Stati firmatari. Un'indagine sullo stato globale della legislazione sulla criminalità informatica, concluso nel 2020, ha dimostrato che circa il 92% degli Stati aveva avviato delle riforme o stava per farlo, e che 153 membri delle Nazioni Unite avevano adottato la Convenzione di Budapest come riferimento per tali interventi legislativi.

Inoltre, circa 106 Stati e, dunque, più della metà del totale, hanno adottato disposizioni di diritto penale che riflettono in linea generale le disposizioni della Convenzione.

Sul piano del diritto processuale, il 42% degli Stati si sono dotati poteri procedurali specifici. Diversamente, molti altri hanno continuato a fare affidamento su disposizioni procedurali generali per indagare sulla criminalità informatica e salvaguardare le prove elettroniche[113].

---

[110] Consiglio d'Europa, *Council of Europe action against Cybercrime*.

[111] In tal senso MONACO, *Prolegomena alla riforma del diritto penale dell'informatica nell'ordinamento giuridico della repubblica di San Marino*, in *Studi Urb., A - Sci. Giur. Pol. Econ.*, 2017, 3-4, 340.

[112] In argomento ARENA, *La convenzione di Budapest del Consiglio d'Europa Sulla repressione della criminalità informatica*, in *CRIO Papers*, 2021, 59, 5 s.

[113] Council of Europe*, The Budapest Convention on Cybercrime: benefits and impact in practice,* Strasbourg, 13 July 2020 così citato in ARENA, *La convenzione di Budapest del Consiglio d'Europa Sulla repressione della criminalità informatica*, cit., 6 s.

Primariamente, il Trattato in esame svolge una funzione di prevenzione rispetto a comportamenti illeciti che compromettono la segretezza, l'integrità e la disponibilità dei sistemi informatici, delle reti e dei dati, nonché l'utilizzo improprio di tali sistemi. Tale finalità preventiva si realizza attraverso la criminalizzazione di questi comportamenti e nell'adozione di poteri sufficienti a combatterli in modo efficace. Ciò consente di facilitare l'identificazione degli autori, le indagini e l'avvio di procedimenti penali, sia a livello nazionale che internazionale, prevedendo accordi per una collaborazione tra Stati più rapida ed efficiente.

Parimenti, richiamando la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, il Patto internazionale sui diritti civili e politici e ogni altri strumenti internazionale applicabile, la Convenzione mira a garantire un adeguato livello di bilanciamento tra le misure statali adottate dagli Stati per limitare l'accesso a Internet e il rispetto dei diritti fondamentali[114]. È possibile affermare che la Convenzione si articola su tre direttrici principali: la chiara definizione dell'ambito di applicazione delle misure processuali previste; l'introduzione di misure specifiche per l'acquisizione di dati informatici; e, infine, la previsione di misure coattive per ottenere tali dati da soggetti terzi.

Nello specifico, le misure coattive si concretizzano in disposizioni normative che gli Stati aderenti alla Convenzione devono adottare affinché venga garantita la conservazione dei dati informatici e del traffico, anche quando questi siano detenuti presso terzi, in particolare presso i *provider*. Tali soggetti hanno l'obbligo di proteggere e mantenere l'integrità dei dati per un periodo di tempo sufficiente a permettere alle autorità competenti di richiederne l'accesso o la divulgazione.

Talvolta i fornitori di servizi possono essere obbligati a fornire tutte le informazioni relative ai loro abbonati, dal tipo di servizio di comunicazione utilizzato a qualsiasi altro elemento utile alla loro identificazione, come l'indirizzo, il numero telefono, i dati di fatturazione e altri dati analoghi[115].

---

[114] Cfr. ARENA, *La convenzione di Budapest del Consiglio d'Europa Sulla repressione della criminalità informatica*, cit., 8.

[115] In tal senso SENOR, *Convenzione di Budapest: le modifiche al c.p.p. ed al codice della* privacy, in *Altalex*, 2008, 1.

All'inizio, il processo di approvazione della Convenzione di Budapest è stato accompagnato da incertezze e perplessità da parte degli Stati. Con il tempo però, è maturata una crescente consapevolezza dell'importanza di uno strumento giuridico di portata internazionale capace di delineare un quadro giuridico condiviso e indispensabile per far fronte alla criminalità informatica.

Questa consapevolezza si è concretizzata nel 2006, quando, a soli due anni dall'entrata in vigore della Convenzione, il Consiglio d'Europa ha approvato un Primo Protocollo addizionale volto a introdurre la criminalizzazione di atti di natura razzista e xenofobica commessi attraverso sistemi informatici.

A novembre 2021, il Comitato dei Ministri del Consiglio d'Europa è intervenuto nuovamente approvando il Secondo Protocollo Addizionale al fine di rafforzare a livello transnazionale i poteri delle autorità tenute all'applicazione della legge per il recepimento, l'archiviazione e l'impiego delle prove digitali.

In tal senso, esso non si limita a prevedere delle norme di carattere più generale, ma introduce delle specifiche disposizioni a carattere tecnico pensate per facilitare e accelerare le procedure di comunicazione tra autorità statali e fornitori di servizi. Queste norme riguardano in particolare la trasmissione di informazioni specifiche sugli abbonati, sui dati di traffico e sulla registrazione dei nomi di dominio.

Da ciò appare chiaro che le nuove norme in materia di indagini non interessano solo le autorità competenti dei Paesi, ma anche soggetti privati, come *provider* e società di telecomunicazione[116].

1.4.2. Il diritto dell'Unione europea

Negli ultimi anni, l'Unione europea si è focalizzata sulla tutela dei diritti *online*, con l'obiettivo di assicurare trasparenza ed equità nei contenuti.

L'attenzione si è spostata sulla protezione dei diritti all'interno di un nuovo spazio pubblico digitale, dove i fornitori di servizi assumono un ruolo sempre più centrale.

---

[116] Si rinvia a BUCCARELLA, *Il Secondo Protocollo addizionale alla Convenzione di Budapest e le nuove frontiere della cooperazione internazionale in ambito digitale. Quali rischi per la protezione dei dati personali nell'Unione europea?*, in *Quaderni AISDUE*, 2023, 8, 186 ss.

Per far fronte alla frammentazione del settore dell'informazione (c.d. *information disorder*), le politiche europee hanno promosso alcune *best practices*, vale a dire delle procedure volte ad armonizzare il settore digitale e ad assicurare trasparenza, a tutela degli utenti.

Queste iniziative nascono dalla consapevolezza che le piattaforme digitali non sono più neutre, ma sono in grado di influenzare l'opinione pubblica e di diffondere contenuti capaci di condizionare le idee, attraverso sistemi algoritmici.

In particolare, l'Unione europea, ha adottato una regolamentazione a "doppio binario": da un lato ha fissato, a livello sovranazionale, dei principi comuni; dall'altro, ha lasciato agli Stati membri il compito di individuare quali contenuti ritenere illeciti. In una prima fase, l'intervento dell'Ue si è concretizzato con atti di *soft law*, come i Codici di condotta che consentivano agli ISP di autoregolarsi, decidendo in autonomia l'adeguatezza dei contenuti pubblicati e comminando le relative sanzioni. In un secondo momento, però, la Commissione europea ha cambiato strategia, optando per una disciplina di *hard law*, basata sulla co-regolamentazione: in questo modello, le autorità pubbliche definiscono i principi generali, mentre i gestori delle piattaforme definiscono le norme di dettaglio, nel rispetto di tali principi.

L'obiettivo è quello di sancire delle procedure più strutturate e rendere competitivo il mercato digitale, fondato sui valori della Carta dei diritti fondamentali dell'Ue e delle tradizioni costituzionali comuni. Così, l'Unione ha intrapreso un percorso verso un costituzionalismo digitale, volto a sottoporre le piattaforme digitali a un controllo democratico attraverso regole *ex ante*[117]. Questa evoluzione normativa si è affermata con atti fondamentali come la Direttiva 2000/31 sul commercio elettronico, in tema di responsabilità degli intermediari di servizi telematici.

A questa Direttiva si sono affiancate poi altre norme a tutela dei dati personali degli utenti come la Direttiva 2002/58/CE, ma anche interventi più restrittivi come la Direttiva 2006/24/CE concernente la conservazione dei dati

[117] In questo senso GIRARDI, *Libertà e limiti della comunicazione nello spazio pubblico digitale*, cit., 155 s.

generati e trattati nell'ambito di servizi pubblici di comunicazione elettronica erogati tramite reti pubbliche[118].

1.4.2.1. Direttiva 2000/31/CE (*Direttiva sul commercio elettronico*)

La Direttiva sul commercio elettronico (Direttiva 2000/31/CE) rappresenta il primo intervento normativo a livello europeo volto a disciplinare la responsabilità dell'*Internet Service Provider*[119].

Questo provvedimento si inseriva in un contesto in cui l'Unione europea si trovava in contrasto con l'intraprendente modello americano, avvantaggiato da un settore informatico più avanzato. Grazie a tutte le sue potenzialità economiche, l'espansione di Internet costituiva un'imperdibile opportunità per favorire lo sviluppo e il benessere collettivo.

Tuttavia, non si può trascurare come la rete rappresenti un ambiente favorevole per la commissione di illeciti. Pertanto, la Direttiva ha cercato di trovare un punto di equilibrio tra due esigenze contrapposte: da una parte, rafforzare la fiducia dei consumatori, spesso diffidenti nei confronti del commercio elettronico, e, dall'altra, attenuare il regime di responsabilità dei *provider*, per evitare che un sistema troppo oneroso li scoraggiasse dal continuare a offrire i propri servizi, ormai indispensabili[120].

In quest'ottica, il provvedimento è stato emanato con l'intento di favorire la libera circolazione e la promozione dei "servizi della società dell'informazione", rimuovendo gli ostacoli che impedivano lo sviluppo del commercio elettronico e promuovendo l'attività degli ISP, evitando di imporre loro obblighi eccessivamente gravosi[121].

I capisaldi della Direttiva *E-Commerce* possono essere individuati in due caratteristiche di fondo. Innanzitutto, essa non prevede nessun obbligo generale di sorveglianza in capo al fornitore di servizi, sia esso un *mere conduit*, un *caching* o

---

[118]Cfr. PERDONÒ, *Le responsabilità penali collegate all'uso di* internet *fra comparazione e prospettive di riforma*, cit., 326 ss.
[119] V. ABALDO, *Una prospettiva di regolamentazione degli ISP attraverso il* DigitalService Act, in *MediaLaws*, 2022, 1.
[120] Così FERRARESE, *La responsabilità civile degli* internet provider*: un'analisi degli artt. 14 – 17 del d.lgs. N. 70/2003*, in *Jei-Jus e Internet*, 2008, 1.
[121] Cfr. ALLEGRI, Ubi Social, Ibi Ius. *Fondamenti costituzionali dei* social network *e profili giuridici della responsabilità dei* provider, Milano, 2018, 54.

un *hosting provider*. Questo obbligo implicherebbe un controllo *ex ante* dei flussi di comunicazioni elettroniche trasmessi e dei contenuti pubblicati dagli utenti. La previsione di un tale dovere sarebbe problematica per diversi motivi. Non solo perché una sorveglianza preventiva risulterebbe tecnicamente impossibile, ma anche perché renderebbe economicamente sconveniente l'attività dell'ISP. Egli, infatti, dovrebbe sostenere dei costi elevati per implementare i sistemi di filtraggio e incorrerebbe nel rischio di responsabilità nei confronti degli utenti, venendo di fatto trasformato in un censore privato.

Inoltre, è grazie alla capacità dei fornitori di sviluppare nuovi modelli economici in grado di favorire lo scambio e la circolazione di contenuti che è aumentata la possibilità di esercitare la libertà di manifestazione del pensiero.

Chiaramente, riconoscere il contributo dei *provider* non può significare esonerarli da ogni genere di responsabilità.

Il secondo caposaldo, strettamente legato al primo, riguarda gli obblighi che insorgono in capo all'ISP nella fase *ex post*. Egli è tenuto ad attivarsi nel caso in cui venga effettivamente a conoscenza di fatti o attività illecite da parte degli utenti che si avvalgono dei suoi servizi. In caso contrario, potrà essere considerato responsabile al pari dell'utente che ha commesso l'attività illecita[122].
Con la legge delega 1° marzo 2002, n. 39 e il d. lgs. 9 aprile 2003, n. 70, il legislatore italiano ha recepito la Direttiva avviando il processo di armonizzazione in materia di responsabilità dell'ISP, limitandosi a trasporre il contenuto nel diritto interno[123].

Come già precedentemente visto, tre sono le tipologie di *provider* che si distinguono in base all'attività che viene concretamente svolta: *mere conduit*, *caching* e *hosting*[124].

Negli articoli 14, 15 e 16 del d.lgs. 70/2003 si afferma semplicemente che i fornitori di servizi non rispondono dei contenuti veicolati per loro tramite, a condizione che non intervengano su di essi.

---

[122] In tal senso BASSINI, *La rilettura giurisprudenziale della disciplina sulla responsabilità degli* internet service provider*. Verso un modello di responsabilità «complessa»?*, in *Federalismi.it*, 2015, 3, 46 ss.
[123] V. MICELI, *Profili evolutivi della responsabilità in Rete: il ruolo degli* Internet Service Provider *tra prevenzione e repressione*, in *MediaLaws*, 2017, 1, 109.
[124] A riguardo ABALDO, *Una prospettiva di regolamentazione degli ISP attraverso il* Digital Service Act, cit., 1.

Agli articoli 12 comma 3, 13 comma 2 e 14 comma 3, della direttiva 2000/31/CE relativi alle tre principali categorie di *provider*, si riconosce agli Stati membri la possibilità di autorizzare un organo giurisdizionale o un'autorità amministrativa a ordinare al prestatore di interrompere la violazione e, con riferimento alla sola attività di *hosting*, consente si predisporre delle procedure per la rimozione dei contenuti illeciti o la disattivazione dell'accesso agli stessi.

Inoltre, l'articolo 17 del d.lgs. 70/2003 – corrispondente all'art. 15 della Direttiva – esclude un sia la possibilità di prevedere un obbligo generale di sorveglianza a carico dei *provider* sui contenuti trasmessi o memorizzati, che un dovere di ricercare attivamente eventuali condotte illecite.

Tuttavia, il comma 2 dell'art. 17 del d.lgs. 70/2003 consente agli Stati membri è consentito imporre ai prestatori di servizi di informare tempestivamente all'autorità competente qualsiasi attività o informazione illecita di cui vengano a conoscenza, nonché di comunicare, su richiesta, le informazioni utili a identificare i destinatari dei servizi con cui abbiano stipulato accordi per la memorizzazione delle informazioni.

Infine, gli Stati possono introdurre degli standard di diligenza per gli intermediari, volti a individuare preventivamente i contenuti illeciti, senza però trasformarli in un vero e proprio dovere di ricercarli attivamente[125]. Questo assetto normativo è rimasto in vigore per più di vent'anni, talvolta rivelandosi inadeguato alle diverse situazioni concrete, richiedendo quindi di essere integrato dall'intervento ermeneutico della giurisprudenza.

Quest'ultima, infatti ha finito per arricchire le regole sulla responsabilità dell'ISP che il legislatore europeo è dovuto intervenire nuovamente sull'argomento[126].

1.4.2.2. Direttiva 2011/93/UE (*Direttiva sull'abuso sessuale e la pedopornografia online*)

[125] Così MICELI, *Profili evolutivi della responsabilità in Rete: il ruolo degli* Internet Service Provider *tra prevenzione e repressione*, cit., 109.
[126] In argomento MASSA, *L'evoluzione della responsabilità degli* internet service providers*: dalla direttiva e-commerce al* Digital Services Act, in *Giustizia*, 2022, 2, 45.

L'abuso e lo sfruttamento sessuale dei minori costituiscono, prima ancora che un fenomeno giuridico-penale, un problema sociale di grande rilevanza, che genera un forte allarme collettivo. Si tratta di un fenomeno complesso e articolato, la cui riduzione a un'unica definizione rischierebbe di semplificare la sua gravità.

La protezione dei minori da condotte di violenza sessuale rappresenta una priorità fondamentale per le politiche criminali. In questa prospettiva, le Organizzazioni Internazionali hanno svolto un ruolo decisivo, promuovendo il progressivo avvicinamento delle normative nazionali e incentivando una cooperazione rafforzata tra autorità giudiziarie e di polizia, con l'obiettivo principale di migliorare le strategie di prevenzione e contrasto delle condotte illecite commesse ai danni dei minori[127].

Considerando la gravità del fenomeno degli abusi sessuali di minori commessi in rete, un settore particolarmente delicato è quello relativo ai contenuti pedopornografici.

Queste condotte esistono sin dagli albori della comunicazione *online*, ma con l'avvento della pandemia da coronavirus hanno registrato un incremento, a causa del maggior utilizzo di Internet da parte dei minori costretti a rimanere in casa[128].

L'abuso sessuale dei minori, sia *online* che *offline*, si configura come un reato di natura transfrontaliera, che richiede quindi una collaborazione internazionale per arginarlo. Le reti criminali attive in questo ambito sono molto sofisticate e le autorità di contrasto spesso si trovano a far fronte a questi fenomeni con strumenti normativi non sempre adeguate e aggiornate alle esigenze del futuro[129]. Al fine di contrastare tali fenomeni, sempre più frequenti, il legislatore dell'Unione europea ha adottato la Direttiva 2011/93/UE. L'obiettivo perseguito dalla citata Direttiva è armonizzare ulteriormente le legislazioni penali nazionali in materia di abuso e sfruttamento sessuale dei minori, pornografia minorile e

---

[127] V. BAFFA, MASSARO, *Pedopornografia* online*: strumenti di prevenzione e contrasto*, Roma, 2020, 15 s.

[128] Cfr. MORGESE, *Moderazione e rimozione dei contenuti illegali* online *nel diritto dell'UE*, in *Federalismi.it*, 2022, 1, 93.

[129] V. Parlamento europeo, *Relazione sull'attuazione della direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile (2015/2129(INI))*, 2017, 3.

adescamento di minori per scopi sessuali, stabilendo degli standard minimi per la definizione di questi reati e delle relative sanzioni applicabili.

Inoltre, mira introdurre delle norme volte a rafforzare le misure di prevenzione e a garantire la tutela delle vittime minorenni.

Sebbene la materia fosse già oggetto di regolamentazione da parte di altri atti normativi, quali la Carta dei diritti fondamentali dell'Unione europea e la Convenzione ONU sui diritti del fanciullo, il legislatore europeo ha sentito comunque l'esigenza di intervenire, talvolta dettando disposizioni dal contenuto analogo poiché la Direttiva, per la sua diversa forza applicativa prevede la possibilità di attivare una procedura d'infrazione contro gli Stati membri che non rispettano le sue disposizioni[130].

Anzitutto, la Direttiva stabilisce che gli Stati membri debbano mettere a disposizione dei responsabili delle indagini e dell'azione penale degli strumenti adeguati per indagare sui reati di abuso sessuale a danno di minori e per individuare rapidamente le vittime.

In queste situazioni è spesso complicato determinare quale Stato abbia la giurisdizione e quale sia la normativa da applicare per l'acquisizione delle prove. Per questo motivo, la Direttiva amplia la competenza giurisdizionale per tali reati ed elimina il principio di doppia incriminazione[131], riconoscendo come essenziale un rafforzamento della cooperazione internazionale ed europea.

La Direttiva, inoltre, incoraggia gli Stati a promuovere delle campagne di informazione, sensibilizzazione del fenomeno, e formazione dei soggetti coinvolti.

In aggiunta, al fine di ridurre il rischio di recidiva, questa fonte normativa promuove l'introduzione di misure interdittive in caso di condanna e dei programmi di intervento mirati per le persone condannate.

La rimozione del materiale pedopornografico *online* da parte degli Stati membri deve essere attuata tempestivamente, secondo quanto stabilito dall'articolo 25 della Direttiva. Tale disposizione si pone l'obiettivo di assicurare la prevenzione

---

[130] In tal senso VERRI, *Contenuto ed effetti (attuali e futuri) della Direttiva 2011/93/UE. Approvate dal legislatore europeo nuove norme contro l'abuso, lo sfruttamento sessuale dei minori e la pornografia minorile*, in *DPC.*, 2012, 1 s.

[131] V. Enciclopedia Treccani, "*In via generale, ai fini dell'estradizione passiva il principio della doppia incriminazione stabilisce che il fatto deve costituire reato per la legge penale sia dello Stato richiedente, che di quello concedente, indipendentemente dalla diversità dei regimi sanzionatori*".

dell'abuso e dello sfruttamento sessuale dei minori, nonché di assicurare la riduzione della vittimizzazione secondaria.

La rimozione del materiale pedopornografico non è limitata ai siti *Web* ospitati nel territorio degli Stati membri, ma anche a quelli ospitati altrove. In particolare, per quanto riguarda il materiale ospitato al di fuori del loro territorio è prevista l'istituzione di una linea telefonica di pronto intervento per valutare il materiale ed eventualmente contattare il Paese in cui il sito *Web* è ospitato.

Questa linea telefonica può essere predisposta o attraverso la rete INHOPE o con la collaborazione di Europol[132] o Interpol[133].

È inoltre prevista la possibilità di introdurre delle misure di blocco volte a impedire l'accesso al materiale pedopornografico, misure spesso attuate utilizzando "liste nere" di siti Web contenti tale materiale. Tuttavia, l'attuazione di queste misure è stata effettuata solo dalla metà degli Stati membri. In ogni caso, la partecipazione attiva dei fornitori di servizi della società dell'informazione resta fondamentale – seppur spesso volontaria – per rendere possibile il processo di rimozione e blocco del materiale pedopornografico *online*[134].

1.4.2.3. Direttiva 790/2019/UE (*Direttiva sul diritto d'autore nel mercato unico digitale*)

Per garantire che l'ordinamento giuridico sia adeguato al rapido sviluppo delle tecnologie informatiche e alle esigenze di tutela dei diritti sulle opere d'ingegno che ne sono conseguite, il legislatore comunitario si è occupato della delicata questione della responsabilità dell'ISP in relazione alla diffusione delle opere protette dal diritto d'autore da parte degli utenti.

---

[132] L'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto – Europol è un'agenzia dell'Unione europea con sede all'Aia (Paesi Bassi), il cui obiettivo principale è rafforzare la sicurezza in Europa. La sua missione consiste nel sostenere i paesi dell'Ue nella prevenzione e nella lotta contro il crimine internazionale e il terrorismo. A tal fine, facilita agevola la cooperazione tra le autorità di polizia nazionali dei paesi dell'Ue e le autorità preposte all'applicazione della legge.

[133] L'Organizzazione internazionale della polizia criminale – Interpol è un'organizzazione che coordina l'attività di polizia internazionale dei Paesi che ne fanno parte, al fine di contrastare la criminalità organizzata a livello globale.

[134] Cfr. Parlamento europeo, *Relazione sull'attuazione della direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile (2015/2129(INI))*, cit., 4 ss.

Le Direttive 1996/9/CE e 2001/29/CE, che hanno rispettivamente disciplinato i diritti d'autore sulle banche dati e i diritti d'autore nella società dell'informazione, non erano più adeguate a rispondere all'evoluzione tecnologica e alle sfide legate alla tutela delle opere d'ingegno.

Per far fronte a tali criticità, è stata adottata la Direttiva 790/2019 volta ad aggiornare e rafforzare la tutela del diritto d'autore nel mercato digitale[135].

In altre parole, le normative precedenti miravano soprattutto a introdurre nuove e maggiori tutele di fronte all'esponenziale avanzamento tecnologico.

Diversamente, il legislatore europeo ha scelto di favorire la diffusione della cultura e dell'informazione, incoraggiando al contempo la creazione di nuovi contenuti e incentivando gli investimenti nel settore digitale. Questo approccio è stato accompagnato dalla volontà di garantire un alto livello di tutela autoriale delle opere diffuse in rete, in risposta alla crescente circolazione di opere protette da copyright, spesso condivise senza il consenso dei titolari. Tale fenomeno è stato amplificato dalla rapida espansione delle grandi piattaforme digitali, che hanno reso sempre più accessibile la distribuzione dei contenuti su larga scala. Di conseguenza, per evitare che la normativa esistente limitasse il progresso quotidiano, si è reso necessario aggiornare il quadro giuridico precedente alle nuove esigenze del mercato.

La Direttiva 790/2019 introduce delle norme pensate per rendere più uniforme il quadro giuridico comunitario in materia di diritto d'autore e diritti connessi. Tra le principali finalità vi è quella di armonizzare le eccezioni e le limitazioni al diritto d'autore, soprattutto nei campi della ricerca scientifica, dell'istruzione e della conservazione del patrimonio culturale. La Direttiva si propone, inoltre, di semplificare le procedure per la concessione delle licenze e di migliorare il funzionamento complessivo del mercato delle opere dell'ingegno. Queste misure, nel loro insieme, mirano a rafforzare il mercato interno dell'Unione europea, con particolare attenzione al settore digitale[136].

---

[135] Si rinvia a COSTA, *La responsabilità dell'*Internet Service Provider *per i reati in materia di diritto d'autore*, *Giur.pen.*, 2022, 2, 20 s.

[136] V. SCENNA, *Il bilanciamento tra i diritti d'autore e i diritti fondamentali alla luce della direttiva UE 2019/790. Note alla sentenza della Corte di giustizia europea*, in *DPCE Online*, 2022, 3, 1759 s.

Un aspetto centrale della Direttiva *Copyright* è rappresentato dall'articolo 17, che impone ai prestatori di servizi *online* di ottenere dai titolari dei diritti l'autorizzazione, tramite accordi di licenza, quando rendono accessibile al pubblico opere o altri materiali caricati dagli utenti.

Questa autorizzazione copre anche gli atti compiuti dagli utenti, purché non operino a fini commerciali o non generino ricavi significativi.

Nel caso in cui dovesse mancare l'autorizzazione, il fornitore del servizio sarà chiamato a rispondere per la diffusione di opere o materiali coperte dal diritto d'autore.

Tuttavia, non è ritenuto responsabile se dimostra di aver fatto il possibile per ottenere la predetta autorizzazione, di aver adottato misure adeguate per evitare che opere protette siano accessibili e di essere intervenuto tempestivamente per disabilitare l'accesso o rimuovere il contenuto protetto dal proprio sito Web e prevenirne il caricamento futuro.

Dal punto di vista degli utenti, la Direttiva stabilisce che, per i contenuti caricati e condivisi, essi possano beneficare di alcune eccezioni, come la citazione, la critica, la rassegna o l'uso per fini di parodia, caricatura o pastiche, garantendo così gli usi legittimi previsti dal diritto comunitario.

In caso di rimozione o blocco dei contenuti, sono previsti dei meccanismi di reclamo e di ricorso, anche stragiudiziale, e obblighi di informativa delle piattaforme nei confronti degli utenti.

Pertanto, anche se viene confermata l'assenza di un obbligo generale di sorveglianza da parte delle piattaforme, la Direttiva rafforza comunque i loro doveri e le loro responsabilità[137].

1.4.2.4. Regolamento UE 2021/784 (*Regolamento sul contrasto alla diffusione di contenuti terroristici online*)

A seguito ai drammatici attentati dell'11 settembre 2001, l'Unione europea ha riconosciuto l'urgenza di adottare strategie efficaci per prevenire e contrastare il terrorismo internazionale: da un lato, attraverso misure repressive volte a

[137] In tal senso ZANCAN, *La nuova direttiva sul diritto d'autore e sui diritti connessi nel mercato unico digitale*, in *MediaLaws*, 2019, 2, 342 s.

uniformare le normative penali tra gli Stati membri e a potenziare la cooperazione giudiziaria e lo scambio di informazioni; dall'altro, mediante l'attuazione di politiche di sicurezza e iniziative socio-culturali capaci di contrastare il fenomeno della radicalizzazione violenta[138].

L'evoluzione normativa dell'Unione europea in materia di contrasto al terrorismo, in particolare, prende avvio dalla decisione quadro 2002/475/GAI[139]. L'obiettivo principale di tale provvedimento – che si fonda sul riconoscimento del terrorismo come una delle più gravi minacce ai principi fondamentali della democrazia e dello stato di diritto, considerati patrimonio comune degli Stati membri – era quello di uniformare la definizione dei reati terroristici all'interno dell'Unione.

Successivamente la disciplina è stata aggiornata con la decisione quadro 2008/919/GAI[140], che assume particolare importanza poiché, a differenza del testo del 2002, pone l'accento sul crescente impatto delle tecnologie digitali e, in particolare, sull'utilizzo di Internet nel contesto delle attività terroristiche.

Il momento decisivo nella strategia antiterrorismo dell'Unione, che segna l'inizio del coinvolgimento attivo dei *social network*, si è verificato dopo l'attentato del 7 gennaio 2015 contro la redazione del giornale satirico "*Charlie Hebdo*" a Parigi.

In risposta a questo attacco, infatti, il Parlamento europeo ha approvato una risoluzione[141] nella quale, riconoscendo che la propaganda terroristica trova terreno fertile nella diffusione attraverso Internet e le piattaforme *social*, ha invitato le aziende del settore digitale a collaborare con i governi, le autorità competenti e la società civile per contrastare il terrorismo, nel rispetto della libertà di espressione e della privacy degli individui.

Nel 2016, in seguito all'attentato terroristico avvenuto a Bruxelles, l'Unione europea ha deciso altresì di introdurre il Codice di condotta per contrastare le forme

---

[138] Sul punto PEZZUTO, *Contenuti terroristici* online*: l'Unione europea lavora a nuove norme per prevenirne la diffusione*, in *DPC*, 2019, 4, 35.

[139] Decisione quadro del Consiglio del 13 giugno 2002 sulla lotta contro il terrorismo (2002/475/GAI).

[140] Decisione quadro 2008/919/GAI del Consiglio del 28 novembre 2008 che modifica la decisione quadro 2002/475/GAI sulla lotta contro il terrorismo.

[141] Risoluzione del Parlamento europeo dell'11 febbraio 2015 sulle misure antiterrorismo (2015/2530(RSP)).

illegali di incitamento all'odio *online*, in base al quale le aziende digitali che vi aderiscono si impegnano attivamente a combattere i contenuti che promuovono odio in rete. Inoltre, tra le prescrizioni previste dal Codice, assume rilevanza il meccanismo di *notice and takedown*, che permette agli utenti delle piattaforme di segnalare la presenza di contenuti illegali su queste ultime[142].

Nel 2017 l'Unione europea è intervenuta nuovamente in materia, adottando la Direttiva 2017/541[143], che rappresenta uno degli strumenti principali adottati in risposta alla crescente minaccia degli attentati terroristici – spesso riconducibili a gruppi legati all'estremismo islamico – sul territorio europeo.La Direttiva, pur disciplinando la rimozione dei contenuti terroristici *online*, non si limita a tale ambito. Infatti, essa può essere considerata una normativa di carattere generale, in quanto contempla disposizioni che intervengono su molteplici ambiti rilevanti nella lotta contro il terrorismo internazionale: dalla definizione delle fattispecie di reato terroristico e atti preparatori, alla protezione delle vittime e dei loro familiari; dalle strategie di contrasto dei *foreign fighters*, al finanziamento delle organizzazioni terroristiche, sino alle misure volte a prevenire la radicalizzazione attraverso la rete.

Con riferimento alla rimozione dei contenuti terroristici *online*, particolarmente rilevante è l'art. 21 della Direttiva, che impone agli Stati membri di «assicurare la tempestiva rimozione dei contenuti online ospitati nel loro territorio che costituiscono una pubblica provocazione per commettere un reato di terrorismo»[144] e di adoperarsi per ottenere la rimozione di contenuti analoghi ospitati al di fuori del loro territorio. Tuttavia, la Direttiva non contiene alcun riferimento all'utilizzo di strumenti automatizzati, sebbene questi siano largamente impiegati nella pratica. Pertanto, pur affrontando la questione della rimozione dei contenuti pericolosi di stampo terroristico, la normativa lo fa in modo limitato,

[142] Sul punto STELLA, *Il contrasto alla diffusione dei contenuti terroristici* online *a seguito dell'adozione del* Digital Services Act*: riflessi sulla tutela della libertà di espressione*, in *DPCE Online*, 2025, 2, 801 s.
[143] Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio.
[144] Direttiva (UE) 2017/541, art. 21.

tralasciando il delicato aspetto legato ai meccanismi automatizzati di rilevamento e rimozione[145].

Un ulteriore aspetto particolarmente significativo è rappresentato dal reato di "pubblica provocazione alla commissione di atti terroristici", disciplinato dall'art. 5 della Direttiva. A differenza di quanto previsto dalla decisione quadro 2008/919/GAI, questa definizione estende esplicitamente la rilevanza del reato anche all'ambito digitale, riconoscendo la possibilità che esso venga commesso *online*[146].

In merito alla rimozione dei contenuti *online* che incitano pubblicamente alla commissione di atti terroristici, è intervenuto anche il Consiglio europeo nelle conclusioni formulate durante la riunione del 22 e 23 giugno 2017. In tale occasione, è stato sottolineato che il settore privato ha la responsabilità di collaborare attivamente nella lotta contro il terrorismo e la criminalità informatica.

Il processo di responsabilizzazione delle piattaforme digitali, in tal senso, ha trovato concreta attuazione con la Raccomandazione (UE) 2018/334[147], volta a contrastare in modo efficace la diffusione di contenuti illeciti *online*. In tale contesto, infatti, la Commissione europea ha sottolineato il dovere delle piattaforme di tutelare gli utenti, impedendo che i servizi offerti vengano strumentalizzati da soggetti coinvolti in attività criminali. Le piattaforme sono quindi chiamate a individuare, bloccare e rimuovere contenuti illegali, garantendo al contempo il rispetto dei diritti fondamentali. In particolare, data la loro centralità nell'accesso all'informazione, è essenziale evitare la rimozione ingiustificata di contenuti leciti, che potrebbe compromettere la libertà di espressione e il pluralismo informativo.

---

[145] Così GRAZIANI, *Intelligenza artificiale e fonti del diritto: verso un nuovo concetto di* soft law*? La rimozione dei contenuti terroristici* online *come* case-study, in *DPCE Online*, 2022, 1478.

[146] Art. 5 Direttiva (UE) 2017/541 – "Pubblica provocazione per commettere reati di terrorismo": «Gli Stati membri adottano le misure necessarie affinché sia punibile come reato, se compiuta intenzionalmente, la diffusione o qualunque altra forma di pubblica divulgazione di un messaggio, con qualsiasi mezzo, sia online che offline, con l'intento di istigare alla commissione di uno dei reati di cui all'articolo 3, paragrafo 1, lettere da a) a i), se tale comportamento, direttamente o indirettamente, ad esempio mediante l'apologia di atti terroristici, promuova il compimento di reati di terrorismo, creando in tal modo il pericolo che uno o più di tali reati possano essere commessi».

[147] Raccomandazione (UE) 2018/334 della Commissione del 1° marzo 2018 sulle misure per contrastare efficacemente i contenuti illegali *online*.

Le esigenze di un quadro più incisivo e uniforme hanno portato all'adozione del Regolamento (UE) 2021/784[148], relativo al contrasto della diffusione dei contenuti terroristici *online*. Il regolamento nei suoi considerando riconosce che l'Unione europea ha avviato iniziative basate sulla cooperazione volontaria tra Stati membri e *provider* sin dal 2015 ma che, ad oggi, queste devono essere rafforzate da un quadro normativo chiaro e vincolante, capace di limitare ulteriormente l'accesso a contenuti pericolosi[149].

Nella sua versione attuale, il Regolamento introduce un insieme di regole armonizzate volte ad assicurare la rapida rimozione dei contenuti terroristici presenti *online*.

In particolare, il principale strumento di contrasto consiste nell'adozione degli ordini di rimozione (o.d.r.), previsti dall'art. 12 par. 1, lett. a) e b) del Regolamento. La disciplina prevede che l'autorità competente di ciascuno Stato membro possa emettere un o.d.r., imponendo ai prestatori di servizi di eliminare i contenuti terroristici o di disabilitarne l'accesso in tutto il territorio dell'Unione, comunicandone procedure e termini da rispettare con almeno 12 ore di preavviso. Conseguentemente, gli *hosting provider* sono tenuti a rimuovere i contenuti terroristici o a disabilitare l'accesso a tali contenuti in tutti gli Stati membri nel più breve tempo possibile, e comunque, non oltre un'ora dal ricevimento dell'o.d.r.

Ai fini della sussistenza di eventuali ipotesi di reato, il prestatore di servizi di *hosting* è anche tenuto a indicare all'autorità competente la data e l'ora dell'eventuale rimozione o disabilitazione[150].

Per garantire il rispetto di tali obblighi, il Regolamento prevede l'applicazione di sanzioni pecuniarie significative in caso di inadempienza, che possono arrivare fino al 4% del fatturato globale registrato dal *provider* nell'esercizio finanziario precedente[151].

---

[148] Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio del 29 aprile 2021 relativo al contrasto della diffusione di contenuti terroristici *online*.

[149] V. STELLA, *Il contrasto alla diffusione dei contenuti terroristici* online, cit., 803 ss.

[150] In argomento CISTERNA, *Il contrasto al terrorismo* online *e la tutela delle infrastrutture informatiche*, in *Dir. pen. proc.*, 2023, 11, 1436.

[151] Reg. (UE), art. 18, par. 3: «Gli Stati membri provvedono a che la sistematica o persistente inosservanza degli obblighi ai sensi dell'articolo 3, paragrafo 3, sia passibile di sanzioni pecuniarie fino al 4 % del fatturato mondiale del prestatore di servizi di hosting del precedente esercizio finanziario».

Ciononostante, alcune previsioni del Regolamento sono state oggetto di censure.

La prima riguarda la definizione di "contenuto terroristico" su cui si basa l'intero impianto normativo. L'art. 2, par. 7, propone una formulazione particolarmente ampia, individuando cinque categorie di materiali che possono essere classificati come "contenuti terroristici": i primi sono quelli che incitano, anche indirettamente, alla commissione di atti terroristici; i secondi sono quelli che ne sollecitano l'esecuzione; i terzi sono quelli che hanno la finalità invitare gli utenti a unirsi a gruppi terroristici; i quarti sono quelli che forniscono istruzioni sull'uso di armi, esplosivi o sostanze pericolose; e infine, gli ultimi sono quelli che costituiscono una minaccia di compiere reati di matrice terroristica.

Tuttavia, l'art. 1, par. 3, esclude dalla rimozione i contenuti diffusi per finalità educative, giornalistiche, artistiche, di ricerca, di prevenzione o di contrasto al terrorismo, nonché le opinioni espresse nell'ambito del dibattito politico.

Nonostante ciò, la dottrina[152] ha sollevato preoccupazioni circa l'ampiezza della definizione adottata, che potrebbe lasciare spazio a interpretazioni soggettive e, di conseguenza, portare alla rimozione di contenuti che non rientrano realmente nella categoria dei materiali terroristici.

Questo rischio è ulteriormente aggravato dalla previsione di sanzioni economiche significative, che potrebbe indurre gli *hosting provider* a optare per la rimozione indiscriminata dei contenuti, senza effettuare le necessarie verifiche.

Un secondo elemento problematico riguarda l'assenza nel Regolamento di una chiara definizione dell'autorità competente a disporre la rimozione dei contenuti ritenuti terroristici. Questa lacuna ha portato i singoli Stati membri ad attribuire tale funzione a enti molto diversi tra loro: ad esempio, alle forze di polizia (come in Germania, Irlanda e Svezia), oppure al Ministero dell'Interno (come in Spagna) o, ancora, alle Procure (come in Italia).

Questa libertà di scelta potrebbe però, secondo la dottrina[153], compromettere il principio di separazione dei poteri, soprattutto laddove non sia previsto un

[152] Cfr. ROJSZCZAK, *Gone in 60 Minutes: Distribution of Terrorist Content and Free Speech in the European Union*, in *Democracy & Sec.*, 2024, 192.
[153] V. FERRARIO, *La portata transnazionale del regolamento (UE) 2021/784 e i possibili profili di incompatibilità con le normative di Stati terzi: un'analisi comparata*, in IMPARATO, PIGNATIELLO (a

controllo giurisdizionale sull'ordine di rimozione. Inoltre, questa eterogeneità rischia di ostacolare l'applicazione coerente e uniforme del Regolamento a livello europeo.

Una terza criticità riguarda la dimensione transnazionale del Regolamento: poiché i contenuti terroristici vengono spesso diffusi da fornitori di servizi di *hosting* con sede legale al di fuori dell'Ue, l'art. 4 del Regolamento consente alle autorità nazionali competenti di ordinare la rimozione di tali contenuti, purché siano accessibili nel territorio degli Stati membri.

Per rendere operativa questa disposizione, l'art. 17 impone ai fornitori di *hosting* privi di una sede principale nell'UE di nominare un rappresentante legale incaricato di ricevere e gestire gli ordini di rimozione provenienti dalle autorità degli Stati membri.

Sebbene questa misura rafforzi l'efficacia del Regolamento, da un lato si teme che alcuni Stati membri possano abusare della definizione ampia di "contenuto terroristico" per giustificare la rimozione di materiali scomodi, limitando così la libertà di espressione e reprimendo il dissenso politico; dall'altro lato, l'applicazione extraterritoriale del Regolamento potrebbe entrare in contrasto con le normative vigenti nei Paesi terzi, che pur non facendo parte dell'Unione europea, si troverebbero comunque coinvolti nell'attuazione delle disposizioni europee.

L'enorme aumento dei contenuti condivisi *online*, insieme alle tempistiche estremamente ristrette previste dal Regolamento, ha reso sostanzialmente impossibile affidare la gestione di tali attività esclusivamente all'intervento umano.

Per rispettare gli obblighi imposti dalla normativa, infatti, come già rilevato molto spesso i fornitori di servizi di *hosting* utilizzano strumenti automatizzati, facendo ricorso in particolare a tecnologie di *hashing*[154] e ad algoritmi basati su

---

cura di), *La libertà di espressione nel diritto comparato tra stato di diritto e stati di emergenza*, Torino, 2024, 344 ss.

[154] Il termine *hashing* indica un processo di corrispondenza che si basa sulla generazione di un *hash*, cioè una sorta di impronta digitale del contenuto. Quando viene rilevato un materiale potenzialmente terroristico, come un'immagine o un video, questo viene trasformato in un codice univoco e archiviato in un *database*. In seguito, se un contenuto simile viene caricato *online*, il sistema lo riconosce rapidamente grazie al confronto con l'*hash* già registrato, permettendone la rimozione prima che possa diffondersi ampiamente.

machine learning[155] e *natural language processing*[156]; aspetti questi oggi ancor più di centrale rilevanza alla luce dell'entrata in vigore dell'*AI Act.*

Sebbene l'impiego di sistemi automatizzati consenta di trattare enormi volumi di dati e di rilevare e cancellare con rapidità i contenuti di natura terroristica, il loro utilizzo solleva diverse problematiche significative, in particolare di natura tecnica, giuridica ed etica.

Innanzitutto, gli strumenti automatizzati portano con sé il rischio di identificare i c.d. "falsi positivi" (contenuti in realtà non terroristici) e i c.d. "falsi negativi" (contenuti terroristici non identificati come tali e, pertanto, non rimossi).

Inoltre, questi sistemi non tengono conto del contesto in cui tali contenuti vengono caricati.

A tutto ciò si affianca il problema di una definizione accurata di "contenuto terroristico" , per cui diviene fondamentale una forma di coerenza negli effetti che questi sistemi automatizzati hanno sulle varie piattaforme.

Emblematico sul tema è il caso delle c.d. *Big Four*[157] che, per questo motivo, hanno creato un database condiviso in base al quale ogni contenuto ritenuto illegale su una piattaforma viene automaticamente eliminato anche dalle altre. Resta difficile da risolvere il fatto che l'evoluzione delle tecniche impiegate dai terroristi renda l'elusione dei sistemi automatizzati sempre più facile.

Oltre a rischi di natura tecnica, i sistemi automatizzati portano con sé anche rischi di natura giuridica. In particolare, non è raro che l'utilizzo di tali sistemi renda difficile il bilanciamento tra il contrasto del terrorismo online e la tutela dei diritti fondamentali. Inoltre, questi stessi sistemi rischiano di essere oggetto di strumentalizzazione da parte di alcuni Stati che, avvalendosi di un'ampia definizione di "contenuto terroristico", potrebbero sfruttarli per la rimozione di contenuti "scomodi", come quelli provenienti da oppositori politici, ambienti accademici, giornalistici o religiosi.

---

[155] Il *machine learning* è una branca dell'intelligenza artificiale focalizzata sulla creazione di algoritmi capaci di apprendere automaticamente e di analizzare grandi quantità di dati eterogenei in tempi estremamente rapidi.

[156] Il *natural language processing* (NLP) è un settore dell'intelligenza artificiale che si occupa di sviluppare tecniche informatiche capaci di rendere il linguaggio umano interpretabile dai computer, permettendo loro non solo di comprenderlo, ma anche di produrlo autonomamente.

[157] Facebook, Google, Microsoft e Twitter.

Resta anche da considerare che, dietro la decisione di rimuovere un certo contenuto, vi è comunque la presenza degli *hosting service provider*, i quali, mossi da ragioni prettamente economiche, molto spesso si disinteressano del rispetto dei diritti fondamentali.

Anche il diverso standard di protezione della libertà di espressione tra i diversi Paesi rappresenta un problema, soprattutto in ragione della portata transnazionale del Regolamento.

Infine, l'utilizzo di strumenti automatizzati potrebbe anche ledere la libera concorrenza nel mercato. Basti pensare al fatto che, assoggettando tutte le piattaforme –grandi e piccole – alla regola di rimozione entro un'ora, molte di queste ultime si potrebbero trovare in una condizione di forte difficoltà, con la conseguenza, in molti casi, di comprometterne la sostenibilità economica e persino di determinarne l'uscita dal mercato. A ciò si aggiungono rilevanti questioni etiche, non soltanto perché il processo di scelta e rimozione dei contenuti da parte di sistemi automatizzati risulta opaco, ma anche perché risulta difficile risalire al responsabile della rimozione stessa, dato che non è chiarito se la decisione sia stata presa da un algoritmo o da un operatore umano che non ha esercitato un controllo adeguato[158].

1.4.2.5. "Digital Services Act" (DSA)

Il 27 ottobre 2022 è stato pubblicato nella Gazzetta Ufficiale dell'Unione europea il nuovo Regolamento (UE) 2022/2065, noto come *Digital Services Act* (DSA), che disciplina il mercato unico dei servizi digitali.

Il Regolamento si inserisce in un piano d'azione più ampio finalizzato a ridefinire il ruolo degli operatori nel settore dei servizi digitali. In questo quadro rientra il Regolamento 2022/1925 (c.d. *Digital Market Act*), che si pone l'obiettivo di garantire concorrenza equa nei mercati digitali. In questo quadro si inserisce anche il Regolamento sull'intelligenza artificiale, concepito per assicurare che lo sviluppo e l'impiego si sistemi di IA avvengano in maniera etica e responsabile[159].

---

[158] In argomento FERRARIO, *Gli algoritmi come decisori nel contrasto al terrorismo* online. *Alcune riflessioni a partire dal Regolamento (UE) 2021/784*, in *DPCE Online*, 2025, 2, 634 ss.
[159] V. approfondimento del Consiglio dell'Unione europea, *Regolamento sull'intelligenza artificiale*.

Tutti questi interventi normativi segnano il superamento dell'idea di una Rete completamente neutrale e puntano ad assicurare che la tecnologia sia utilizzata nel rispetto dei diritti fondamentali e del principio di dignità personale.

Per un inquadramento generale, il DSA rafforza gli obblighi di controllo in capo ai *provider*, andando a garantire la legalità delle comunicazioni via *Web*.

Inoltre, il Regolamento (UE) 2022/2065 vuole uniformare la disciplina delle grandi piattaforme digitali, che finora sono state oggetto di diverse normative nei vari Stati membri.

Così facendo, si contribuisce alla creazione di un mercato unico digitale[160]. Non si tratta semplicemente di introdurre nuove fattispecie legate all'ambiente digitale, caratterizzato da tecnologie avanzate e specifiche.

L'obiettivo principale è assicurare il rispetto dei diritti fondamentali attraverso una *governance* adeguata. Ciò implica la costruzione di una struttura istituzionale "a rete", che coinvolga istituzioni nazionali e sovranazionali, e al tempo stesso la necessità di adeguare l'assetto amministrativo e giudiziario degli Stati membri alla realtà transnazionale della comunicazione digitale[161]. Il DSA interviene andando ad aggiornare e ampliare il contenuto delle *Direttiva E-Commerce*. Sebbene la Direttiva abbia posto le basi per il commercio elettronico e fissato le regole essenziali sulla responsabilità degli intermediari, il DSA introduce norme più dettagliate e specifiche, finalizzate a migliorare la gestione dei contenuti, garantire una maggiore trasparenza delle piattaforme e rafforzare la tutela dei diritti degli utenti.

Dunque, pur ponendosi in continuità con la Direttiva e mantenendo i suoi principi fondamentali, il Regolamento fissa nuovi obblighi in settori sensibili, come la disinformazione, la violenza *online*, le pratiche ingannevoli e la pubblicità mirata[162].

---

[160] Sul punto BRASCHI, *Il nuovo Regolamento sui servizi digitali: quale futuro per la responsabilità degli* Internet Service Provider*?*, in *Dir. pen. proc.*, 2023, 3, 367 s.
[161] Cfr. CAGGIANO, *La proposta di* Digital Service Act *per la regolazione dei servizi e delle piattaforme* online *nel diritto dell'Unione europea*, in *AISDUE*, 2021, 1, 4.
[162] V. FOTI, *Regolamentazione digitale: il* Digital Services Act *e le piattaforme* online, in *Altalex*, 2024, 1.

Per quanto riguarda gli obblighi generali applicabili a tutti gli ISP, il DSA prevede una regolamentazione simile a quella già prevista dalla Direttiva 2000/31/CE.

Infatti, sul punto, la normativa ribadisce le condizioni in presenza delle quali si applica l'esonero dalla responsabilità dei *provider*, distinguendo i servizi di *mere conduit*, *caching* e *hosting*, rispetto ai contenuti caricati da terzi.

La novità principale rispetto alla precedente Direttiva riguarda la responsabilità del *provider* nel caso in cui fornisca contenuti o informazioni in modo da far credere all'utente che sia lui stesso a fornirlo, o che l'operatore agisca sotto il suo controllo.

Il Considerando 18 del DSA, però, chiarisce che l'esenzione non si applica quando il fornitore, anziché limitarsi a un ruolo tecnico e automatico, svolge un ruolo attivo che gli consente di conoscere e controllare le informazioni trasmesse dagli utenti[163].

Il DSA amplia l'elenco dei doveri di collaborazione a carico dei *provider* e, al contempo, chiarisce che per questi l'esonero da responsabilità non può escludersi solo perché, di propria iniziativa e con diligenza, svolgono controlli o adottano misure per individuare, identificare o rimuovere contenuti illegali.

In questo senso, il Regolamento si propone di superare interpretazioni che scoraggiano l'adozione di misure per prevenire la diffusione di contenuti illeciti[164]. Il *Digital Services Act* introduce un nuovo quadro giuridico dei servizi digitali, con il fine di rafforzare il mercato unico digitale e assicurare il rispetto dei diritti fondamentali e dei valori dell'Unione europea.

L'importanza di questo intervento si apprezza se si considera che, in sua assenza, ciascun Stato membro potrebbe adottare misure autonome, favorendo così una frammentazione normativa che ostacolerebbe lo sviluppo delle imprese europee e accrescerebbe il potere delle grandi *tech companies*.

---

[163] Sul punto CAGGIANO, *La proposta di* Digital Service Act *per la regolazione dei servizi e delle piattaforme* online *nel diritto dell'Unione europea*, cit., 17.
[164] Cfr. BRASCHI, *Il nuovo Regolamento sui servizi digitali: quale futuro per la responsabilità degli* Internet Service Provider*?*, cit., 370.

Inoltre, senza una regolamentazione comune i cittadini non disporrebbero di tutele uniformi per la salvaguardia dei diritti e delle libertà garantiti dal diritto dell'Unione[165].

1.4.3. La disciplina dell'ordinamento italiano

Per quanto riguarda la normativa nazionale, la legge delega 39/2002, nel recepire la Direttiva 2000/31/CE, si è limitata a riprodurre fedelmente il testo della Direttiva.

In particolare, essa si è limitata a prevedere, nei casi di violazione dei diritti dei privati, l'obbligo di introdurre delle sanzioni «effettive, proporzionate e dissuasive»[166], senza però definire in modo specifico la loro natura.

Questo rispecchia il modello tipico delle direttive europee, che impongono agli Stati membri di adottare delle sanzioni con determinate caratteristiche, lasciandoli però liberi di scegliere se optare per sanzioni penali o sanzioni diverse. Sul tema, non si può negare che il legislatore nazionale abbia posto in essere una tecnica legislativa ottimale.

Infatti, nel conferire la delega al Governo, il Parlamento ha di fatto ignorato le garanzie proprie della riserva di legge, lasciando all'esecutivo una piena discrezionalità nella scelta del tipo e della misura della sanzione. Successivamente, con il D.lgs. 70/2003, il legislatore delegato ha deciso di non introdurre delle sanzioni penali per i *provider*, privilegiando la tutela con strumenti di reazione civile, salvo alcune eccezioni limitate di sanzioni amministrative. Tuttavia, altre tipologie sanzionatorie avrebbero potuto garantire una maggior efficacia[167]. Il *Digital Services Act*, come visto, ha sostituito le disposizioni della *Direttiva E-Commerce*, il quale, ad oggi, detta quindi il regime di responsabilità per i servizi digitali[168].

---

[165] In tal senso RUM, *Le nuove frontiere della normativa sui servizi digitali nel mercato unico europeo: si rafforza la protezione dei diritti fondamentali degli utenti* online *con la garanzia pubblicistica delle* Authorities*. Il* Digital Services Act, in *Dir. amm.*, 2022, 15.
[166] Art. 20, Direttiva 2000/31/CE.
[167] V. PERDONÒ, *Le responsabilità penali collegate all'uso di internet fra comparazione e prospettive di riforma*, cit., 338 s.
[168] Cfr. ROMITO, Digital Services Act *(DSA): cosa prevede e quali sono le implicazioni?*, in *Il QG*, 2023, 1.

Alla luce dell'articolo 49 del DSA, ciascuno Stato membro è tenuto a nominare una o più autorità incaricate di vigilare sui fornitori di servizi e garantire l'applicazione del Regolamento.

Inoltre, ogni Paese deve nominare un *coordinatore dei servizi digitali* che sarà responsabile, a livello nazionale, di tutte le questioni inerenti alla vigilanza e all'applicazione del DSA, a meno che alcuni compiti non siano affidati ad altre autorità competenti.

Al fine di evitare la frammentazione dei compiti, il *coordinatore dei servizi digitali* avrà il compito di garantire un'applicazione efficace e coerente del Regolamento, oltre a coordinare le eventuali altre autorità nazionali coinvolte.

In Italia, l'autorità individuata per il ruolo coordinatore è l'Autorità per le garanzie nelle comunicazioni (AGCOM).

Il *coordinatore dei servizi digitali*, che deve disporre autonomamente di risorse e operare in piena indipendenza da influenze esterne, è investito di poteri d'indagine, esecuzione e sanzione nei confronti dei *provider*.

Inoltre, in via residuale e solo nel caso in cui l'attuazione degli altri poteri non abbia condotto a nessun risultato concreto, è possibile adottare delle misure a carattere "ingiunzionale/inibitorio". Nello specifico, il coordinatore nazionale può: esigere dai *provider* informazioni, effettuare ispezioni nei locali dei fornitori e raccogliere dichiarazioni.

I poteri d'indagine possono anche estendersi a soggetti terzi che operano in ambito commerciale, imprenditoriale, artigianale o professionale e che potrebbero essere a conoscenza di informazioni utili.

Quanto ai poteri di esecuzione, i coordinatori possono accettare gli impegni offerti dai *provider* e renderli vincolanti, ordinare la cessazione delle violazioni tramite autorità giudiziarie e adottare misure provvisorie per prevenire il rischio di un danno grave.

Inoltre, possono imporre sanzioni pecuniarie per l'inosservanza del Regolamento, nonché la penalità di mora per garantire l'adempimento delle disposizioni correttive. Le sanzioni, pertanto, non mirano solo a punire le violazioni del DSA, ma servono a garantire il rispetto degli ordini ingiuntivi, come la fornitura di informazioni o la cooperazione nelle indagini.

Nel caso in cui la violazione dovesse persistere e causare un danno grave, è prevista la possibilità di richiedere al giudice delle misure più stringenti, come la restrizione temporanea dell'accesso al servizio. Poiché queste misure incidono sui diritti fondamentali, il coordinatore, prima di disporre una restrizione, è tenuto a invitare le parti interessate, valutare l'impatto della misura e assicurarsi che sia proporzionata. In ogni caso, spetta a ciascuno Stato membro definire le condizioni e le procedure attuative di tali poteri, in conformità con la Carta di Nizza e il diritto dell'Unione europea, ponendo particolare attenzione al rispetto della vita privata e del diritto di difesa[169].

[169] In argomento SABIA, *L'*enforcement *pubblico del* Digital Services Act *tra Stati membri e Commissione europea: implementazione, monitoraggio e sanzioni*, in *MediaLaws*, 2023, 2, 94 ss.

CAPITOLO II

PROFILI PENALISTICI DELLA RESPONSABILITÀ DEL *PROVIDER*

2.1. Diritto europeo e responsabilità del *Provider*

Alla fine del secondo millennio si è affermata l'idea che l'informazione rappresenti un aspetto fondamentale delle economie moderne, soprattutto quando è disponibile tramite la Rete *Internet*.

Questa evoluzione ha spinto il legislatore dell'Unione europea a intervenire regolamentando alcuni aspetti giuridici dei servizi della società dell'informazione nel mercato interno attraverso la Direttiva 2000/31/CE.

Con questa Direttiva l'Unione ha iniziato a definire giuridicamente il contesto in cui avvengono le transazioni giuridiche *online*, individuando i principali soggetti coinvolti. Tra questi ultimi, un ruolo particolare è assunto dagli *Internet Service Provider* (IPS), la cui presenza è essenziale non solo per il funzionamento della Rete, ma anche per garantire l'esistenza della stessa.

Gli ISP non sono tutti uguali e, a causa della loro specificità, non possono essere racchiusi in un'unica definizione. Per questo motivo, la Direttiva all'articolo 2 che è dedicato alle definizioni, ha scelto di non definire esplicitamente gli ISP, ma ha preferito usare il termine più generico "prestatori intermediari"[170] della società dell'informazione.

Solo in un secondo momento, la Direttiva ha operato una distinzione tra le categorie di intermediari più rilevanti in base alla natura del servizio offerto, identificando le tre tipologie principali: gli operatori di *mere conduit*, quelli di *caching* e quelli di *hosting*.

Inoltre, il predetto atto normativo ha regolato i profili di responsabilità di tali categorie di *provider*, stabilendo un trattamento giuridico di *favor* alle tre figure di prestatori, giustificato dalla necessità di creare sistemi efficienti e affidabili per la rimozione di contenuti illeciti e la disabilitazione del loro accesso.

---

[170] Ai sensi dell'art. 2, lett. b) della Direttiva 2000/31/CE si intende «la persona fisica o giuridica che presta un servizio della società dell'informazione».

Questo obiettivo è stato considerato essenziale per la realizzazione di un mercato unico digitale privo di barriere interne[171]. Sul punto, all'articolo 15[172] la Direttiva stabilisce che i *provider* non hanno l'obbligo di monitorare i contenuti che gestiscono, trasmettono o archiviano, né sono tenuti a ricercare attivamente eventuali attività illecite. Tuttavia, qualora dovessero venire a conoscenza di contenuti illeciti, è necessario che informino prontamente le autorità competenti.

Inoltre, se le autorità richiedono di fornire informazioni o la disabilitazione dell'accesso a determinati contenuti sono tenuti a intervenire senza ritardi[173].

Nel tempo, il ruolo dei prestatori di servizio di accesso e di fruizione della Rete si è evoluto in modo significativo, distanziandosi progressivamente dal modello originariamente delineato dalla Direttiva *E-commerce*[174].

In molti casi, hanno persino superato la loro funzione originaria, trasformandosi in veri e propri spazi di creazione di nuovi servizi e modalità di scambio[175].

Nel contesto della strategia dell'Unione europea, per rafforzare il controllo sul settore della digitalizzazione e per ridurre l'influenza degli Stati membri, si colloca la proposta del *Digital Services Act*, presentata il 15 dicembre 2020.

Questo provvedimento nasce dalla consapevolezza che, a vent'anni dall'entrata in vigore della Direttiva sul commercio elettronico, il mercato dei servizi digitali ha subito una profonda trasformazione.

---

[171] Così MASSA, *L'evoluzione della responsabilità degli* Internet Service Provider*: dalla Direttiva E-Commerce al* Digital Services Act, in *Giustizia*, 2022, 2, 42 ss.

[172] Art. 15 Direttiva 2000/31/CE – "Assenza dell'obbligo generale di sorveglianza": «Nella prestazione dei servizi di cui agli articoli 12, 13 e 14, gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.
Gli Stati membri possono stabilire che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati».

[173] Sul punto MARTINELLI, *L'autorità privata del* provider, in SIRENA, ZOPPINI (a cura di), *I poteri privati e il diritto della regolazione. A quarant'anni da «Le autorità private» di C.M. Bianca*, Roma, 2018, 557 s.

[174] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»).

[175] Cfr. COLLETTI, *Il compromesso tra diritto all'oblio e responsabilità dell'*internet service provider *nell'ottica dell'individuazione di rimedi diversi dalla deindicizzazione*, in *Dirittifondamentali.it*, 2024, 1, 341.

L'evoluzione del settore ha dato origine a una crescente diversificazione di servizi, prodotti e fornitori, rendendo il quadro normativo esistente inadeguato a rispondere alle esigenze della realtà attuale.

Nel presentare la proposta del DSA, la Commissione europea ha tenuto in considerazione le tre risoluzioni adottate dal Parlamento europeo nella seduta del 20 ottobre 2020. Queste risoluzioni ribadiscono la necessità di confermare i principi fondamentali della Direttiva sul commercio elettronico, in particolare l'esenzione di responsabilità per i *provider* rispetto ai contenuti *user-generated* e il divieto di sorveglianza e filtraggio preventivo. Inoltre, viene ribadita la necessità di garantire la tutela dei diritti fondamentali nell'ambiente digitale e il mantenimento dell'anonimato *online*, laddove tecnicamente possibile. Parallelamente, il Parlamento europeo richiede ai prestatori di servizi digitali una maggiore trasparenza e il rispetto di obblighi più rigorosi in materia di informazione, delineando un quadro di responsabilità più chiaro e uniforme. Infine, viene proposta l'istituzione di un sistema di vigilanza pubblica a livello nazionale e europeo, unitamente al rafforzamento della cooperazione tra le autorità competenti delle diverse giurisdizioni, soprattutto per affrontare le problematiche di natura transfrontaliera[176].

L'evoluzione dell'approccio regolatorio rispetto alle Direttiva 2000/31/CE emerge chiaramente dalla struttura normativa del DSA, che affianca a un primo livello di disciplina (Capo II) – nel quale mantiene, a determinate condizioni, l'esenzione di responsabilità per i *provider* in relazione alle informazioni trasmesse, memorizzate temporaneamente o ospitate da terzi – un secondo livello (Capo III), caratterizzato da misure differenziate in base ai soggetti coinvolti. Tali misure consistono in obblighi specifici, derivanti da un principio di *due diligence* e in funzione del ruolo e della dimensione del *provider*.

Nello specifico, il Capo III stabilisce una struttura di obblighi, partendo da requisiti applicabili a tutti gli intermediari (Sezione 1), seguiti da disposizioni aggiuntive per i servizi di *hosting* (Sezione 2) e ulteriori prescrizioni per le

[176] V. ALLEGRI, *Il diritto all'oblio e la libertà di informazione nel bilanciamento operato dalla Corte di giustizia*, in *Riv. it. inf. dir.*, 2022, 13 s.

piattaforme *online* (Sezione 3), con requisiti ancora più stringenti per quelle di grandi dimensioni (Sezione 4).

Per evitare oneri eccessivi, le microimprese e le piccole imprese sono esentate dagli obblighi supplementari previsti per le piattaforme *online*, salvo che il loro impatto le qualifichi come piattaforme di grandi dimensioni (Art. 16). Il legislatore europeo mantiene dunque l'esenzione di responsabilità per gli ISP rispetto agli illeciti commessi da terzi, bilanciandola con una maggiore responsabilizzazione. Questo avviene attraverso l'incremento degli obblighi sia nella fase antecedente che successiva alla diffusione di contenuti vietati.

Inoltre, l'esenzione non si limita all'ambito civilistico, ma si estende a livello amministrativo e penale, sollevando i prestatori da responsabilità per gli illeciti commessi dagli utenti[177].

2.2. Ordinamento nazionale e responsabilità del *Provider*

Prima che l'Unione europea intervenisse con una normativa specifica, gli *Internet Service Provider* erano già oggetto di un ampio dibattito giuridico.

In assenza di una legge *ad hoc* e di una presa di posizione esplicita da parte dell'ordinamento europeo, l'Italia – e in generale tutti i Paesi europei – cercava di applicare le regole generali già esistenti del Codice Civile e del Codice Penale, per capire se e a quali condizioni un *provider* potesse essere ritenuto responsabile per i contenuti pubblicati dagli utenti.

La responsabilità civile si configurava nel caso di un comportamento illecito che causasse un danno ingiusto nei confronti di un altro soggetto, con la possibilità di ottenere un risarcimento del danno a determinate condizioni.

La responsabilità penale, invece, si configurava quando l'ISP poneva in essere una condotta particolarmente dannosa, prevista dalla legge come reato.

Nell'ipotesi in cui fosse il *provider* stesso ad aver commesso un illecito, si riteneva applicabile l'art. 2043 c.c., che imponeva una responsabilità per fatto proprio. Inoltre, anche il codice di autoregolamentazione dell'Associazione Italiana

[177] Così PURPURA, *Osservazioni sul* Digital Services Act*: responsabilità e gestione del rischio nella prestazione di servizi intermediari*, in *Comp. dir. civ.*, 2022, 3, 1039 ss.

Internet Provider[178] (AIIP) riconosceva che l'ISP potesse essere ritenuto responsabile per i contenuti diffusi attraverso i suoi servizi.

La questione era divenuta più complessa quando il *provider* non si limitava più a creare contenuti ma cominciava a fornire servizi, come l'accesso alla Rete, la memorizzazione temporanea di dati e la memorizzazione di contenuti di terzi.

I primi commentatori, sul tema, ritenevano evidente come l'attività dell'ISP fosse formalmente separata da quella illecita dell'utente, pur essendo *condicio sine qua non* affinché quest'ultima si realizzasse.

In questo scenario, tra le diverse ipotesi avanzate per delineare una responsabilità del *provider,* quella che inizialmente si era affermata equiparava responsabile editoriale e fornitore, attribuendogli il dovere di controllo dei contenuti immessi in Rete dagli utenti[179].

In assenza di una legge specifica che regolasse il ruolo degli ISP, la giurisprudenza aveva cercato di ricostruirne il regime di responsabilità di questi soggetti applicando - per analogia - l'art. 11 della l. 47/1948 per la responsabilità civile e l'art. 13 della stessa legge per la responsabilità penale, il tutto supportato inoltre dall'art. 30 della l. 223/1990, relativo alle trasmissioni televisive e radiofoniche.

Questa interpretazione portava a richiedere al *provider* un dovere di vigilanza sui contenuti caricati dagli utenti e diffusi mediante i suoi servizi, altrimenti sarebbe potuto incorrere in una corresponsabilità per eventuali illeciti commessi da terzi.

Sebbene questa impostazione giurisprudenziale[180] che imputava - di fatto - ai *provider* una forma di responsabilità oggettiva si è affermata per lungo tempo, la stessa è stata oggetto di numerose critiche.

---

[178] L'Associazione Italiana Internet Provider (AIIP), fondata nel 1995, si pone l'obiettivo di tutelare gli interessi e garantire i diritti di utenti e operatori. L'associazione riunisce i più rilevanti operatori di medie e piccole dimensioni, attivi soprattutto a livello locale e regionale, capaci di fornire soluzioni di connettività personalizzate anche in aree caratterizzate dal *digital divide*. AIIP permette agli *Internet Service Provider* associati un costante aggiornamento sulle tematiche di settore più rilevanti, assistenza rispetto agli adempimenti normativi, occasioni di confronto tra operatori sulle più interessanti opportunità di *business*, nonché un'adeguata rappresentanza presso le autorità più influenti del settore.

[179] Cfr. BASSINI, *La Cassazione e il simulacro del* provider *attivo:* mala tempora currunt, in *MediaLaws*, 2019, 2, 251.

[180] Cfr. Trib. Napoli, 8 agosto 1997; Trib. Teramo, 11 dicembre 1997.

L'art. 1 della l. 47/1948 era pensato per le sole pubblicazioni cartacee e, quindi, difficilmente adattabile al contesto digitale. Lo stesso valeva per l'applicazione in ambito penale, che risultava penalizzante per i *provider*, trattandosi di un'applicazione in *malam partem*[181].

Alla fine degli anni '90 gli Stati Uniti registravano una forte espansione nel settore del commercio elettronico, tanto che il legislatore statunitense intervenne con l'emanazione del noto *Digital Millennium Copyright Act* (DMCA).

Così l'Unione europea, consapevole del proprio ritardo normativo, prese atto del fatto che era necessario intervenire per non rimanere indietro.

Attraverso la Direttiva 2000/31/CE, recepita dall'ordinamento italiano con il d.lgs. 9 aprile 2003, n. 70[182], si voleva fornire un quadro giuridico comune per le attività economiche svolte *online*, ponendo le basi per un'armonizzazione normativa in un contesto profondamente frammentato dalle differenti legislazioni nazionali[183].

2.2.1 Il Decreto legislativo n. 70/2003

Fino al 2003, l'orientamento giurisprudenziale[184] italiano prevalente tendeva a ricondurre la responsabilità degli ISP all'ambito dell'art. 2043 c.c., ovvero, richiamava per analogia la responsabilità attribuita agli editori fondata sulla *culpa in vigilando*. In entrambi i casi, si finiva per adottare criteri di imputazione della responsabilità che prescindevano dalla colpa effettiva del *provider*, cioè caratterizzati da una natura oggettiva.

Nel 2001 il legislatore europeo, consapevole delle criticità di questa situazione, è intervenuto con la Direttiva 2000/31/CE, recepita in Italia con il D.lgs. 9 aprile 2003, n. 70. Con tale intervento si è proposta una soluzione intermedia tra

[181] Sul punto CAMARELLA, *La responsabilità dell'*Internet Service Provider *alla luce della nuova direttiva sul diritto d'autore nel mercato unico digitale*, in *LawTech*, 2020, 77 ss.
[182] Cfr. § 2.2.1.
[183] Sul punto CAMARELLA, *La responsabilità dell'*Internet Service Provider *alla luce della nuova direttiva sul diritto d'autore nel mercato unico digitale*, cit., 81.
[184] V. Trib. Napoli, 8 agosto 1997; Trib. Teramo, 11 dicembre 1997.

l'esclusione totale della responsabilità del *provider* e l'imposizione di un regime eccessivamente gravoso[185].

Nell'intento di individuare con chiarezza i soggetti cui si applica la normativa, l'art. 2 fornisce alcune definizioni chiave. In particolare, la lett. d) identifica come "destinatario del servizio" colui che, per motivi professionali e non, usufruisce di un servizio della società dell'informazione per accedere o condividere informazioni. La lett. b), invece, definisce "prestatore" la persona fisica o giuridica che offre tale servizio.

Tuttavia, quest'ultima definizione risulta piuttosto generica e non consente di individuare con precisione chi, tra i numerosi attori in *Internet*, possa effettivamente rivestire il ruolo di prestatore. Proprio per questo motivo negli articoli successivi – artt. 14, 15 e 16 – il legislatore distingue tre distinti regimi di responsabilità in base tipo di funzione svolta dal *provider*[186].

Più nello specifico, l'art. 14 del D.lgs. 70/2003 disciplina le attività di semplice trasporto (*mere conduit*), che si limitano alla trasmissione di dati – un esempio è il caso dei fornitori di posta elettronica o di accesso *Internet* – senza alcun intervento sul contenuto trasmesso.

L'art. 15 del medesimo decreto riguarda la memorizzazione intermedia e temporanea delle informazioni (*caching*), esclusivamente finalizzata a rendere più efficiente la trasmissione a successivi destinatari. Infine, l'art. 16 disciplina l'attività di memorizzazione di contenuti forniti dagli utenti tramite servizi come la messa a disposizione di uno *server* per siti o pagine *web* (*hosting*).

A completamento di questo assetto normativo, l'art. 17 del D.lgs. 70/2003 – come si vedrà nel paragrafo 2.6 – esclude per i *provider* un obbligo generale di sorveglianza sui contenuti trasmessi o memorizzati tramite i loro servizi[187].

Pur non essendo espressamente volte a regolare gli aspetti penalistici, le citate norme assumono comunque rilievo, poiché costituiscono il presupposto

---

[185] In argomento PIRAINO, *Spunti per una rilettura della disciplina giuridica degli* Internet Service Provider, in *d/SEAS Working Paper*, 2018, 173 s.

[186] V. PIROZZOLI, *La responsabilità dell'*Internet Service Provider. *Il nuovo orientamento giurisprudenziale nell'ultimo caso Google*, in *AIC*, 2012, 3, 6.

[187] In argomento BRIGANTI, *Commercio elettronico: il Dlgs 70/2003 di attuazione della direttiva europea*, in *Altalex*, 2010, 12.

necessario per affrontare le implicazioni penali connesse al ruolo svolto dagli ISP nell'ambiente digitale[188].

Il D.lgs. 70/2003 non prevede una forma di responsabilità autonoma per i fornitori, ma stabilisce che, salvo quanto previsto dalle regole generali di diritto comune, questi possono essere ritenuti responsabili per gli illeciti commessi dagli utenti solo nel caso in cui non siano rispettate le condizioni esplicitamente indicate nel Decreto.

In altri termini, viene riconosciuta una "responsabilità condizionata" agli ISP in base alla quale gli stessi vanno esenti da responsabilità se non intervengano attivamente sui contenuti trattati.

Dunque, la responsabilità del prestatore viene definita in negativo: egli non può essere chiamato a rispondere degli illeciti commessi dagli utenti, a condizione che vengano rispettati i requisiti stabiliti dal D.lgs. 70/2003[189].

La responsabilità degli intermediari è attualmente disciplinata dal *Digital Services Act* (DSA), regolamento direttamente applicabile nell'ordinamento italiano. Nello specifico, l'art. 89 del Regolamento (UE) 2022/2065 ha abrogato gli artt. 14, 15, 16 e 17 del d.lgs. n. 70 del 2003, relativi alla responsabilità degli ISP. A seguito di tale abrogazione, qualsiasi riferimento normativo a tali articoli deve ora intendersi sostituito con il rinvio alle nuove disposizioni contenute negli

[188] Così COSTA, *La responsabilità dell'*Internet Service Provider *per i reati in materia di diritto d'autore*, in *Giur. pen.* 2022, 2, 14.
[189] V. BRIGANTI, *Commercio elettronico: il Dlgs 70/2003 di attuazione della direttiva europea*, cit., 12 s.

artt.4[190], 5[191], 6[192] e 8[193] del DSA, le quali introducono un assetto regolatorio aggiornato e più organico per i fornitori di servizi digitali[194].

2.2.2. L'obbligo di fornire informazioni generali sui prestatori dei servizi

Uno degli aspetti più critici del commercio elettronico riguarda l'incertezza sull'identità e sull'affidabilità della parte contrattuale, unitamente alla carenza o poca chiarezza delle informazioni relative alle condizioni contrattuali, ai meccanismi di reclamo e alla risoluzione delle controversie.

Proprio per questo, tra le regole comuni auspicate dal legislatore europeo, rivestono un ruolo fondamentale quelle che impongono ai fornitori di servizi *online*

---

[190] L'art. 4, Reg. (UE) 2022/2065 disciplina il regime di responsabilità per i fornitori di servizi di trasmissione e accesso a reti di comunicazione, stabilendo che tali fornitori non sono responsabili per le informazioni trasmesse o rese accessibili, a condizione che: non abbiano originato la trasmissione; non abbiano selezionato il destinatario; e non abbiano modificato i contenuti trasmessi. La norma include anche la memorizzazione automatica, intermedia e transitoria delle informazioni, purché limitata al tempo necessario per la trasmissione. Resta salva, tuttavia, la possibilità per le autorità giudiziarie o amministrative degli Stati membri di ordinare ai prestatori di impedire o porre fine a violazioni di legge.

[191] L'art. 5, Reg. (UE) 2022/2065 stabilisce che un prestatore che si limita a trasmettere informazioni su una rete di comunicazione, non è responsabile per la memorizzazione automatica, intermedia e temporanea di tali dati, purché questa avvenga esclusivamente per rendere più efficiente o sicuro il loro inoltro. Tuttavia, per godere dell'esenzione di responsabilità il prestatore non deve modificare le informazioni, deve attenersi alle condizioni di accesso e alle regole di aggiornamento riconosciute nel settore, non deve ostacolare tecnologie lecite utilizzate per monitorare l'uso delle informazioni, e deve intervenire prontamente per rimuovere o disabilitare l'accesso ai contenuti quando viene a conoscenza della loro rimozione dalla rete o di un ordine da parte di un'autorità competente. Infine, tale esenzione non impedisce alle autorità giudiziarie o amministrative, secondo le leggi nazionali, di ordinare al prestatore di impedire o far cessare una violazione.

[192] L'art. 6, Reg. (UE) 2022/2065 stabilisce che un prestatore che si limita a memorizzare informazioni su richiesta di un utente, non è responsabile per i contenuti memorizzati, a condizione che non sia a conoscenza della loro illegalità. In particolare, il prestatore non deve essere consapevole né delle attività né dei contenuti illeciti, né di fatti che rendano evidente la loro natura illegale. Tuttavia, se viene a conoscenza di tali contenuti o attività, è tenuto ad agire immediatamente per rimuoverli o per disabilitarne l'accesso. Questa esenzione di responsabilità non si applica nei casi in cui l'utente agisca sotto la direzione o il controllo del prestatore stesso. Inoltre, non vale per le piattaforme online che permettono ai consumatori di concludere contratti a distanza con operatori commerciali, se la presentazione delle informazioni o dell'operazione induce il consumatore medio a credere che il prodotto, il servizio o le informazioni provengano direttamente dalla piattaforma o da soggetti sotto il suo controllo. Infine, indipendentemente da queste condizioni, le autorità giudiziarie o amministrative possono comunque ordinare al prestatore di impedire o far cessare una violazione, secondo quanto previsto dalla normativa nazionale.

[193] Art. 8, Reg. (UE) 2022/2065 – Assenza di obblighi generali di sorveglianza o di accertamento attivo dei fatti «Ai prestatori di servizi intermediari non è imposto alcun obbligo generale di sorveglianza sulle informazioni che tali prestatori trasmettono o memorizzano, né di accertare attivamente fatti o circostanze che indichino la presenza di attività illegali».

[194] Cfr. Servizio Studi – Dipartimento Attività Produttive, *Disposizioni concernenti l'impiego di sistemi di intelligenza artificiale nel settore del commercio elettronico nonché delega al Governo in materia di disciplina delle funzioni di vigilanza* (A.C. 1940), Schede di lettura, 4 novembre 2024.

l'obbligo di rendere accessibili determinate informazioni ai loro interlocutori. Questi obblighi informativi si applicano non solo nei confronti dei consumatori, tipologia sicuramente più delicata, ma anche in via generale a chiunque utilizzi, per finalità professionali o meno, un servizio della società dell'informazione.

Nel d.lgs. 70/2003 gli obblighi informativi imposti ai prestatori di servizi della società dell'informazione si articolano in tre categorie principali. La prima riguarda le informazioni generali obbligatorie che il prestatore deve rendere pubblicamente disponibili (art. 7); la seconda attiene agli obblighi relativi alle comunicazioni commerciali, compresi i messaggi promozionali e quelli non sollecitati (artt. 8 e 9); la terza, infine, concerne le informazioni da fornire in fase precontrattuale quando il contratto è concluso per via elettronica (art. 12).

L'art. 7 del d.lgs. 70/2003, corrispondente all'art. 5 della direttiva 2000/31/CE, impone al prestatore di servizi l'obbligo di rendere accessibili in maniera chiara, diretta e continuativa tutta una serie di informazioni, rivolte sia agli utenti del servizio che alle Autorità competenti[195].

In particolare, la disposizione in parole stabilisce debba fornire le seguenti informazioni: «a) il nome, la denominazione o la ragione sociale; b) il domicilio o la sede legale; c) gli estremi che permettono di contattare rapidamente il prestatore e di comunicare direttamente ed efficacemente con lo stesso, compreso l'indirizzo di posta elettronica; d) il numero di iscrizione al repertorio delle attività economiche, REA, o al registro delle imprese; e) gli elementi di individuazione nonché gli estremi della competente autorità di vigilanza qualora un'attività sia soggetta a concessione, licenza od autorizzazione; f) per quanto riguarda in particolare le professioni regolamentate, come definite dall'art. 2: 1) l'ordine professionale o istituzione analoga, presso cui il prestatore sia iscritto e il numero di iscrizione; 2) il titolo professionale e lo Stato membro in cui è stato rilasciato; 3) il riferimento alle norme professionali e agli eventuali codici di condotta vigenti nello Stato membro di stabilimento e le modalità di consultazione dei medesimi; g) il numero della partita IVA o altro numero di identificazione considerato equivalente nello Stato membro, qualora il prestatore eserciti un'attività soggetta

[195] In argomento ROSSELLO, *Gli obblighi informativi del prestatore di servizi,* in BESSONE (diretto da), *Commercio elettronico*, Torino, 2007, 136 s.

ad imposta; h) l'indicazione in modo chiaro ed inequivocabile dei prezzi e delle tariffe dei diversi servizi della società dell'informazione forniti, evidenziando se comprendono le imposte, i costi di consegna ed altri elementi aggiuntivi da specificare; i) l'indicazione delle attività consentite al consumatore e al destinatario del servizio e gli estremi del contratto qualora un'attività sia soggetta ad autorizzazione o l'oggetto della prestazione sia fornito sulla base di un contratto di licenza d'uso»[196]. Altresì, il secondo comma della stessa disposizione stabilisce che il prestatore debba mantenere costantemente aggiornate le informazioni rese disponibili, in modo da garantirne l'attendibilità e la validità nel tempo[197].

In merito alle modalità di comunicazione delle informazioni richieste, si può ritenere che queste debbano essere pubblicate sul sito *Web* tramite il quale viene erogato il bene o il servizio. Dal punto di vista tecnico, tali informazioni devono essere rese «facilmente accessibili, in modo diretto e permanente»[198].

La "facilità" all'accesso alle informazioni implica che qualsiasi utente medio debba essere in grado di consultarle senza particolari difficoltà.

Per accessibilità "diretta" si intende che tali informazioni debbano essere disponibili nello stesso sito in cui è offerto il bene o il servizio, senza rinvii tramite *link* a siti terzi o riferimenti indiretti.

Quanto all'accessibilità "permanente", infine, essa indica la possibilità per l'utente di trovare le informazioni in maniera continuativa, e non l'immutabilità dei contenuti[199].

Sebbene le informazioni previste dall'art. 7 del Decreto costituiscano una trasposizione fede di quanto stabilito dall'art. 5 della Direttiva, il legislatore italiano ha apportato alcune integrazioni.

Un primo elemento di novità è rappresentato dalla lett. i) dell'art. 7, che introduce un riferimento alla normativa sul diritto d'autore. Questa disposizione si applica ai servizi che implicano la fruizione di contenuti protetti, come file musicali, opere letterarie, immagini o *software*.

---

[196] Art. 7, d.lgs. 70/2003 – "Informazioni generali e obbligatorie".
[197] Cfr. BRIGANTI, *Commercio elettronico: il D.lgs. 70/2003 di attuazione della direttiva europea*, in *Altalex*, 2010, 6.
[198] Art. 7, comma 1, d.lgs. 70/2003.
[199] V. ROSSELLO, *Gli obblighi informativi del prestatore di servizi*, cit., 139.

In questi casi, il prestatore è tenuto a indicare chiaramente le attività consentite all'utente e a fornire gli estremi del contratto, qualora il servizio sia soggetto ad autorizzazione o sia regolato da una licenza d'uso. Questo aspetto assume particolare rilievo per i servizi basati su *software* o *database*, che prevedono contratti specifici anche per le prestazioni connesse.

Un'ulteriore novità è contenuta al n. 3 dell'art. 7, nel quale si prevede che la registrazione di una testata editoriale telematica sia obbligatoria solo il prestatore intenda beneficiare delle agevolazioni previste dalla l. 7 marzo 2001, n. 62[200]. Si tratta dunque di un obbligo condizionato, inserito dal legislatore nazionale a fini specifici di accesso agli incentivi editoriali[201].

Il DSA ha introdotto un rafforzamento e un'estensione degli obblighi informativi già contemplati dalla normativa previgente, contribuendo così ad accrescere gli obblighi di trasparenza e diligenza in continuità rispetto alla disciplina sul commercio elettronico[202].

Tutti i fornitori che rientrano nell'ambito soggettivo del Regolamento sono tenuti a rispettare una serie di obblighi comuni. Tra questi vi è l'obbligo di creare un punto di contatto per le autorità o un rappresentante legale, nell'ipotesi in cui non siano stabiliti nel territorio dell'Unione (artt. 10 e 11 DSA).

Particolarmente rilevante è l'obbligo, imposto ai fornitori di servizi, di indicare le eventuali informazioni sulle restrizioni normative che impattano sui loro servizi, specificando in modo chiaro le misure adottate per la moderazione dei contenuti, al fine di garantire la trasparenza delle proprie condizioni generali d'uso (art. 12 DSA)[203].

2.2.3. Definizione degli ambiti di responsabilità per *internet service providers* ed *hosting service providers*

[200] Legge 7 marzo 2001, n. 62 "*Nuove norme sull'editoria e sui prodotti editoriali e modifiche alla legge 5 agosto 1981, n. 416*" pubblicata nella *Gazzetta Ufficiale* n. 67 del 21 marzo 2001.
[201] Così ROSSELLO, *Gli obblighi informativi del prestatore di servizi*, cit., 139 s.
[202] In tal senso FINOCCHITO, Digital Services Act*, che cambia per le aziende italiane*, in *Agenda Digitale*, 2024, 2 e 4.
[203] In argomento CAGGIANO, *La proposta di* Digital Service Act *per la regolazione dei servizi e delle piattaforme* online *nel diritto dell'Unione europea*, in *Quaderni AISDUE*, 2021, 1, 22.

La Direttiva 2000/31/CE – come si è già avuto modo di vedere – offre una struttura sistematica per la regolamentazione degli ISP, distinguendone le diverse funzioni agli artt. 12, 13 e 14.

In particolare, la normativa europea individua il ruolo di *hosting*, tipico dei *social network*, che consiste nella memorizzazione di contenuti forniti direttamente dagli utenti. Questa funzione si differenzia da quella di altri tipi di *provider* che si limitano a trasmettere dati attraverso delle reti di comunicazione, come avviene nel caso del *mere conduit*, il quale si limita a fornire l'accesso alla Rete[204].

Il *Digital Services Act* (DSA), con l'obiettivo di aggiornare le regole che disciplinano la responsabilità dei fornitori di servizi digitali, introduce una classificazione degli stessi, graduandone gli obblighi e le responsabilità in base al grado di consapevolezza che essi possono avere sui contenuti caricati dagli utenti[205].

Il Regolamento, in particolare, prevede un sistema di obblighi sempre più stringenti – strutturati secondo una logica "a cerchi concentrici" – in base al tipo di attività svolto dagli ISP[206].

Al livello più ampio si colloca la macrocategoria degli *Internet Services Provider*, al cui interno rientrano i fornitori di servizi intermediari, suddivisi nelle tre tipologie di *mere conduit*, *caching* e *hosting*.

Tra i servizi di *hosting* si distingue una categoria più ristretta, quella delle piattaforme digitali, caratterizzate dalla funzione principale di consentire la diffusione di contenuti al pubblico. È proprio questo elemento – la comunicazione pubblica – a costituire il criterio distintivo rispetto agli altri servizi di *hosting*.

A un livello ancora più specifico si collocano le piattaforme *online* di dimensioni molto grandi – c.d. VLOPs (*Very Large Online Platforms*) – che, per

---

[204] Così NOVELLI, *Il social giudizioso. La giurisprudenza italiana sulla responsabilità civile degli* Internet Service Providers, in *RIID*, 2019, 1, 99 s.
[205] Sul punto RUOTOLO, *Le proposte europee di riforma della responsabilità dei fornitori di servizi su* Internet, in *RIID*, 2022, 1, 19.
[206] Sul punto MORGESE *Proposta di* Digital Services Act *e rimozione dei contenuti illegali* online, in CAGGIANO, CONTALDI, MANZINI (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2021, 47.

numero di utenti e impatto potenziale, sono soggette a obblighi normativi più stringenti[207].

Pur introducendo una revisione del regime di responsabilità dei fornitori di servizi, il DSA conferma i principi fondamentali del quadro normativo previgente. Infatti, gli artt. 4, 5, 6 e 8 del Regolamento riprendono, in larga parte, il contenuto degli artt. 12, 13, 14 e 15 della direttiva sul commercio elettronico.

Sul piano della responsabilità, gli intermediari continuano a beneficiare di un'esenzione dalla responsabilità per i contenuti generati dagli utenti, salvo nei casi in cui siano effettivamente a conoscenza della loro natura illecita e non intervengano per rimuoverli, come previsto dall'art. 6 DSA[208].

Inoltre, ai sensi dell'art. 8 DSA[209], continua a non essere previsto alcun obbligo generale di sorveglianza preventiva sui contenuti trasmessi dagli utenti[210].

La Sezione 1 del Capo III del DSA contiene le norme che si applicano in modo uniforme a tutti gli ISP, stabilendo, nello specifico, che essi sono tenuti a istituire punti di contatto dedicati per agevolare la comunicazione con gli utenti e con le autorità nazionali ed europee; qualora non siano stabiliti nell'Unione, designare un rappresentante legale in uno degli Stati membri; redigere e rendere accessibili le condizioni d'uso del servizio; pubblicare ogni anno un rapporto di trasparenza sulle attività svolte[211].

---

[207] V. VICINANZA, *La responsabilità delle piattaforme digitali nei confronti dei contenuti illegali: dal caso Telegram al Digital Services Act*, in *Quaderni AISDUE*, 2025, 1, 3 s.

[208] L'art. 6, Reg. (UE) 2022/2065 stabilisce che un prestatore che si limita a memorizzare informazioni su richiesta di un utente, non è responsabile per i contenuti memorizzati, a condizione che non sia a conoscenza della loro illegalità. In particolare, il prestatore non deve essere consapevole né delle attività né dei contenuti illeciti, né di fatti che rendano evidente la loro natura illegale. Tuttavia, se viene a conoscenza di tali contenuti o attività, è tenuto ad agire immediatamente per rimuoverli o per disabilitarne l'accesso. Questa esenzione di responsabilità non si applica nei casi in cui l'utente agisca sotto la direzione o il controllo del prestatore stesso. Inoltre, non vale per le piattaforme online che permettono ai consumatori di concludere contratti a distanza con operatori commerciali, se la presentazione delle informazioni o dell'operazione induce il consumatore medio a credere che il prodotto, il servizio o le informazioni provengano direttamente dalla piattaforma o da soggetti sotto il suo controllo. Infine, indipendentemente da queste condizioni, le autorità giudiziarie o amministrative possono comunque ordinare al prestatore di impedire o far cessare una violazione, secondo quanto previsto dalla normativa nazionale.

[209] Art. 8, Reg. (UE) 2022/2065 – Assenza di obblighi generali di sorveglianza o di accertamento attivo dei fatti: «Ai prestatori di servizi intermediari non è imposto alcun obbligo generale di sorveglianza sulle informazioni che tali prestatori trasmettono o memorizzano, né di accertare attivamente fatti o circostanze che indichino la presenza di attività illegali».

[210] V. VICINANZA, *La responsabilità delle piattaforme*, cit., 10.

[211] "*Disposizioni applicabili a tutti i prestatori di servizi intermediari*", Capo III, Sezione 1 Regolamento (UE) 2022/2065.

Oltre a questi obblighi generali, le norme successive – artt. 16 e 18 – introducono obblighi specifici per i fornitori di servizi di *hosting*.

L'art. 16 DSA prevede che i fornitori devono implementare un sistema di segnalazione dei contenuti illeciti, noto come *notice and take down*, che consenta agli utenti di notificare la presenza di contenuti illegali. Se tali segnalazioni sono presentate in modo corretto, si presume che il *provider* sia a conoscenza dell'illegalità del contenuto, con la conseguente perdita della sua esenzione da responsabilità.

L'articolo 18, invece, stabilisce che, nel caso in cui il prestatore venga a conoscenza di informazioni che facciano sospettare la commissione di un reato, è tenuto a informare tempestivamente le autorità competenti dello Stato membro interessato, fornendo tutte le informazioni rilevanti in suo possesso.

Nel complesso, queste disposizioni mostrano come, sebbene il principio di non responsabilità per i contenuti generati da terzi venga formalmente confermato, il suo ambito di applicazione risulti progressivamente più limitato[212].

2.3. La responsabilità del '*Internet Service Provider*' per contenuti illeciti

Negli ultimi decenni, con la costante espansione di *Internet* e il suo utilizzo sempre più diffuso, una delle questioni principali emerse in ambito penalistico riguarda la possibilità di configurare una responsabilità penale in capo agli *Internet Service Provider* per la diffusione di contenuti illeciti pubblicati da terzi.

Infatti, quotidianamente si verificano *online* numerose condotte penalmente rilevanti, nell'ambito di contesti come *social network*, forum, piattaforme dedicate o siti Web interattivi, offerti da soggetti la cui attività principale è proprio quella di creare e gestire spazi virtuali. In tale contesto, dottrina e giurisprudenza si sono interrogate sull'eventuale sussistenza di una responsabilità in capo a tali soggetti, tenuto conto del concreto contributo da essi prestato nella diffusione di contenuti illeciti.

Originariamente nati per offrire accesso alle principali reti di comunicazione e per consentire una diffusione passiva dei contenuti, i *provider* hanno progressivamente assunto un ruolo sempre più attivo, abbandonando la posizione di intermediari neutri per iniziare a intervenire direttamente sui contenuti pubblicati

[212] Cfr. VICINANZA, *La responsabilità delle piattaforme*, cit., 12.

dagli utenti, allo scopo di aumentare la visibilità e amplificare la diffusione. Questo cambiamento di funzione ha comportato inevitabilmente un'evoluzione sul piano della responsabilità.

Dunque, è diventato imprescindibile domandarsi se sussista un obbligo per gli ISP di esercitare un controllo sui contenuti pubblicati dagli utenti e a che titolo possano essere ritenuti responsabili nell'ipotesi in cui abbiano concretamente contribuito alla diffusione dei contenuti illeciti[213].

In quest'ottica si inserisce, ad esempio, il Codice di condotta per il contrasto all'illecito incitamento all'odio *online*, promosso dalla Commissione il 31 maggio 2016, in attuazione alla decisione quadro 2008/913/GAI[214] e dell'art. 16 della Direttiva *E-commerce*. Questa iniziativa è stata sottoscritta dai principali fornitori privati di servizi *online*, tra cui Google, Instagram, Snapchat, Facebook, Twitter, Microsoft e YouTube.

Il Codice, nello specifico, prevede che le aziende firmatarie si impegnino a mettere in atto procedure chiare ed efficaci per un rapido esame delle segnalazioni di discorsi d'odio, così da poter garantire la rimozione tempestiva dei contenuti illeciti.

Inoltre, le imprese si impegnano ad adottare linee guida che vietino la promozione o l'istigazione alla violenza e all'odio, e ad esaminare le richieste di rimozione in conformità sia con tali linee guida sia con la normativa nazionale di recepimento della sopracitata decisione quadro.

Questa procedura deve avvenire tramite specifici gruppi di lavoro e deve essere completata entro 24 ore dalla conoscenza dell'illecito[215].

Infatti, l'intervento dell'Unione europea per contrastare la diffusione di contenuti illeciti *online* è il risultato di un percorso avviato già da tempo, articolato in misure legislative, non legislative e volontarie sia di carattere generale – cioè applicabili a tutti i contenuti illeciti – che di carattere speciale – pensate per determinate categorie di contenuti.

---

[213] Così BACCIN, *Responsabilità penale dell'*internet service provider *e concorso degli algoritmi negli illeciti* online*: Il caso* Force v. Facebook, in *Sist. pen.*, 2020, 5, 75 s.
[214] Decisione quadro 2008/913/GAI, del Consiglio, del 28 novembre 2008, sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale.
[215] Cfr. RUOTOLO, *Le proposte europee di riforma della responsabilità dei fornitori*, cit. 18.

Il quadro generale dettato dalla direttiva 2000/31/CE adotta un approccio particolarmente favorevole per gli ISP. La normativa europea, infatti, non impone specifici obblighi, ma si limita a prevedere un onere di rimozione o disabilitazione dei contenuti illeciti *online*. Solo adempiendo a tale onere, i prestatori possono avvalersi dell'esenzione da responsabilità per le attività compiute dagli utenti.

Questa specifica questione riguarda in particolare gli *hosting provider*, i quali – secondo l'art. 14 della Direttiva *E-Commerce* – possono beneficiare dell'esonero da responsabilità solo se non sono a conoscenza delle attività o di contenuti illeciti, e, nel momento in cui ne vengano a conoscenza, devono intervenire immediatamente per rimuoverli o renderli inaccessibili.

Inoltre, l'art. 15, par. 1 della stessa direttiva vieta agli Stati membri di imporre obblighi generali di sorveglianza sui contenuti ospitati o di accertare attivamente fatti o attività illecite.

L'impostazione della Direttiva ha permesso, nel tempo, di tutelare sia la libertà di manifestazione del pensiero in Rete che la libertà di iniziativa economica dei *provider*.

Negli ultimi anni, l'avvento del *Web 2.0* e la nascita di nuovi servizi di *hosting* hanno rivelato l'inadeguatezza della direttiva 2000/31/CE rispetto ai cambiamenti avvenuti nel contesto digitale. La Direttiva, infatti, non chiarisce gli aspetti sostanziali e procedurali relativi alla rimozione o alla disabilitazione. Questa lacuna ha così determinato una disciplina frammentata a livello nazionale, con delle notevoli differenze tra gli ordinamenti degli Stati membri. Di conseguenza, risulta difficile superare l'approccio favorevole fondato sull'intervento *ex post* sui soli contenuti illeciti espressamente segnalati.

Un ulteriore limite della regola dell'esonera dalla responsabilità ai sensi dell'art. 14 della Direttiva ha demandato agli *hosting provider* la definizione di regole sulla moderazione dei contenuti, rinviando alle *community rules* da loro stabilite.

Inoltre, la Direttiva ha scoraggiato l'adozione di iniziative proattive nella gestione dei contenuti illeciti, temendo che interventi volontari possano far venir meno la qualifica di intermediari passivi.

Un ulteriore limite della Direttiva *E-Commerce* consiste nella mancata previsione di obblighi di trasparenza e diligenza a carico dei prestatori nei confronti dei destinatari di servizi. Infine, la normativa non riconosce poteri di supervisione e controllo delle autorità nazionali e internazionali in merito alla correttezza delle attività svolte da tali operatori.

Per colmare le lacune emerse si è inizialmente intervenuti attraverso strumenti di natura non vincolante.

Ed infatti, nel 2018, è stata adottata dalla Commissione la Raccomandazione 2018/334[216], volta a rafforzare le misure contro la diffusione di contenuti illegali *online*. Pur non essendo un atto vincolante, questa Raccomandazione, non mette in discussione il principio del divieto di imporre obblighi generali di sorveglianza o accertamento attivo. Tuttavia, sollecita i prestatori ad adottare ulteriori iniziative per prevenire e contrastare tutte le tipologie di contenuti illeciti presenti in Rete[217].

Una delle questioni più delicate affrontate dal DSA riguarda l'elaborazione di disposizioni efficaci volte alla rimozione dei contenuti illegali generati dagli utenti *online*. Ai sensi dell'art. 3, lett. h) del Regolamento i contenuti illegali vengono definiti come «qualsiasi informazione che, di per sé o in relazione a un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme al diritto dell'Unione o di qualunque Stato membro conforme con il diritto dell'Unione, indipendentemente dalla natura o dall'oggetto specifico di tale diritto»[218].

La sezione 2 del Capo III introduce ulteriori obblighi in capo ai fornitori di servizi di memorizzazione delle informazioni.

Nello specifico, l'art. 16 del DSA richiede la predisposizione di meccanismi adeguati che permettano ai soggetti terzi di segnalare contenuti potenzialmente illeciti e prevedano una risposta a tali segnalazioni.

L'art. 17 del Regolamento (UE) 2065/2022, invece, impone al prestatore l'obbligo di motivare in modo chiaro ogni decisione di rimozione dei contenuti. L'art. 18, conclusivo della sezione, è intitolato «notifica di sospetti di reati» e

[216] Raccomandazione (UE) 2018/334 della Commissione del 1° marzo 2018 sulle misure per contrastare efficacemente i contenuti illegali online.
[217] Cfr. MORGESE, *Proposta di* Digital Services Act, cit., 32 ss.
[218] Articolo 3, lett. h), Reg. 2022/2065.

stabilisce che, qualora un fornitore di servizi di memorizzazione venga a conoscenza di elementi che facciano presumere la commissione — presente, passata o incombente — di un reato che rappresenti una minaccia per la vita o la sicurezza di una o più persone, è obbligato a informare tempestivamente le autorità giudiziarie o di contrasto dello Stato interessato[219].

2.3.1 Le possibili forme di responsabilità

Gli *Internet Service Provider* assumono un ruolo chiave nell'attuale ordinamento giuridico, sia dal punto di vista economico – poiché agevolano la maggior parte delle attività imprenditoriali *online* – sia dal punto di vista sociale e culturale, garantendo l'accesso all'informazione.

Tuttavia, vi sono delle preoccupazioni riguardanti il fatto che molti illeciti telematici avvengono proprio in virtù dei servizi offerti da questi intermediari. Di conseguenza, si discute sulla necessità di coinvolgerli nella responsabilità, o almeno nei processi di prevenzione e rimozione, per tali illeciti[220].

Mentre sul piano civile sono emerse alcune risposte parziali, in ambito penale la situazione è diversa.

Infatti, il principale orientamento[221] tende a escludere la responsabilità dei *provider*, e rimangono diversi interrogativi sul modello di responsabilità più adeguato da applicare.

La dottrina italiana[222], basandosi sul D.lgs. 70/2003, che recepisce la Direttiva *E-Commerce*, ha individuato tre modelli principali di responsabilità. Il primo si configura come una responsabilità a titolo di concorso commissivo tra l'ISP e l'autore del contenuto illecito. Il secondo paradigma, invece, si fonda sulla responsabilità da reato omissivo improprio, derivante dal mancato impedimento del

---

[219] In argomento ANRÒ, Online hate speech*: la prospettiva dell'unione europea. Tra regolamentazione della condotta dei prestatori di Servizi intermediari e ricorso al diritto penale*, in *Osservatorio sulle fonti*, 2023, 1, 28.

[220] Cfr. DE GIOIA, *La responsabilità degli* internet service providers *in caso di pratiche commerciali scorrette*, in *NJUS*, 2021, 1.

[221] V. Cass. pen., Sez. III, 17 dicembre 2013, n. 5107.

[222] In tal senso SPAGNOLETTI, *La responsabilità del* provider *per i contenuti illeciti di* Internet, in *Giur. mer.*, 2004; INGRASSIA, *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine*, in LUPÁRIA (a cura di), Internet Provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012.

reato altrui secondo l'articolo 40, comma 2 del codice penale. Infine, il terzo modello riguarda la mancata sorveglianza adeguata sulla condotta degli utenti e la mancata attuazione delle misure necessarie per contenere le conseguenze del reato, seguendo il modello del reato omissivo proprio[223].

Ciascun modello idealtipico di imputazione penale applicabile agli ISP implica un diverso ruolo sociale attribuito al prestatore di servizi e un differente bilanciamento dei diritti fondamentali in conflitto.

Il primo paradigma, che mira a tutelare al massimo la libertà di comunicazione ed espressione del pensiero nel contesto digitale, equipara l'ISP agli altri utenti della Rete.

In questa prospettiva, il prestatore non è gravato da doveri di controllo su comportamenti altrui, né da doveri di denuncia di reati di cui viene a conoscenza o obblighi di collaborazione con le autorità nella repressione di illeciti.

Ciò implica, sul piano penalistico una responsabilità limitata ai casi in cui sia direttamente autore o concorrente doloso nella commissione di un reato. In questo scenario, dunque, il ruolo sociale dell'ISP è equiparabile a quello di un comune cittadino nel ciberspazio.

In netta contrapposizione al primo modello, il secondo pone l'accento sulla tutela dei soggetti terzi e della collettività. Si caratterizza per l'introduzione di forti limitazioni della libertà di comunicazione degli utenti, attuata tramite un controllo preventivo dei contenuti da parte dell'ISP.

Il paradigma di responsabilità che ne deriva è quello de reato omissivo improprio: al *provider* si rimprovera di non aver impedito la commissione di un reato altrui. Ne deriva un ruolo sociale dell'ISP assimilabile a quello di un controllore, incaricato di decidere quali contenuti possano o meno trovare spazio nel contesto digitale.

Il terzo paradigma idealtipico si pone a metà rispetto ai precedenti, cercando un equilibrio tra la libertà di manifestazione del pensiero degli utenti e la tutela di terzi e della collettività. Secondo questo modello, la libertà di comunicazione viene parzialmente limitata, ad esempio attraverso la riduzione o l'esclusione dell'anonimato degli utenti.

---

[223] In tal senso BACCIN, *Responsabilità penale dell'*internet service provider, cit., 76 s.

Le strategie di contrasto ai reati prevedono il coinvolgimento dell'ISP solo in una fase successiva alla loro commissione. Nello specifico, il *provider* ha l'obbligo di denunciare gli illeciti di cui venga a conoscenza, collaborare all'identificazione degli autori e provvedere alla rimozione dei contenuti illeciti dal Web. Dunque, l'ISP non è imposto un controllo preventivo sui contenuti, ma è chiamato ad attivarsi per contenere le conseguenze degli illeciti e ad agevolare l'individuazione degli autori.

Questo modello si basa sulla responsabilità del reato omissivo proprio, con un rimprovero per non aver tenuto le condotte volte a garantire l'effettività della risposta sanzionatoria. In tale assetto, il ruolo dell'ISP si configura come quello di tutore dell'ordine nell'ambiente digitale.

Il grado di responsabilità attribuito al *provider* varia progressivamente a seconda del paradigma considerato.

Nell'ipotesi di ISP cittadino, questo risponde unicamente per i reati che ha commesso personalmente o a cui ha partecipato attivamente, senza essere soggetto a obblighi di controllo o collaborazione, la cui violazione comporta responsabilità penale.

Nel modello dell'ISP tutore dell'ordine, egli può essere ritenuto penalmente responsabile, oltre che per le condotte commissive e di concorso, qualora ometta di collaborare con le autorità nelle forme precedentemente indicate.

Infine, l'ISP controllore risponde non solo per eventuali condotte proprie, ma anche per omissioni rilevanti nel caso in cui non abbia impedito reati commessi dagli utenti su cui ha specifici doveri di controllo. Inoltre, è responsabile anche se, dopo che il reato è consumato, non ha contribuito alla repressione dell'illecito collaborando con le autorità[224].

2.3.1.1 Responsabilità omissiva

La responsabilità del *provider* per un reato commesso *online* può essere valutata considerando due momenti separati: il primo implica un comportamento in cui l'ISP partecipa attivamente all'evento illecito; il secondo momento, invece,

[224] V. INGRASSIA, *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine*, in LUPÁRIA (a cura di), Internet Provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012, 5 ss.

implica situazioni in cui all'ISP si può imputare un'omissione, ossia il fatto di non aver controllato o di non aver impedito la circolazione di materiali illeciti attraverso le proprie strutture di rete.

A seconda che si ponga l'accento su un intervento diretto e attivo oppure su una condotta omissiva, il *provider* potrà essere ritenuto penalmente responsabile a titolo d'azione – come autore o coautore del reato[225]– o per omissione, per non aver interrotto o impedito la condotta illecita[226].

Il delicato bilanciamento tra la tutela della libertà di espressione e la necessità di controllo costituisce una questione dibattuta e di lunga durata. Dal punto di vista del diritto penale, questa tensione si traduce nell'opportunità di considerare il fornitore di servizi come titolare di una posizione di garanzia – cioè, tenuto a impedire la commissione di reati all'interno della propria piattaforma, ai sensi dell'art. 40, comma 2, c.p. – oppure come soggetto unicamente tenuto ad attivarsi solo successivamente la realizzazione di un illecito[227].

In via preliminare, è necessario fare una differenza tra due diverse situazioni.

L'omissione da parte del prestatore di servizi può consistere, da un lato, nel mancato esercizio di un controllo preventivo sul contenuto illecito caricato o diffuso da un utente sulla piattaforma; dall'altro nell'omessa rimozione di tale contenuto reso accessibile al pubblico sul sito *Web*.

Da questa distinzione si delineano, dunque, due forme di responsabilità: una di tipo *ex ante*, che si riferisce alla fase precedente alla messa in Rete dei dati, e una di tipo *ex post*, relativa alla permanenza del contenuto illecito *online* e alla mancata eliminazione dello stesso da parte del *provider*.

La prima forma di responsabilità viene esclusa sia dalla giurisprudenza prevalente[228] che dalla maggior parte della dottrina.

---

[225] Sul tema v. infra § 2.3.1.2. e § 2.3.1.3.

[226] V. FUMAGALLI, *La responsabilità penale del* provider, in *Salvis Juribus*, 2020, 2.

[227] In tal senso D'AGOSTINO, *Disinformazione e responsabilità delle piattaforme. Obblighi di attivazione e misure di compliance*, in *DPC.*, 2021, 4, 287.

[228] Corte di giustizia europea, sentenza del 24 novembre 2011, C-70/10, Scarlet Extended, EU:C:2011:771; sentenza del 16 febbraio 2012, C-360/10, SABAM, EU:C:2012:85; Corte europea dei diritti dell'uomo, 9 marzo 2017, Pihl c. Svezia. Nella giurisprudenza nazionale basti richiamare il noto caso Google c. ViviDown, Cass. Pen., Sez. III, 17 dicembre 2013, n. 5107, in *Dir. fam.*, 2014, 2, 675 ss.

Infatti, è stato sottolineato come non esiste *de jure condito* alcuna fonte giuridica che imponga agli intermediari l'obbligo di prevenire la commissione[229].

Tuttavia, si è sollevato un dubbio circa la legittimità di attribuire una posizione di garanzia in capo all'ISP, richiedendo una riflessione sugli elementi costitutivi di tale figura per verificare se essa possa sussistere in capo al *provider*.

Anzitutto, l'espressione "posizione di garanzia" individua l'obbligo giuridico – in capo a un determinato soggetto – di impedire il verificarsi di un evento dannoso che fonda la responsabilità penale. Secondo un'importante pronuncia[230] tale posizione si fonda sulla vicinanza tra il soggetto e il bene giuridico da tutelare, da cui deriva l'attribuzione di specifici poteri e obblighi giuridici, finalizzati a impedire che quel bene venga leso o messo in pericolo. Inoltre, affinché possa configurarsi una posizione di garanzia è necessario che, in primo luogo, vi sia un bene giuridico bisognoso di tutela; in secondo luogo, è necessaria una fonte giuridica che abbia la finalità di proteggere tale bene.

A ciò si deve aggiungere che tale obbligo sia attribuito a uno o più soggetti specificatamente individuabili, e che tali soggetti siano in grado di prevenire la lesione del bene in questione.

È altresì necessario che via sia una connessione tra l'evento dannoso concretamente realizzatosi e l'obbligo di protezione che mirava a evitare.

Infine, il soggetto che si assume essere garante non deve aver concorso attivamente alla produzione dell'evento, altrimenti verrebbe meno il presupposto dell'omissione quale fondamento della sua responsabilità.

Partendo da questo assunto, si è ritenuto che non sia possibile attribuire al *provider* una posizione di garanzia fondata sull'obbligo di impedire la diffusione di contenuti diffamatori. Questo perché, da un lato, manca una norma che imponga al *provider* un controllo preventivo e sistematico su tutti i dati immessi *online*; dall'altro, non vi sarebbe - anche in concreto - la capacità effettiva di esercitare un controllo efficace sui numerosi video caricati dagli utenti, a causa del volume ingente di dati che transitano su Internet[231].

---

[229] Così PANATTONI, *Gli effetti dell'automazione sui modelli di responsabilità: il caso delle piattaforme* online, in *DPC*, 2019, 2, 40.
[230] Cass., 29 gennaio 2013, n. 18569, in *Dir. e Giust.*, 29.4.2013, con nota di CECCARELLI.
[231] Cfr. GARGANI, *La posizione di garanzia*, in *Giur. it.*, 2016, 214 ss.

Il legislatore, infatti, con l'art. 17 del d.lgs. 70/2003 – confermato dall'art. 8 del DSA[232] – ha stabilito che, in capo all'ISP, non grava alcun obbligo generale di sorveglianza sui contenuti caricati dagli utenti, né l'onere di ricercare autonomamente eventuali fatti o circostanze sintomatici di attività illecite[233].

Secondo una parte della dottrina, l'unico obbligo che può ragionevolmente gravare sul *provider* è quello di intervenire solo successivamente alla pubblicazione di un contenuto illecito. Imputargli, invece, un dovere di prevenzione e controllo attivo su tutti i contenuti equivarrebbe, secondo questa visione, a introdurre forme di censura preventiva che comprometterebbero i principi fondanti della libertà in Rete[234].

L'adozione di sistemi di controllo preventivo, infatti, comporterebbe costi e oneri sproporzionati, tali da compromettere il diritto alla libertà d'impresa riconosciuta agli ISP dall'art. 16 della Carta di Nizza[235], e potrebbe non essere in grado di distingue con precisione i contenuti leciti e illeciti, con il rischio di ledere il diritto fondamentale degli utenti alla libertà di comunicazione e di accesso all'informazione, sancito dall'art. 11 della Carta di Nizza[236].

Pertanto, è evidente che, con riferimento alla responsabilità *ex ante* degli intermediari, sia la giurisprudenza che le normative europee tendono a escluderne la configurabilità[237].

Al contrario, secondo un diverso orientamento interpretativo, la previsione di meccanismo di controllo nel *cyberspace* è ritenuta essenziale per la tutela dei diritti fondamentali degli individui e, indirettamente, per un'effettiva libertà della Rete.

---

[232] Art. 8 Reg. (UE) 2022/2065 – "Assenza di obblighi generali di sorveglianza o di accertamento attivo dei fatti": «Ai prestatori di servizi intermediari non è imposto alcun obbligo generale di sorveglianza sulle informazioni che tali prestatori trasmettono o memorizzano, né di accertare attivamente fatti o circostanze che indichino la presenza di attività illegali».

[233] Così NARDI, *I discorsi d'odio nell'era digitale: quale ruolo per l'*internet service provider*?*, in *DPC*, 2019, 12 ss.

[234] Cfr. D'AGOSTINO, *Disinformazione e responsabilità delle piattaforme*, cit., 287 s.

[235] Carta dei diritti fondamentali dell'Unione europea, art. 16 – "Libertà d'impresa": «È riconosciuta la libertà d'impresa, conformemente al diritto dell'Unione e alle legislazioni e prassi nazionali».

[236] Carta dei diritti fondamentali dell'Unione europea, art. 11 – "Libertà di espressione e d'informazione": «1. Ogni persona ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera.
2. La libertà dei media e il loro pluralismo sono rispettati».

[237] Sul punto PANATTONI, *Gli effetti dell'automazione sui modelli di responsabilità*, cit., 41.

In quest'ottica, è necessario che il legislatore non resti indifferente dinnanzi a minacce così gravi, ma piuttosto predisponga strumenti di prevenzione adeguati.

Il crescente ricorso all'informatica nei settori produttivi, informativi e decisionali evidenzia con sempre maggiore urgenza la necessità di forme strutturate di controllo, nonché l'attribuzione di responsabilità chiare a soggetti deputati all'implementazione di filtri o alla rimozione di contenuti illeciti.

La prima tesi, largamente condivisa da dottrina e giurisprudenza[238], è quella che più riflette l'impostazione seguita dal legislatore nazionale e europeo in materia: questo orientamento ritiene che spetti al legislatore il compito di definire in modo chiaro e puntuale le condizioni che legittimano a limitare le libertà su Internet, per evitare che la garanzia della sicurezza venga usata come strumento generalizzato di censura preventiva[239].

Ed invece, una parte della dottrina[240] esclude l'esistenza di un obbligo per gli ISP di impedire i reati commessi dagli utenti e ritiene che tale obbligo non sussista neppure nella fase successiva alla commissione dell'illecito.

Tuttavia, sul punto è intervenuta la Corte di Cassazione che, in una sentenza del 2019[241], ha stabilito un importante principio: in caso di mancata rimozione dei contenuti illeciti – quando l'illiceità della condotta dell'utente sia manifesta, l'ISP – in particolare l'*hosting provider* – può essere ritenuto responsabile per una propria condotta colpevole, configurandosi così una responsabilità commissiva per omissione, avendo concorso, con la sua inerzia, alla prosecuzione dell'illecito.

Inoltre, una parte minoritaria della dottrina[242] sostiene che già da tempo esistono delle norme extra-penali che impongano agli ISP obblighi specifici in

---

[238] Cfr. INGRASSIA, *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine*, in LUPÁRIA (a cura di), Internet Provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012; CGUE, Corte Giust. UE, 23 marzo 2010, Google France c. Louis Vuitton, C-236/08–C-238/08.

[239] V. D'AGOSTINO, *Disinformazione e responsabilità delle piattaforme*, cit., 287 s.

[240] Cfr. SEMINARA, *La responsabilità penale degli operatori su* internet, in *Dir. inf.*, 1998; MANNA, *Considerazioni sulla responsabilità penale dell'*Internet provider *in tema di pedofilia*, in *Dir. inf.*, 2001; RUGGIERO, *Individuazione nel ciberspazio del soggetto penalmente responsabile e ruolo dell'*internet provider, in *Giur. mer.*, 2001.

[241] Cass. civ. Sez. I, 19 marzo 2019, n. 7708.

[242] V. PICOTTI, *La responsabilità penale dei* service providers *in Italia*, in *Dir. pen. proc.*, 1999, 501; PICOTTI, *La legge contro lo sfruttamento sessuale dei minori e la pedopornografia in* Internet *(L. 6 febbraio 2006, n. 38) (Parte seconda)*", in *Studium Iuris*, 2007, 1196; FLOR, *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di* Internet*. Un'indagine comparata in prospettiva europea ed internazionale*, Padova, 2010; FLOR, Social network *e violazioni penali dei*

materia di diffusione di materiale pedopornografico, in materia di tutela del diritto d'autore e anche dal D.lgs. 70/2003. Queste disposizioni sarebbero idonee, secondo questa interpretazione, a fondare una responsabilità penale per reato omissivo.

Pertanto, prendendo in considerazione le recenti evoluzioni e le nuove normative a livello europeo, che prevedono obblighi giuridici derivanti dal diritto europeo e nazionale, nonché l'affermazione di un dovere di diligenza nell'esercizio delle attività digitali, non sembra più possibile escludere totalmente l'attribuzione, in capo agli intermediari, di obblighi giuridicamente rilevanti ad attivarsi per impedire la commissione di reati[243].

Sul tema, occorre altresì considerare due fonti normative di recente introduzione in base alle quali, ad oggi, sembrano sussistere forme di responsabilità omissiva propria in capo agli ISP, che si affiancano alle discusse ipotesi di responsabilità omissiva *ex* art. 40 co.2 c.p.

In particolare, assumono specifico rilievo l'art. 174-*sexies* della legge sul diritto d'autore (L. 22 aprile 1941, n. 633)[244] e l'art. 7 del d. lgs. 107/2023.

L'art. 174-*sexies* della legge sul diritto d'autore[245] disciplina la tutela del diritto d'autore e dei diritti ad esso connessi. In particolare, il prima comma della norma prevede [246] un vero e proprio obbligo di segnalazione in capo a una vasta categoria di operatori digitali, che sorge nel momento in cui essi vengano a conoscenza di condotte penalmente rilevanti, indipendentemente dal fatto che siano in corso, già realizzate o solo tentate. Le fattispecie di reato per cui grava l'obbligo di segnalazione sono quelle previste dalla stessa normativa in materia di diritto d'autore (L. 22 aprile 1941, n. 633), l'accesso abusivo a sistema informatico o telematico (art. 615-*ter* c.p.) e la frode informatica (art. 640-*ter* c.p.).

---

diritti d'autore. Quali prospettive per la responsabilità del fornitore del servizio?, in *Riv. trim. dir. pen. econ.*, 2012, 3, 647.

[243] Sul punto V. PANATTONI, *Gli effetti dell'automazione sui modelli di responsabilità*, cit., 44 ss.

[244] Introdotto dall' art. 6-ter, comma 1 del D.L. 9 agosto 2024, n. 113 (c.d. "decreto Omnibus"), convertito con modificazioni dalla L. 7 ottobre 2024, n. 143.

[245] L. n. 633 del 1941.

[246] Art. 174-*sexies*, comma 1, l. 633/1941: «I prestatori di servizi di accesso alla rete, i soggetti gestori di motori di ricerca e i fornitori di servizi della società dell'informazione, ivi inclusi i fornitori e gli intermediari di Virtual Private Network (VPN) o comunque di soluzioni tecniche che ostacolano l'identificazione dell'indirizzo IP di origine, gli operatori di content delivery network, i fornitori di servizi di sicurezza internet e di DNS distribuiti, che si pongono tra i visitatori di un sito e gli hosting provider che agiscono come reverse proxy server per siti web […]».

L'obbligo di denuncia sorge solo quando gli intermediari della rete espressamente indicati dalla norma hanno conoscenza piena e certa della commissione degli illeciti; le situazioni di dubbio o sospetto non sono sufficienti a far sorgere l'obbligo di segnalazione in capo agli stessi.

La norma – al comma 2 – prevede ulteriori obblighi nei confronti dei soggetti di cui al comma 1. Nello specifico, se si tratta di soggetti stabiliti nell'Unione europea, questi sono tenuti a designare e notificare all'Autorità per le garanzie nelle comunicazioni (AGCOM) un punto di contatto, così da consentire uno scambio diretto e telematico con l'Autorità stessa per l'attuazione della legge; diversamente, i soggetti non stabiliti nell'Unione europea ma che offrono servizi in Italia devono nominare un rappresentante legale nel territorio nazionale, persona fisica o giuridica, del quale comunicare ad i dati identificativi e di contatto (indirizzo postale ed elettronico). In tal modo, l'Autorità dispone sempre di un referente certo e facilmente raggiungibile, anche nei confronti di operatori esteri, assicurando così l'effettiva applicazione della disciplina anche nei confronti di chi non ha sede nell'Unione.

Infine, il terzo comma dell'art. 174-*sexies* disciplina il regime sanzionatorio applicabile in caso di violazione dei commi precedenti. La norma prevede testualmente che «salvo i casi di concorso nel reato, le omissioni della segnalazione di cui al comma 1 e della comunicazione di cui al comma 2 sono punite con la reclusione fino ad un anno», specificando che trova applicazione anche l'articolo 24 bis del decreto legislativo 8 giugno 2001, n. 231 [247].

Il rinvio all'art. 24-*bis* del d. lgs. 231/2001 rappresenta un profilo critico, poiché la formulazione generica utilizzata («si applica l'art. 24-*bis*»[248]) non permette di individuare con chiarezza quale, tra i numerosi reati elencati nell'art. 24-*bis*, debba essere considerato come presupposto né quale tipo di sanzione – pecuniaria o interdittiva – debba essere applicata, generando così incertezza interpretativa e problemi di legittimità alla luce del principio di tassatività.

[247] Art. 174-*sexies*, comma 3, l. 633/1941.
[248] Art. 174-*sexies*, comma 3, l. 633/1941.

Pertanto, si ritiene necessario un intervento legislativo che chiarisca come debba essere applicata la disciplina del d.lgs. 231/2001 alle nuove ipotesi di reato introdotte, al fine definire in modo preciso i confini operativi alla norma[249].

In questa prospettiva, assume rilevanza anche il d.lgs. 107/2023[250], con cui l'ordinamento italiano ha adeguato la normativa interna al Regolamento (UE) 2021/784 relativo alla diffusione di contenuti terroristici *online*[251].

In particolare, l'art. 7 del decreto introduce un regime sanzionatorio a carico dei prestatori di servizi di *hosting* che non rispettino gli obblighi previsti dal Regolamento.

Nel dettaglio, il prestatore di servizi che viola l'art. 15, par. 1 del Regolamento o che «non avendo lo stabilimento principale nell'Unione europea, omette di designare, per iscritto, una persona fisica o giuridica quale suo rappresentante legale nell'Unione ai fini del ricevimento, dell'attuazione e dell'esecuzione degli ordini di rimozione e delle decisioni emesse dalle autorità competenti, oppure designa un rappresentante legale che non risiede o non è stabilito in uno degli Stati membri in cui il prestatore di servizi di hosting offre i propri servizi, oppure omette di conferire al rappresentante legale i poteri e le risorse necessari per ottemperare agli ordini di esecuzione e per cooperare con le autorità competenti»[252] è punito con l'arresto fino a sei mesi o con l'ammenda da 100.000 a 400.000 euro, salvo che il fatto non costituisca più grave reato.

Inoltre, sono sanzionati con l'arresto fino a sei mesi e con l'ammenda da 100.000 a 400.000 euro sia l'*hosting service provider* che il rappresentante legale designato ai sensi dell'art. 17del Reg. quando «a) omettono di rimuovere i contenuti terroristici entro un'ora dal ricevimento dell'ordine di rimozione o di disabilitare l'accesso ad essi entro il medesimo termine; b) nel caso di cui all'articolo 11, paragrafo 3, del regolamento, forniscono informazioni riguardanti la rimozione o la disabilitazione dell'accesso a contenuti terroristici; c) nel caso di cui all'articolo 14,

---

[249] In argomento PEZZANO, BUONGIORNO, P*rofili di criticità del nuovo art. 174-sexies Legge n. 633/1941 in relazione al D. Lgs. n. 231/2001*, in *Giur. Pen. Web*, 2024, 11.

[250] Decreto Legislativo 24 luglio 2023, n. 107 – Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio, del 29 aprile 2021, relativo al contrasto della diffusione di contenuti terroristici on-line.

[251] Così CISTERNA, *Il contrasto al terrorismo* online *e la tutela delle infrastrutture informatiche*, in *Dir. pen. proc.*, 2023, 11, 1432.

[252] Art. 7 comma 1 lett. b) d.lgs.107/2023.

paragrafo 5, del regolamento, non informano immediatamente della presenza dei contenuti terroristici l'autorità giudiziaria o altra autorità che a quella abbia l'obbligo di riferire»[253].

Il comma 3 stabilisce, invece, che la pena è aggravata se l'omissione di cui al comma 2 lett. a) è sistematica o persistente[254].

Infine, il quarto comma dell'art. 7 stabilisce che, nei casi previsti dal comma 1, se il prestatore di servizi di *hosting* non adempie entro quindici giorni dall'accertamento e dalla contestazione delle violazioni, l'autorità giudiziaria può ordinare la sospensione dell'accesso al dominio Internet, applicando le modalità stabilite dall'art. 321 c.p.p.

2.3.1.2 Responsabilità monosoggettiva autonoma

Nell'ipotesi in cui il *provider* agisca in prima persona, ponendo in essere una condotta penalmente rilevante, si parla di responsabilità monosoggettiva autonoma.

Pur essendo pacifico nell'ordinamento italiano, che l'ISP sia penalmente responsabile per i reati da lui commessi o realizzati in concorso con altri utenti, permangono incertezze riguardo l'esatta delimitazione dei confini di tale responsabilità. In punto d'autoria, le maggiori criticità sono emerse nei casi in cui la giurisprudenza, talvolta ricorrendo a forzature interpretative, ha ampliato o limitato l'ambito di applicazione di alcune fattispecie penali, al fine di includere o escludere la responsabilità degli ISP rispetto a condotte largamente diffuse nel mondo digitale[255].

Al fine di analizzare in modo completo le ipotesi di responsabilità monosoggettiva autonoma del *provider*, è utile richiamare la definizione di reati informatici, che comprende gli illeciti caratterizzati dalla realizzazione diretta del fatto tipico in Rete, oppure, almeno, nella sua immediata connessione con essa[256].

---

[253] Art. 7 comma 2 lett. b) d.lgs. 107/2023.
[254] In argomento CISTERNA, *Il contrasto al terrorismo* online, cit., 1440 s.
[255] In tal senso INGRASSIA, *Il ruolo dell'ISP nel ciberspazio*, cit. 7.
[256] In argomento PICOTTI, *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. eco.*, 2011, 4, 847.

A loro volta, i reati informatici si distinguono in due categorie. Nella prima categoria, quella dei "reati informatici in senso stretto", rientrano generalmente le fattispecie incriminatrici che contengono esplicitamente elementi descrittivi riferiti a modalità, oggetti o condotte caratterizzati dalla tecnologia informatica, cioè che implicano, sono connessi o attinenti a processi di elaborazione automatizzata di dati mediante programmi informatici. Ne sono esempio il reato di "accesso abusivo a sistema informatico o telematico" (art. 615-*ter* c.p.), la "frode informatica" (art. 640-*ter* c.p.) e il "danneggiamento di informazioni, dati e programmi informatici" (art. 635-*bis* c.p.).

Nella seconda categoria, quella dei "reati informatici in senso lato", rientrano quelle fattispecie penali che, pur non contenendo espliciti riferimenti a elementi tecnico-informatici nella loro formulazione, possono essere realizzate anche attraverso l'uso del cyberspazio.

Si tratta, sostanzialmente, di condotte che rappresentano modalità nuove di aggressione a beni giuridici già tutelati da norme incriminatrici generali. Ne sono esempi il reato di diffamazione, quando viene perpetrato tramite la pubblicazione *online* di contenuti lesivi della reputazione altrui; la sostituzione di persona, che si configura quando si utilizzano le generalità di un altro soggetto per creare un falso profilo con l'intento di ingannare; oppure le truffe commesse su *Internet* mediante la diffusione di annunci ingannevoli[257].

Per quanto riguarda i reati cibernetici in senso stretto, non vi sono dubbicirca la possibilità che l'ISP ne risponda in qualità di autore. Anzi, il ruolo del fornitore è rilevante al punto tale da configurare, in alcuni casi, ipotesi aggravate del reato, soprattutto quando egli riveste, come spesso accade, la qualifica di operatore di sistema. Il legislatore ha infatti previsto specifiche circostanze aggravanti per l'operatore del sistema, che incidono sia sull'entità della pena sia sulle condizioni di procedibilità, escludendo, in tali casi, la necessità della querela da parte della persona offesa.

Un esempio emblematico è quello dell'ISP che fornisce un servizio di posta elettronica e che intercetta le e-mail degli utenti, consentendone la lettura ai propri

[257] Cfr. PIETRELLA, *Reati informatici e concorso di norme: come l'evoluzione tecnologica informa il diritto penale. Il caso delle* Botnets, in *Dis. Crimen.*, 2021, 3 s.

dipendenti al fine di profilare gli interessati e inviare loro offerte commerciali mirate. In una simile ipotesi, la qualifica di operatore attribuita all'ISP conferisce al reato di intercettazione illecita di comunicazioni informatiche o telematiche un ulteriore grado di gravità.

La possibilità che i reati cibernetici in senso lato vengano realizzati in forma monosoggettiva dall'ISP dipende strettamente dalla struttura del fatto tipico previsto dalla norma incriminatrice. Ad esempio, è fuori discussione che il *provider* possa essere autore diretto di reati basati sulla diffusione di contenuti illeciti — come materiale pedopornografico o protetto da diritto d'autore — oppure di reati che riguardano l'espressione del pensiero, quali la diffamazione, l'istigazione all'odio razziale o la divulgazione di informazioni riservate o segrete.

Accanto a ipotesi in cui tale configurazione è pacificamente ammessa, esiste un'ampia area di incertezza interpretativa. Questa zona grigia è rappresentata da casi limite (c.d. *hard cases*) in cui l'applicazione delle norme ha dato luogo a soluzioni differenti, riconoscendo o escludendo la responsabilità dell'ISP . Ciò è avvenuto attraverso interpretazioni della norma incriminatrice che si sono rivelate, a seconda dei casi, estensive, restrittive o persino analogiche *in malam partem*, sempre ritagliate su condotte che assumono caratteristiche particolari proprio in ragione del loro svolgimento in Rete[258].

Un esempio emblematico è rappresentato dal delitto di favoreggiamento della prostituzione, disciplinato dall'art. 3, n. 8), della L. 75/1958[259]. Tale norma, data la descrizione poco tipizzata della condotta, è stata applicata dalla giurisprudenza a tutti i gestori di siti *Internet* che favorivano incontri con finalità sessuali.

La Corte ha ricondotto l'attività del titolare del sito *Web* che pubblica annunci per il reperimento di clienti da parte delle *escort* al favoreggiamento della prostituzione previsto dall'art. 3 della Legge Merlin.

---

[258] Cfr. INGRASSIA, *Il ruolo dell'ISP nel ciberspazio*, cit., 8.

[259] L'art. 3, n. 8), della L. 75/1958 punisce «con la reclusione da due a sei anni e con la multa da lire 100.000 a lire 4.000.000, salvo in ogni caso l'applicazione dell'art. 210 del Codice penale: […] chiunque in qualsiasi modo favorisca o sfrutti la prostituzione altrui».

Tuttavia, i giudici di legittimità, facendo riferimento a una distinzione ampiamente accolta in dottrina[260] tra favoreggiamento della prostituzione – penalmente rilevante – e favoreggiamento della persona che si prostituisce – considerato invece penalmente irrilevante – ha costantemente escluso che la semplice pubblicazione di annunci integri un reato. Questa attività viene infatti qualificata come un servizio ordinario reso alla persona che esercita il meretricio, e non come una forma di promozione della prostituzione in sé, a condizione che non sia accompagnata da ulteriori condotte volte a rendere più accattivante l'offerta sessuale, come può essere ad esempio l'organizzazione di servizi fotografici con pose erotiche.

La scelta di escludere quelle condotte dal perimetro della fattispecie penale, che per la stessa definizione fornita dalla giurisprudenza vi rientrerebbero, pare motivata dalla scarsa percezione di disvalore associato alla semplice creazione del sito. La Corte, infatti, paragona tale attività a quella svolta da numerosi quotidiani che pubblicano annunci dello stesso tipo, considerata come un servizio offerto dalla prostituta[261].

Dunque, non vi è alcun dubbio sul fatto che il gestore della piattaforma risponda per i reati da lui stesso commessi, sia in via autonoma sia in concorso con gli altri utenti.

Sul punto, la dottrina si interroga da tempo sulla natura del contributo atipico che l'ISP può fornire alla realizzazione del reato e se la responsabilità a titolo di concorso commissivo – come si vedrà nel paragrafo successivo – debba essere valutata secondo i criteri generali del concorso di persone nel reato, oppure se richieda un inquadramento specifico e autonomo[262].

2.3.1.3 Responsabilità concorsuale

Nell'ambito della responsabilità concorsuale, ciò che si rimprovera al *provider* di aver offerto un contributo causale alla realizzazione di un reato, partecipando, insieme all'utente, alla sua realizzazione.

---

[260] La distinzione risale a VASSALLI, *I delitti previsti nella l. 20 febbraio 1958, n. 75*, in *Argomenti di medicina sociale*, 1963, 32.
[261] V. INGRASSIA, *Il ruolo dell'ISP nel ciberspazio*, cit., 11 s.
[262] Così D'AGOSTINO, *Disinformazione e responsabilità delle piattaforme*, cit., 287.

Com'è noto, in assenza di una disciplina che imponga agli ISP un obbligo di controllo preventivo, si è ipotizzato un possibile coinvolgimento del *provider* negli illeciti commessi dagli utenti facendo riferimento alla responsabilità per concorso, secondo il modello delineato dall'art. 110 c.p.[263]. In tal senso, si è ritenuto che l'ISP potesse offrire un contributo causale o agevolativo, ad esempio, nella predisposizione di un collegamento in Rete o nella messa a disposizione di *software* e strumenti per la condivisione di contenuti[264].

Secondo l'orientamento giurisprudenziale maggioritario[265], affinché un soggetto possa essere ritenuto concorrente in un reato, devono sussistere una serie di requisiti.

Dal punto di vista oggettivo è necessario che il reato sia stato effettivamente commesso — anche solo nella forma del tentativo — da più persone, e che il concorrente abbia fornito un contributo che, pur non essendo indispensabile, abbia comunque agevolato la realizzazione dell'illecito, rendendola meno incerta o difficoltosa.

Sotto il profilo soggettivo, si richiede che il concorrente agisca con dolo, ossia con la consapevolezza della commissione del reato e con la volontà di contribuire alla sua realizzazione attraverso la propria condotta. In questa prospettiva quindi, il contributo fornito dal *provider* viene valutato alla luce delle regole generali sul concorso di persone nel reato.

A questo orientamento, sostenuto dalla dottrina prevalente[266], se ne contrappone un altro secondo il quale l'ISP debba beneficiare di un regime più garantista in tema di responsabilità concorsuale. Secondo tale impostazione, la

---

[263] Art. 110 c.p. – "Pena per coloro che concorrono nel reato": «Quando più persone concorrono nel medesimo reato, ciascuna di esse soggiace alla pena per questo stabilita, salve le disposizioni degli articoli seguenti».

[264] Così FIORINELLI, *L'attuale ruolo del* provider *nella società digitale: modelli di responsabilità penale*, in *Leg. pen.*, 2022, 4, 4.

[265] Cfr.Cass. pen., sez. IV, 22 maggio 2007, n. 24895, in *Guida dir.*, 2007, 111; Cass. pen., sez. un., 30 ottobre 2003, ANDREOTTI, in *Cass. Pen.*, 2004, 811; Cass. pen., Sez. IV, 13 aprile 2004, n. 21082, in *Cass. Pen.*, 2006, 514; Cass. pen., sez. IV, 22 novembre 1994, A.V.C.I., in *C.E.D. Cass.*, n. 201244; Cass. pen., sez. IV, 28 gennaio 1993, MANGANI, ivi, n. 195476.

[266] Cfr. DE NATALE, *Responsabilità penale dell'*internet service provider*, per omesso impedimento e per concorso nel reato di pedopornografia*, in GRASSO, PICOTTI, SICURELLA (a cura di), *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milano, 323 ss.; FLOR, *Tutela penale e autotutela tecnologica, dei diritti d'autore nell'epoca di* internet*. Un'indagine comparata in prospettiva europea ed internazionale, Padova, 2010,* 417 ss.; PETRINI, *La responsabilità penale per i reati via* internet, Napoli, 2004, 147 ss.

responsabilità del *provider* può configurarsi solo a partire dal riconoscimento che la sua attività, di per sé, ha natura neutra e lecita secondo l'ordinamento giuridico.

La qualificazione della condotta come lecita o illecita dipende dunque dalle concrete modalità con cui il servizio viene prestato. In questa prospettiva, la responsabilità concorsuale dell'ISP può essere affermata solo in presenza di un dolo di partecipazione particolarmente marcato e di una reale possibilità, da parte sua, di impedire la commissione del reato[267].

In questo contesto, va osservato come l'elaborazione delle varie possibili forme del concorso del *provider* nei reati commessi *online* è stata fortemente influenzata dall'interpretazione fornita dalla giurisprudenza di legittimità in due noti casi[268].

Il caso *Sky-calcio libero*[269] ha avuto origine dalla richiesta di sequestro di un sito *Web* che permetteva ai propri utenti, grazie alla pubblicazione di *link* a *server* cinesi, di vedere le partite del campionato di calcio italiano, trasmesse in esclusiva da Sky. La trasmissione *online* era effettuata da una televisione cinese, titolare della licenza per la diffusione nel proprio territorio.

La Corte di Cassazione è intervenuta per decidere sul predetto sequestro dopo che sia il Giudice per le indagini preliminari (GIP) sia il Tribunale del riesame avevano rigettato la richiesta della Procura di Milano. Secondo questi giudici, l'art. 171, comma 1, lett. a) *bis* della legge n. 633/1941 punisce esclusivamente l'immissione in un sistema di reti telematiche di un'opera protetta dal diritto d'autore.

Nel caso di specie, i gestori del sito italiano si erano limitati a pubblicizzare la trasmissione già resa disponibile *online* dal sito cinese, senza intervenire direttamente nell'immissione dell'opera protetta in Rete. Pertanto, la condotta dei gestori del sito italiano si collocava in un momento successivo alla consumazione del reato, e di conseguenza, non poteva ritenersi penalmente rilevante.

Il giudice di legittimità ha invece ammesso in astratto la possibilità di un concorso nel reato da parte dei gestori del sito italiano. Secondo la Suprema Corte, gli indagati avevano effettivamente agevolato la diffusione delle partite, fornendo

---

[267] V. INGRASSIA, *Il ruolo dell'ISP nel ciberspazio*, cit., 15 s.
[268] Cfr. FIORINELLI, *L'attuale ruolo del* provider *nella società digitale*, cit., 7.
[269] Cass. Pen., Sez. III, 4 luglio 2006, n. 3394.

agli utenti le informazioni dettagliate su come accedere allo *streaming* per la visione delle partite in Italia. Secondo i giudici, tale attività, ha avuto un impatto causale sulla lesione del bene tutelato, pur non avendo, gli indagati, compiuto l'azione tipica.

Tuttavia, questa interpretazione appare viziata, poiché la Suprema Corte ha in parte frainteso le decisioni di merito. Il problema sollevato dal Tribunale del riesame non era di carattere meramente temporale, ma riguardava le fasi del reato e la descrizione del fatto tipico nella norma incriminatrice. Poiché la norma in questione punisce «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»[270] il reato si consuma nel momento stesso in cui l'opera viene immessa in Rete. di conseguenza, non è possibile configurare un concorso successivo alla commissione del reato.

Anche seguendo la logica della Cassazione, il fatto di informare gli utenti che un'opera verrà messa a disposizione da altri e spiegare le modalità di fruizione non equivale a contribuire alla sua immissione in *Internet*.

Nel caso in oggetto, i gestori del sito italiano non avevano alcun ruolo sulla diffusione online delle partite, in quanto, gli utenti avrebbero potuto accedere al contenuto attraverso il *server* cinese[271].

Al contrario, nel caso *The Pirate Bay*[272] la commissione del reato è strettamente connessa all'esistenza dell'ISP.

Anche in questo secondo caso la Corte di Cassazione è stata chiamata a esprimersi in merito al sequestro di un sito *Web* che permetteva la condivisione tra utenti di opere protette dal diritto d'autore.

Nella sua pronuncia, la Corte ha individuato i requisiti indispensabili affinché la condotta del *provider* possa essere considerata penalmente rilevante quando agevoli la comunicazione tra utenti che commettono l'attività illecita di *uploading*. In particolare, a differenza del primo caso affrontato, qualora la diffusione dell'opera protetta avvenga tramite un protocollo di comunicazione più evoluto, in grado di suddividere l'attività di *uploading* rendendola più efficace e

[270] Art. 171, comma I, lett. a bis), L. 633/1941.
[271] Sul punto INGRASSIA, *Il ruolo dell'ISP nel ciberspazio*, cit., 22 ss.
[272] Cass. Pen., Sez. III, 29 settembre 2009, n. 49437.

veloce, la messa in Rete dell'opera non è più riconducibile a un unico utente, ma ad una pluralità di soggetti, ciascuno dei quali concorre diffondendo una parte del contenuto.

La responsabilità per la diffusione dell'opera, da un punto di vista penalistico, ricade innanzitutto sui singoli utenti, ma l'attività di indicizzazione e tracciamento svolta dal sito, indispensabile per il trasferimento dei contenuti, è imputabile al gestore della piattaforma.

Dunque, nel caso *The Pirate Bay*, l'ISP è coautore dell'illecito, poiché il suo intervento incide direttamente sulle modalità di immissione dell'opera in Rete[273].

A tale orientamento si affianca un indirizzo interpretativo opposto – emerso nella giurisprudenza civile di merito[274] e confermato da una pronuncia della Corte di Cassazione[275] – secondo cui è possibile configurare una responsabilità penale a titolo di concorso omissivo all'*hosting provider* nel reato commesso dall'utente, in ragione dell'obbligo, previsto dall'art. 16 del d.lgs. 70/2003 e confermato dal DSA, di rimuovere i contenuti illeciti non appena venga a conoscenza della loro presenza.

In particolare, la Corte di Cassazione – chiamata a pronunciarsi sulla responsabilità del gestore di un sito *Internet* che aveva ospitato un commento offensivo – ha valorizzato il fatto che il provider, pur essendo a conoscenza del contenuto illecito, lo avesse mantenuto *online*, non adottando le misure necessarie per impedire la persistenza della condotta diffamatoria.

---

[273] Così INGRASSIA, *Il ruolo dell'ISP nel ciberspazio*, cit., 24 s.

[274] Cfr. seppure in ottica civilistica, Trib. Napoli Nord, sez. II, 3 novembre 2016, in *Giur. it.*, 2017, 629 ss., con nota di BOCCHINI, *La responsabilità di* Facebook *per la mancata rimozione dei contenuti illeciti*; in *Resp. civ. prev.*, 2017, 536 ss., con nota di BUGIOLACCHI, *I presupposti dell'obbligo di rimozione dei contenuti da parte dell'*hosting provider *tra interpretazione giurisprudenziale e dettato normativo*, in *Dir. inf.*, 2017, 254 ss., con nota di MONTANARI, *La responsabilità delle piattaforme online (il caso Rosanna Cantone)*; Trib. Torino, 7 aprile 2017, n. 1928, in *www.iusexplorer.it.*; Corte App. Roma, 29 aprile 2017, n. 2883, ivi; Trib. Milano, ord. 8 maggio 2017, sez. impr., ivi; Trib. Roma, 15 febbraio 2019, n. 3512, in *Altalex*.

[275] Cass. pen., sez. V, 27 dicembre 2016, n. 54946, in Foro it., 2017, p. 251 ss., con nota di DI CIOMMO, *Responsabilità dell'*internet hosting provider*, diffamazione a mezzo* Facebook *e principio di tassatività della norma penale: troppa polvere sotto il tappeto*; in Cass. pen., 2017, 2782 ss., con nota di CARBONE, *Responsabilità del Blogger: parziale rivirement della Cassazione?*; in *Giurisprudenza penale web*, 2017, 1, con nota di MIGLIO, *I gestori di un sito internet rispondono penalmente per i commenti offensivi pubblicati dagli utenti*; in *Questione Giustizia* (9 gennaio 2017), con nota di BUFFA, *Responsabilità del gestore del sito internet*. Cfr., altresì, INGRASSIA, *Responsabilità penale degli* internet service provider*: attualità e prospettive*, in *Dir. pen. proc.*, 2017, 1621 ss.

Lo sviluppo di questo orientamento è principalmente dovuto dal fatto che, negli ultimi anni, si è assistito all'emergere di piattaforme *online* che non si limitano più a svolgere funzioni di mera memorizzazione dei dati, ma che affiancano a queste attività più complesse come l'indicizzazione, la categorizzazione e l'organizzazione dei contenuti caricati dagli utenti. Tuttavia, permangono dei dubbi circa la possibilità configurare una responsabilità penale del *provider* secondo lo schema del reato omissivo improprio. Inoltre, la responsabilità per omesso impedimento presuppone che il reato non sia ancora stato consumato. Invece – come si vedrà nel paragrafo successivo – nel caso della diffamazione *online* il reato si perfeziona nel momento in cui il contenuto illecito viene pubblicato.

Pertanto, non è possibile attribuire all'ISP una partecipazione omissiva alla diffamazione per il solo fatto di aver mantenuto online il contenuto o di non averlo rimosso successivamente[276].

2.3.2 Il reato di diffamazione *online*

Il reato di diffamazione è disciplinato dall'art. 595 c.p[277]., il quale tutela la reputazione[278] della persona offesa, intesa come onore e decoro a essa riconosciuti.

Affinché il reato si perfezioni, l'offesa deve essere percepita da una pluralità di persone e in assenza della persona offesa; in alternativa quest'ultima deve venirne a conoscenza in modo indiretto, senza avere la possibilità replicare nell'immediato.

---

[276] In tal senso NARDI, *I discorsi d'odio nell'era digitale*, cit., 16 ss.

[277] Art. 595 c.p. – "Diffamazione": «1. Chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a lire diecimila.
2. Se l'offesa consiste nell'attribuzione di un fatto determinato, la pena è della reclusione fino a due anni, ovvero della multa fino a lire ventimila.
3. Se l'offesa è recata col mezzo della stampa o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico, la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a lire cinquemila.
4. Se l'offesa è recata a un Corpo politico, amministrativo o giudiziario, o ad una sua rappresentanza, o ad una Autorità costituita in collegio, le pene sono aumentate».

[278] Per reputazione si intende il sentimento di stime e dignità personale di cui un individuo gode all'interno del proprio contesto sociale, in base alla considerazione che di lui ha il gruppo di appartenenza. Si rinvia ad ALMA, *Offesa alla reputazione del movimento LGBT e configurabilità del delitto di diffamazione*, in *Sist.pen.*, 2024, 5, 103.

Come evidenziato da una parte della dottrina[279], poiché la diffamazione si basa sulla diffusione di comunicazione offensiva rivolta a più persone, per il suo perfezionamento è necessario che si instauri di un rapporto comunicativo con una pluralità di soggetti terzi, indipendentemente dal fatto che questi percepiscano il contenuto diffamatorio[280].

In particolare, il comma 3 dell'art. 595 c.p., nel descrivere i mezzi attraverso cui può essere commessa la diffamazione aggravata, include anche gli strumenti informatici e digitali, facendo riferimento in modo generico a «qualsiasi altro mezzo di pubblicità»[281].

In questa categoria rientrano, pertanto, secondo la giurisprudenza di legittimità[282], anche i *social media*, riconosciuti come strumenti particolarmente efficaci nella diffusione rapida di opinioni, interpretazioni e contenuti potenzialmente lesivi[283]. Inoltre, la pena prevista per il reato di diffamazione può essere aumentata in presenza di circostanze aggravanti, tra cui, in particolare, quella prevista dal comma 3 dell'articolo 595 c.p., che riguarda i casi in cui l'offesa venga veicolata tramite stampa, pubblicità o un atto pubblico. Poiché tali modalità di diffusione amplificano significativamente la portata del messaggio diffamatorio, la giurisprudenza prevalente[284], considera i social network assimilabili ai mezzi di pubblicità, riconoscendo quindi la sussistenza dell'aggravante quando il contenuto offensivo viene diffuso a una pluralità di destinatari[285].

---

[279] V. PICOTTI, *Profili penali delle comunicazioni illecite via* Internet, in *Dir. inf.*, 1999, 2, 297; TABARELLI DE FATIS, *Prospettive di riforma del delitto di diffamazione, con particolare riferimento alla diffamazione* online, in PICOTTI (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013, 220.

[280] In argomento MARTIN, *Sulla diffamazione e sull'istigazione a delinquere: distinzioni e profili applicativi*, in *Camm.dir.*, 2020, 5.

[281] Art. 595, comma 3, c.p.

[282] Cfr. Cass. Pen., S.U., 17 luglio 2015 (ud. 29 gennaio 2015). n. 31022, in *Giurisprudenza Penale Web*, 2015.

[283] V. TEDESCHI TOSCHI, BERNI FERRETTI, Social media*, profili artificiali e tutela della reputazione. Come l'avvento dei* social bot *per la gestione dei profili* social *possa rappresentare una grave minaccia per la reputazione delle persone e quali potrebbero essere le risposte a tale pericolo*, in *RIID*, 2021, 2, 112.

[284] Cfr. Cass. pen., V sez., n. 7904/19; Cass. pen. sez. V, 13/07/2015, n. 8328; Tribunale Pescara, 05/03/2018, n. 652.

[285] Così LONGO, *Diffamazione via* mass media *e* social network*, tutele e risarcimenti. Requisiti, circostanze aggravanti e principali cause di esclusione del reato alla luce della prevalente giurisprudenza degli ultimi anni*, in *Altalex*, 2020, 3.

Ciò premesso, occorre valutare se l'utilizzo delle tecnologie dell'informazione e della comunicazione (ICT) nella diffusione di contenuti offensivi possa avere delle ricadute sull'evento giuridico previsto dalla fattispecie di cui all'art. 595 c.p.

Nell'ambito delle comunicazioni effettuate tramite piattaforme digitali – come *social network*, *blog* e *forum* – è necessario verificare se l'uso di un linguaggio offensivo sia idoneo a ledere la reputazione dell'utente all'interno dell'ambiente sociale in cui egli vive.

Tuttavia, il pericolo per la reputazione non può essere desunto in modo astratto dalle parole impiegate, ma deve essere valutato in modo concreto, tenendo conto del contesto specifico in cui si manifesta la condotta.

Affinché tale pericolo assuma rilevanza non si può trascurare il fatto che alcuni comportamenti, un tempo considerati denigratori o ingiuriosi, si siano nel tempo "normalizzati" a causa della diffusione di un nuovo registro espressivo e comunicativo, caratterizzato da toni volgari e offensivi, tipico dell'ambiente dei *social network* e delle ICT.

Normalizzare il linguaggio offensivo non significa giustificarne l'utilizzo, ma evidenziare come si sia sviluppata, tra gli utenti, una tolleranza verso tali contenuti. Di conseguenza, se la collettività non da rilevanza all'uso di espressioni ingiuriose, viene meno il rischio concreto che esse ledano la reputazione e l'onore della persona offesa[286].

Le modalità di commissione del reato di diffamazione tramite *social network*, *blog* o siti *Web* pongono delle difficoltà in ordine all'identificazione dell'autore del reato e alla possibilità di attribuire responsabilità penale al gestore della piattaforma per i contenuti diffamatori pubblicati dagli utenti.

Per quanto concerne l'identificazione della vittima, non sorgono particolari problematiche, poiché non è necessario che sia nominata esplicitamente ma, *a contrario*, è sufficiente che sia riconoscibile da elementi indiziari.

In questo contesto, l'individuazione dell'autore del reato è più complessa, poiché non può ritenersi sufficiente l'attribuzione del contenuto diffamatorio al

[286] Sul punto PIETRELLA, *L'incidenza dello sviluppo tecnologico sulla tenuta di condotte offensive. Rilevanza giuridica della comunicazione degradante online nel reato di diffamazione*, in *Sist. pen.*, 2023, 10, 28 ss.

titolare dell'account da cui è stato pubblicato il contenuto diffamatorio, potendo quest'ultimo essere stato clonato o utilizzato da terzi.

Per questo motivo, è considerato essenziale l'accertamento dell'indirizzo IP, ossia il codice numerico che identifica in modo univoco il dispositivo connesso alla *Rete*. Questo dato consente di risalire alla postazione da cui è stato inviato il messaggio e di verificarne l'effettiva riconducibilità al soggetto indagato. In assenza di tale accertamento, la giurisprudenza[287] ha affermato che non può essere emessa una condanna per diffamazione aggravata, ai sensi dell'art. 595, comma 3, c.p., poiché manca il grado di certezza necessario sull'identità dell'autore per attribuire responsabilità penale[288].

Più delicato è il tema della responsabilità del *provider* per i contenuti diffamatori pubblicati dagli utenti nella piattaforma da lui gestita, rispetto al quale è opportuno distinguere tra condotta omissiva e condotta attiva.

Secondo la dottrina[289] e la giurisprudenza[290] maggioritarie non può ritenersi sussistente un obbligo in capo all'ISP di impedire il reato di diffamazione da parte degli utenti. Infatti, da un lato, manca una posizione di garanzia ricavabile da disposizione specifiche, dalla norma generale di cui all'art. 40, comma 2, c.p., o dagli artt. 57 e 57 *bis* c.p.; dall'altro, i *provider* non dispongono di concreti poteri impeditivi per esercitare un controllo efficace su tutti i contenuti caricati *online* dagli utenti. Ciò implica che non può essere configurata una responsabilità per i gestori delle piattaforme e, questa posizione, è stata confermata anche dalla Corte EDU[291].

---

[287] Cfr. Cass. Pen, Sez. V, 5 febbraio 2018 (ud. 22 novembre 2017), n. 5352, in *Giurisprudenza Penale Web*, 2018, 9.

[288] Così LONGO, *Diffamazione via* mass media *e* social network*, tutele e risarcimenti*, cit., 6 s.

[289] Cfr. DE NATALE, *La responsabilità dei fornitori di informazioni in* internet *per i casi di diffamazione* online, in *Riv. trim. dir. pen. ec.*, 2009, 519; FUMO, *La diffamazione mediatica*, Torino, 2011, 53 ss.; GULLO, *I delitti contro l'onore*, in PIERGALLINI, VIGANÒ (a cura di), *Reati contro la persona e contro il patrimonio*, Torino, Giappichelli, 2015, 168 ss; INGRASSIA, *Il ruolo dell'ISP nel ciberspazio. Cittadino, controllore o tutore dell'ordine?*, in *DPC.*, 2012, 25 ss.

[290] Cfr. App. Milano sez. I, sent. 27.2.2013, in *Giur. mer.*, 2013, 7-8, 1577, con nota di SILVESTRE, *La sempreverde tentazione di sostituirsi al legislatore*; RESTA, *Diritti individuali e libertà della rete nel caso Vivi Down. Diversamente, per un controverso caso di responsabilità diretta e monosoggettiva dell'amministratrice di blog per alcuni commenti offensivi lasciati dai lettor*i, G.i.p. Varese, sent. 22.2.2013 n. 116, in *Arch. pen.*, 2013 (s.m.), 3, con nota critica di MINASOLA, *Blogging e diffamazione: responsabilità dell'amministratore del sito per i commenti dei lettori*.

[291] V. Corte EDU, G.C., sent. 16.6.2015, Delfi AS vs Estonia, § 116.

Diversamente, l'ISP può essere ritenuto penalmente responsabile per diffamazione nel caso in cui intervenga attivamente sul contenuto, ad esempio, modificando un messaggio offensivo o riproducendo contenuti diffamatori provenienti da altri siti, così da favorirne la diffusione.

Inoltre, può configurarsi una responsabilità a titolo di concorso con l'autore qualora il *provider* qualora metta a disposizione strumenti tecnici, servizi di memorizzazione o accesso che agevolino la commissione del reato, prima che questo venga realizzato.

Più complessa è, invece, la questione della responsabilità per concorso omissivo, ossia nei casi in cui il provider non rimuova un contenuto diffamatorio dopo aver ricevuto un ordine in tal senso da parte dell'autorità.

Secondo una prima interpretazione l'omessa rimozione potrebbe configurare una responsabilità penale per concorso, ma solo in presenza di un provvedimento formale dell'autorità giudiziaria o amministrativa. Altri, tuttavia, ritengono che il mantenimento *online* del contenuto offensivo rappresenti un fatto successivo alla consumazione del reato e non possa quindi essere considerato una forma di partecipazione al reato stesso, poiché la diffamazione non rientra tra i reati permanenti previsti dall'art. 595 c.p.[292]

2.3.3 Le ipotesi di pedopornografia e diffusione di contenuti illeciti

L'abuso sessuale sui minori rientra tra i fenomeni criminali che hanno trovato nella Rete un nuovo spazio di diffusione e nuovi strumenti di realizzazione del fatto tipico.

L'avvento delle tecnologie ha infatti favorito la nascita di una dimensione virtuale della pedofilia, caratterizzata dallo scambio di materiale pedopornografico, dalla creazione di comunità *online* con finalità pedofile e dai tentativi di adescamento di minori attraverso *Internet*.

[292] Sul punto MAZZANTI, *Il delitto di diffamazione al tempo dei* social network*: punti fermi e spunti problematici*, in PASSAGLIA, POLETTI (a cura di), *Nodi virtuali, legami informali:* Internet *alla ricerca di regole*, Pisa, 2016, 211 ss.

L'utilizzo dei nuovi *media* ha profondamente modificato le modalità con cui questi fenomeni criminali – già noti da tempo – si manifestano, introducendo elementi nuovi rispetto alle forme tradizionali di abuso sessuale.

Particolarmente rilevante è il caso della produzione e diffusione di materiale pedopornografico, che da attività marginale e confinata a contesti ristretti e nascosti, si è trasformata in un fenomeno di portata globale e in continua espansione: l'incontro tra perversioni sessuali e cyberspazio ha amplificato la diffusione e l'impatto di questi crimini a livello mondiale[293].

L'art. 600-*ter* c.p[294]. fornisce una definizione di pornografia minorile, intesa come qualsiasi rappresentazione, con ogni mezzo, di un minore di diciotto anni coinvolto in attività sessuali esplicite, siano esse reali o simulate, oppure qualsiasi raffigurazione degli organi sessuali di un minore con finalità sessuali. Lo stesso articolo regola dettagliatamente le diverse forme di pornografia minorile, prevedendo la pena della reclusione e della multa per chiunque realizzi o metta in commercio materiale pornografico riguardante minori.

Inoltre, l'assetto incriminatorio volto a tutelare l'integrità sessuale e l'immagine dei minori non si limita a sanzionare chi partecipa attivamente alla

---

[293] Cfr. MACILOTTI, *Il contrasto alla pedopornografia* online*: esperienze italiane e francesi a confronto*, in *RCVS*, 2011, 1, 84.

[294] Art. 600-*ter* c.p. – Pornografia minorile «1. È punito con la reclusione da sei a dodici anni e con la multa da euro 24.000 a euro 240.000 chiunque:
1) utilizzando minori di anni diciotto, realizza esibizioni o spettacoli pornografici ovvero produce materiale pornografico;
2) recluta o induce minori di anni diciotto a partecipare a esibizioni o spettacoli pornografici ovvero dai suddetti spettacoli trae altrimenti profitto.
2. Alla stessa pena soggiace chi fa commercio del materiale pornografico di cui al primo comma.
3. Chiunque, al di fuori delle ipotesi di cui al primo e al secondo comma, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, diffonde o pubblicizza il materiale pornografico di cui al primo comma, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto, è punito con la reclusione da uno a cinque anni e con la multa da lire cinque milioni a lire cento milioni.
4. Chiunque, al di fuori delle ipotesi di cui ai commi primo, secondo e terzo, offre o cede ad altri, anche a titolo gratuito, il materiale pornografico di cui al primo comma, è punito con la reclusione fino a tre anni e con la multa da euro 1.549 a euro 5.164.
5. Nei casi previsti dal terzo e dal quarto comma la pena è aumentata in misura non eccedente i due terzi ove il materiale sia di ingente quantità.
6. Salvo che il fatto costituisca più grave reato, chiunque assiste a esibizioni o spettacoli pornografici in cui siano coinvolti minori di anni diciotto è punito con la reclusione fino a tre anni e con la multa da euro 1.500 a euro 6.000.
7. Ai fini di cui al presente articolo per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali».

creazione o diffusione di materiale pedopornografico, ma si estende anche a chi ne fruisce semplicemente.

L'art. 600-*quater* c.p.[295], infatti, punisce chiunque detenga consapevolmente materiale pornografico realizzato con minori di diciotto anni. Pertanto, è penalmente rilevante anche la mera detenzione, purché sia accompagnata dalla consapevolezza della natura illecita del materiale. La norma, dunque, esclude la punibilità nei casi in cui la persona ignori in buona fede che i soggetti rappresentati siano minorenni.

Quest'impostazione dimostra come il legislatore, nel disciplinare la detenzione di materiale pedopornografico, abbia voluto evitare qualsiasi forma di tolleranza verso chi ne fa uso. Difatti, nella prassi applicativa, le condanne per questo tipo di reato sono generalmente severe e la giurisprudenza della Corte di Cassazione ha progressivamente ampliato l'interpretazione del concetto di "detenzione". Inizialmente, si riteneva che la detenzione sussistesse anche quando i file pedopornografici venivano spostati nel cestino del *computer*, poiché ancora tecnicamente recuperabili[296]. Al contrario, la cancellazione definitiva dei file veniva considerata come cessazione della detenzione.

Successivamente, però, la giurisprudenza[297] ha adottato un orientamento più rigoroso: anche la detenzione di file poi cancellati definitivamente può integrare il reato, purché sia accertato che quei file siano stati effettivamente posseduti in precedenza. La cancellazione, infatti, segna solo la fine della permanenza del reato, ma non elimina la rilevanza penale della condotta tenuta fino a quel momento. Questo approccio è coerente con la natura del reato, che si consuma nel momento stesso in cui avviene la detenzione, anche se solo per un periodo limitato.

---

[295] Art. 600-*quater* c.p. – "Detenzione o accesso a materiale pornografico" «1. Chiunque, al di fuori delle ipotesi previste dall'articolo 600-ter, consapevolmente si procura o detiene materiale pornografico realizzato utilizzando minori degli anni diciotto, è punito con la reclusione fino a tre anni e con la multa non inferiore a euro 1.549.
2. La pena è aumentata in misura non eccedente i due terzi ove il materiale detenuto sia di ingente quantità.
3. Fuori dei casi di cui al primo comma, chiunque, mediante l'utilizzo della rete internet o di altre reti o mezzi di comunicazione, accede intenzionalmente e senza giustificato motivo a materiale pornografico realizzato utilizzando minori degli anni diciotto è punito con la reclusione fino a due anni e con la multa non inferiore a euro 1.000».
[296] Cfr. Cass. pen. n. 24345 del 8 giugno 2015.
[297] V. Cass. pen. n. 11044 del 8 marzo 2017.

Questa impostazione particolarmente rigorosa si riflette anche nell'evoluzione normativa, che ha introdotto l'art. 600-*quater*.1 c.p., con l'art. 4 della legge 6 febbraio 2006, n. 38.

Questa disposizione è stata pensata per rafforzare la protezione dei minori, estendendo l'ambito di applicazione delle norme precedenti – artt. 600-*ter* e 600-*quater* – anche ai casi in cui non siano coinvolti minori, ma soltanto immagini generate digitalmente[298].

Nell'affrontare il tema della responsabilità penale degli ISP relativa a reati legati all'abuso sessuale su minori entra in gioco la tutela della riservatezza della *privacy* degli utenti *online*, piuttosto che la libertà di espressione, che invece rileva nei casi di diffamazione[299].

Anzitutto, è stato ipotizzato che il *provider* possa essere ritenuto responsabile per non aver impedito la commissione di reati di pornografia minorile da parte degli utenti. Tuttavia, la posizione prevalente in dottrina[300] tende a escludere questa possibilità, per la mancanza di basi giuridiche su cui fondare un obbligo di controllo da parte dell'ISP. Infatti, secondo questa visione, il *provider* non sarebbe titolare di obblighi giuridici di impedimento e, non sarebbe comunque in grado di esercitare un controllo efficace – come si è già visto – per due motivi principali: da un lato, la necessità di tutelare la riservatezza delle informazioni che transitano in *Rete*; dall'altro, per l'enorme quantità di dati scambiati e alla natura aperta di *Internet*, che permette un flusso continuo e incontrollato di nuove informazioni[301].

Si è già visto che l'art. 600-*ter*, comma 3, c.p.[302], sanziona le condotte di divulgazione, distribuzione, diffusione e pubblicizzazione di materiale

---

[298] Sul punto PELLICONI, *La pornografia minorile nella sfera privata e il reato di pedopornografia virtuale. Considerazioni critiche alla luce di Cass. Pen., Sez. III, Sent. N. 22265/2017*, in *Giustizia*, 2018, 2 ss.

[299] Così BAFFA, MASSARO, *Pedopornografia* online*: strumenti di prevenzione e contrasto*, Roma, 2020, 12.

[300] Così PICOTTI, *Fondamento e limiti della responsabilità penale dei* Service-Providers *in* Internet, in *Dir. pen. proc.*, 1999, 3, 380; SIEBER, *Responsabilità penali per la circolazione di dati nelle reti internazionali di* computer*. Le nuove sfide di* Internet (trad. it. a cura di SFORZI), in *Riv. trim. dir. pen. econ.*, 1997, 3, 1218 ss.

[301] V. BAFFA, MASSARO, *Pedopornografia* online, cit., 125 ss.

[302] Art. 600-*ter*, co. 3 «Chiunque, al di fuori delle ipotesi di cui al primo e al secondo comma, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, diffonde o pubblicizza il materiale pornografico di cui al primo comma, ovvero distribuisce o divulga notizie o informazioni finalizzate

pedopornografico, precisando che tali azioni possono essere compiute con qualsiasi mezzo. La formulazione ampia di questa disposizione ha portato alcuni a ipotizzare una possibile responsabilità commissiva dell'ISP, ritenendo che le attività tipiche svolte dai *provider* non siano del tutto incompatibili con la struttura della fattispecie.

Tuttavia, il vero ostacolo resta l'elemento soggettivo: anche considerando la flessibilità del dolo eventuale, esso non può essere esteso a ogni esigenza di tutela penale. Nondimeno, una possibile soluzione per superare le criticità legate all'elemento soggettivo potrebbe consistere nell'integrare in modo sistematico gli strumenti di intelligenza artificiale già utilizzati dagli ISP, come, ad esempio, l'adozione di algoritmi in grado di individuare contenuti pornografici e la presenza di persone fisiche incaricate di esaminare, entro determinati tempi e modalità, il materiale segnalato dal sistema, nonché di soggetti che verifichino – secondo procedure definite – i contenuti per escludere che abbiano natura pedopornografica.

Così, si potrebbe configurare una responsabilità penale, sia colposa che dolosa, su chi ometta il controllo richiesto oppure, pur avendo avuto conoscenza della presenza di materiale pedopornografico, non attivi le successive fasi previste dalla procedura[303].

Nell'ordinamento italiano un punto di svolta si è avuto con la legge n. 38 del 2006, che ha introdotto gli artt. 14-*bis* e ss. della legge n. 269 del 1998[304].

In particolare, l'art. 14-*bis,* l. 269/1998 ha istituito il Centro nazionale per il contrasto della pedopornografia sulla Rete *Internet*, con il compito raccogliere le segnalazioni – provenienti da autorità italiane e straniere, nonché da soggetti pubblici e privati – relative a siti che diffondono materiale pedopornografico *online*.

Il seguente art. 14-*ter* l. 269/1998 impone ai *provider* l'obbligo di segnalare al Centro, qualora ne vengano a conoscenza, soggetti o imprese che diffondano o commercino materiale pedopornografico, anche in via telematica. Inoltre, devono fornire tempestivamente al Centro ogni informazione contrattuale richiesta su tali

all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto, è punito con la reclusione da uno a cinque anni e con la multa da lire cinque milioni a lire cento milioni».

[303] Cfr. BAFFA, MASSARO, *Pedopornografia* online, cit., 137 ss.

[304] Legge n. 269 del 1998 – "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù".

soggetti. La violazione di questo obbligo, salvo che non costituisca reato, comporta una sanzione amministrativa.

Infine, l'art. 14-*quater* l. 269/1998 impone ai fornitori l'obbligo di rimuovere i contenuti pedopornografici e di impedire l'accesso ai siti segnalati dal Centro, utilizzando strumenti di filtraggio conformi ai requisiti tecnici stabiliti con decreto ministeriale.

Dal punto di vista penale, la mancata osservanza di tali obblighi potrebbe teoricamente configurare la contravvenzione prevista dall'art. 650 c.p. Tuttavia, essendo l'art. 14-*quater* una norma speciale, si applica la sola sanzione amministrativa, come stabilito dall'art. 9 della legge n. 689/1981[305].

Tutte queste previsioni vengono rafforzate dal *Digital Services Act*, il quale, al fine di garantire la tutela dei diritti fondamentali degli utenti *online* ha introdotto delle procedure volte a rendere più efficiente e tempestiva la rimozione dei contenuti illegali – inclusi quelli di natura pedopornografica – come verrà approfondito nel prosieguo[306].

2.4. La posizione del *provider* tra dolo e colpa

Nel definire un quadro penalistico applicabile agli ISP, le difficoltà derivano anche da una serie di criticità legate alla complessità di accertare l'elemento soggettivo.

Infatti, affinché possa configurarsi una responsabilità penale dell'ISP, per concorso ex art. 110 c.p. o per omissione *ex* art. 40, comma 2 c.p., non è possibile prescindere da un'analisi dell'elemento soggettivo[307].

Per poter configurare una responsabilità concorsuale del *provider,* è necessario accertare almeno la presenza di un atteggiamento psicologico

[305] V. BAFFA, MASSARO, *Pedopornografia* online, cit., 137 ss.
[306] Così, RUM, *Le nuove frontiere della normativa sui servizi digitali nel mercato unico europeo: si rafforza la protezione dei diritti fondamentali degli utenti* online *con la garanzia pubblicistica delle* Authorities*. Il* Digital Services Act, in *Dir. amm.*, 2022, 15.
[307] Sul punto COSTA, *La responsabilità dell'*Internet Service Provider, cit., 7.

riconducibile al dolo generico[308]. Ciò implica, da un lato, la consapevolezza e la volontà di fornire un contributo alla condotta illecita realizzata dall'autore principale e, dall'altro, la conoscenza dell'obiettivo perseguito da quest'ultimo.

Tale principio deve leggersi necessariamente con la normativa sul commercio elettronico, in particolare agli artt. 14 e 15 della Direttiva 2000/31/CE, e oggi anche alla luce del Digital Services Act[309], in base ai quali qualsiasi valutazione sulla responsabilità dell'ISP presuppone la sua effettiva conoscenza dell'illiceità delle attività svolte dagli utenti. La richiesta di un'effettiva conoscenza ha implicazioni rilevanti sia per quanto riguarda la responsabilità per concorso attivo che la responsabilità per concorso omissivo.

Con riferimento al concorso *ex* art. 110 c.p., l'ISP non può essere ritenuto responsabile a titolo di concorso, né come partecipe né come coautore, se il suo intervento non è accompagnato almeno dal dolo diretto, che ricorre quando l'evento che si realizza coincide esattamente con il fine ultimo che l'agente vuole ottenere[310].

Il concetto di "effettiva conoscenza", seppur centrale per stabilire l'eventuale responsabilità del *provider*, presenta alcune ambiguità. Questo termine, introdotto dalla Direttiva 2000/31/CE, e recepito nei diversi ordinamenti nazionali, sembra ispirarsi al concetto di *actual knowledge* previsto dal *Digital Millenium Copyright Act* statunitense[311]. Nell' ordinamento italiano, ciò significa che non è sufficiente dimostrare che il *provider* avrebbe potuto venire a conoscenza di attività penalmente rilevanti svolte dagli utenti semplicemente adottando un comportamento diligente. È invece necessario provare che il *provider* avesse una conoscenza concreta e reale dell'illiceità di tali attività[312].

---

[308] Ai sensi dell'art. 43 c.p. – "Elemento psicologico del reato": «Il delitto: 2. è doloso, o secondo l'intenzione, quando l'evento dannoso o pericoloso, che è il risultato dell'azione od omissione e da cui la legge fa dipendere l'esistenza del delitto, è dall'agente preveduto e voluto come conseguenza della propria azione od omissione […]».
In particolare, il dolo è generico quando assume la sua forma più tipica, ossia quella in cui l'agente con la volontà che l'evento si realizzi. Cfr. FRANCESCHETTI, *Dolo*, in *Altalex*, 2016, 12.

[309] Gli artt. 16 e 17 del d.lgs. 70/2003 trovano oggi corrispondenza agli artt. 6 e 7 del Regolamento (UE) 2022/2065, che ne conferma e aggiorna i contenuti.

[310] V. FRANCESCHETTI, *Dolo*, cit., 12.

[311] 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».

[312] Sul punto STEA, *La responsabilità penale dell'*Internet Provider, 4. Così citato in COSTA, *La responsabilità dell'*Internet Service Provider, cit. 53.

Dal requisito dell'effettiva conoscenza deriva che, anche qualora l'ISP svolga consapevolmente o fornisca servizi che contribuiscano attivamente alla commissione di reati da parte degli utenti, tali attività potranno assumere rilevanza penale ai sensi dell'art. 110 c.p. se si dimostra sia la concreta consapevolezza dell'illiceità della condotta dell'utente, sia una volontaria adesione psicologica a tale condotta. In assenza di questi due elementi, si attribuirebbe al *provider* un *dolus in re ipsa*, solo per il fatto di aver messo a disposizione strumenti tecnici.

Dunque, questa osservazione esclude la possibilità di attribuire all'ISP una responsabilità penale non solo a titolo colposo, ma anche sulla base del dolo eventuale. Infatti, è la stessa normativa che disciplina la responsabilità dell'ISP a stabilire che non è sufficiente il semplice fatto di aver previsto e accettato il rischio di contribuire a un'attività illecita per configurare una responsabilità penale. Allo stesso modo, deve escludersi la possibilità che il *provider* possa essere ritenuto responsabile ai sensi dell'art. 116 c.p., per un reato diverso da quello effettivamente voluto e commesso da un altro partecipante, così come non è configurabile una responsabilità per concorso colposo in un reato doloso.

Anche quando si cerca di configurare una responsabilità omissiva in capo al *provider* la possibilità di attribuire al provider un elemento soggettivo risulta particolarmente complessa, soprattutto nei casi in cui egli non intervenga direttamente nella gestione o diffusione dei contenuti *online*.

Nei reati omissivi impropri, il dolo richiede che il soggetto sia consapevole della propria posizione di garanzia, si rappresenti l'evento illecito e ometta volontariamente di impedirlo.

Tuttavia, per gli ISP, le maggiori difficoltà nell'accertare il dolo riguardano soprattutto l'assenza di una norma che riconosca espressamente in capo al fornitore una posizione di garanzia e la capacità di rappresentarsi l'antigiuridicità delle condotte poste in essere dai singoli utenti della Rete. Se, inoltre, si considerano anche le difficoltà tecniche legate al controllo di ogni singolo contenuto trasmesso o memorizzato, risulta evidente la difficoltà nell'attribuire all'ISP una conoscenza effettiva delle condotte illecite compiute dagli utenti.

Inoltre, non sembra possibile estendere all' ISP neppure quell'orientamento giurisprudenziale[313] che riconosce la responsabilità omissiva anche quando l'evento illecito è stato semplicemente considerato come una possibilità. Questa interpretazione, infatti, è in contrasto con le caratteristiche specifiche dell'ISP e con la normativa di riferimento, che richiede una conoscenza effettiva dell'illecito, escludendo quindi sia la semplice possibilità di venirne a conoscenza, sia l'accettazione del rischio che si verifichino reati online.

Di conseguenza, non si può fondare una responsabilità penale né sulla mancata reazione a generici segnali d'allarme, né sulla presunzione che il *provider* non potesse non sapere dei reati commessi attraverso i propri *server*.

Anche nel caso in cui tale conoscenza venga acquisita successivamente, essa non costituisce di per sé un indice di colpevolezza, ma rappresenta solo il punto di partenza per l'attivazione di obblighi di collaborazione e intervento, che non sono penalmente sanzionabili come omissione di impedimento del reato altrui[314].

2.5. Il rapporto con l'art. 27 co. 1 della Costituzione

Uno dei principi cardine del diritto penale è espresso nell'art. 27, comma 1, della Costituzione, il quale afferma che «la responsabilità penale è personale»[315]. Ciò significa che una persona può essere chiamata a rispondere penalmente solo se l'azione contestata non solo è a lei riconducibile, ma anche frutto di una condotta colpevole[316].

La responsabilità degli ISP, come visto, può essere ipotizzata sia in termini di concorso nel reato commesso dagli utenti secondo l'art. 110 c.p., sia come responsabilità del per omissione, ai sensi dell'art. 40 c.p. Tuttavia, risulta estremamente difficile attribuire responsabilità penale agli intermediari per i reati commessi da terzi. Ciò perché il principio della responsabilità personale, sancito dalla Costituzione, esclude ogni forma di responsabilità oggettiva[317].

---

[313] Cfr. Cass. Pen. Sez. III, 12 maggio 2010, n. 2870.
[314] In argomento COSTA, *La responsabilità dell'*Internet Service Provider, cit. 51 ss.
[315] Articolo 27, comma 1, Cost.
[316] Sul punto CADOPPI, VENEZIANI, *Elementi di diritto penale. Parte generale*, Padova, 2023, 130.
[317] V. ALLEGRI, Ubi Social, Ibi Ius. *Fondamenti costituzionali dei* social network *e profili giuridici della responsabilità dei* provider, Milano, 2018, 159 s.

Sebbene non vi sia un riferimento esplicito al principio di personalità della responsabilità penale, il quadro normativo europeo appare coerente con tale principio. Infatti, il legislatore europeo – prima con la Direttiva 2000/31/CE e poi con il *Digital Services Act* (DSA) – riesce a evitare l'introduzione di un regime di responsabilità oggettiva, riconducendo la disciplina nell'ambito della colpa.

Tuttavia, l'elemento soggettivo non viene valutato in base a un generico criterio di diligenza, ma su uno standard di colpa specifica, che si manifesta ogni volta che l'intermediario non rispetta le condizioni previste dalla normativa. Ad esempio, il *provider* è tenuto ad agire per rimuovere le informazioni o a disabilitare l'accesso non appena sia effettivamente a conoscenza della loro illiceità.

Inoltre, in capo ai prestatori non è previsto nessun obbligo di sorveglianza sulle informazioni trasmesse o memorizzate, proprio perché un simile obbligo comporterebbe per gli ISP una forma di responsabilità semi-oggettiva[318].

2.6. Gli obblighi di segnalazione e rimozione dei contenuti illeciti

Se da un lato la Direttiva sul commercio elettronico ha posto le fondamenta per il commercio digitale, definendo i principi generali sulla responsabilità degli intermediari, dall'altro, il Digital Services Act interviene con delle disposizioni più specifiche e dettagliate, focalizzandosi sulla responsabilità, la moderazione dei contenuti, la trasparenza delle piattaforme e la tutela dei diritti degli utenti.

Nell'attuale epoca digitale, le piattaforme *online* occupano una posizione sempre più rilevante nella quotidianità, influenzando significativamente il modo di accesso alle informazioni, di comunicazione e di fruizione dei contenuti. Questo crescente potere ha però sollevato importanti interrogativi in merito alla gestione dei contenuti, alla tutela degli utenti e alla responsabilità delle piattaforme stesse. Su questa scia, il DSA prevede per le piattaforme digitali l'adozione di misure proattive per prevenire e contrastare la circolazione di contenuti illeciti[319].

Fino all'adozione del Regolamento (UE) 2022/2065, la moderazione dei contenuti pubblicati dagli utenti svolta dalle piattaforme digitali era una pratica

[318] Così IMPERADORI, *La responsabilità dell'*Internet Service Provider *per violazione del diritto d'autore: un'analisi comparata*, in *Lawtch*, 2014, 58 ss.
[319] Sul punto FOTI, *Regolamentazione digitale: il* Digital Services Act *e le piattaforme* online, in *Altalex*, 2024, 1 ss.

attuata in assenza di un quadro normativo specifico, pur rappresentando – e continuando a rappresentare – il primo, e spesso unico, strumento sanzionatorio di contrasto alla diffusione della disinformazione in Rete.

Il primo impatto concreto del *Digital Services Act* (DSA) su queste pratiche si riscontra all'art. 3, lett. t), che introduce una definizione esplicita di "moderazione dei contenuti", qualificandola come l'insieme delle «attività, automatizzate o meno, svolte dai prestatori di servizi intermediari con il fine, in particolare, di individuare, identificare e contrastare contenuti illegali e informazioni incompatibili con le condizioni generali, forniti dai destinatari del servizio»[320].

Queste attività a cui si fa riferimento includono interventi che influenzano la disponibilità, la visibilità o l'accesso a tali contenuti, come ad esempio la loro rimozione, la riduzione della loro diffusione, la sospensione della monetizzazione o il blocco dell'accesso. Rientrano inoltre le misure che limitano la possibilità per gli utenti di pubblicare tali contenuti, come la sospensione o la chiusura del loro account[321].

Come stabilito dall'art. 8 del DSA[322], i fornitori continuano a non essere soggetti a un obbligo generale di sorvegliare i contenuti condivisi dagli utenti, sebbene vi siano disposizioni che incidono in modo rilevante sulla loro responsabilità e sugli obblighi rispetto ai contenuti illegali[323].

Circa la struttura delle norme stabilite dal DSA relativa alla *content moderation* si possono individuare tre principali linee di intervento: quella mirata ad assicurare la trasparenza delle operazioni di moderazione, quella volta a definire le procedure attraverso cui vengono adottate eventuali misure restrittive, e infine quella relativa ai meccanismi di tutela a disposizione degli utenti contro le restrizioni subite.

---

[320] Art. 3, lett. t), Regolamento (UE) 2022/2065.

[321] Così BIRRITTERI, *Contrasto alla disinformazione,* Digital Services Act *e attività di* private enforcement*: fondamento, contenuti e limiti degli obblighi di* compliance *e dei poteri di autonormazione degli operatori*, in *MediaLaws*, 2023, 2, 54 s.

[322] Articolo 8 DSA – "Punti di contatto per le autorità degli Stati membri, la Commissione e il Comitato".

[323] V. VICINANZA, *La responsabilità delle piattaforme*, cit., 10 s.

Nel contesto della prima direttrice d'intervento, il Regolamento impone alle piattaforme l'obbligo di includere nei propri termini contrattuali informazioni dettagliate sulle modalità con cui viene effettuata la moderazione dei contenuti.

Inoltre, le piattaforme devono pubblicare almeno una volta all'anno report chiari e facilmente accessibili che illustrino le attività di moderazione svolte. Sempre in nome della trasparenza, i fornitori di servizi di memorizzazione di informazioni sono tenuti a motivare in modo preciso ogni restrizione applicata agli utenti.

Per quanto riguarda l'ambito procedurale – del quale si parlera più nel dettaglio nel proseguo del presente lavoro – il DSA stabilisce un vero e proprio procedimento fondato sulle segnalazioni da parte di terzi.

Infine, per quanto riguarda le forme di tutela previste per gli utenti che subiscono restrizioni, il DSA prevede due strumenti alternativi alla tutela giurisdizionale. Il primo è rappresentato da un sistema interno di gestione dei reclami, messo a disposizione direttamente dal prestatore di servizi. Il secondo consiste nella possibilità di contestazione davanti a un organismo indipendente di risoluzione extragiudiziale delle controversie, che deve rispettare i requisiti stabiliti dall'art. 21 DSA e può essere certificato dal Coordinatore dei servizi digitali dello Stato membro in cui ha sede – in Italia tale funzione è attribuita all'AGCOM, come previsto dal d.l. n. 123/2023[324].

Sul punto, la prima disposizione di rilievo è contenuta nell'art. 16 DSA[325], che prevede il c.d. meccanismo di *notice and action*.

Tale meccanismo impone a tutti i fornitori di servizi di memorizzazione di predisporre dei meccanismi facilmente accessibili e utilizzabili per permettere a chiunque – persona fisica o ente – di segnalare, esclusivamente in formato elettronico, la presenza di contenuti che ritengano illegali all'interno del servizio.

I fornitori devono inoltre adottare misure idonee per agevolare le segnalazioni, in modo tale che risultino sufficientemente dettagliate e ben motivate per poter consentire alla piattaforma di individuare in modo chiaro e tempestivo il

[324] In argomento PICA, *La tutela della libertà di informazione nel* Digital Services Act *tra contrasto alle "manipolazioni algoritmiche" e limiti alla* content moderation, in *MediaLaws*, 2024, 1, 38 ss.
[325] Art. 16 DSA – "Obblighi generali dei prestatori di servizi di hosting in materia di segnalazione e rimozione di contenuti illegali".

contenuto considerato. Sono considerate tali, in particolare, le segnalazioni che contengono gli elementi specifici elencati in modo puntuale al par. 2 dell'art. 16 DSA[326].

L'art. 16 DSA fornisce indicazioni aggiuntive, sia generali che specifiche, sugli obblighi procedurali a carico dei fornitori di servizi e sui diritti riconosciuti agli utenti coinvolti. Da un lato, i prestatori sono tenuti a gestire le segnalazioni ricevute «in modo tempestivo, diligente, non arbitrario e obiettivo»[327] comunicando anche l'eventuale utilizzo di strumenti automatizzati per analizzare e decidere in merito ai contenuti segnalati. Dall'altro, viene garantito un livello minimo di tutela procedurale, prevedendo che chi effettua una segnalazione deve essere informato senza ritardo sia dell'avvenuta ricezione della segnalazione sia della decisione adottata, con indicazioni sulle possibilità di ricorso.

Un aspetto particolarmente rilevante è che, secondo il par. 3 dell'art. 16 DSA, quando una segnalazione consente al *provider* di riconoscere l'illegalità del contenuto, anche senza un'analisi giuridica dettagliata, essa determina per l'operatore una conoscenza effettiva dell'illegalità dell'attività o dell'informazione diffusa. Questa circostanza determina delle conseguenze dirette sul regime di responsabilità dell'*hosting provider*, come previsto dall'articolo 6 del DSA.

È importante sottolineare che l'obbligo di predisporre il meccanismo di *notice and action* riguarda esclusivamente la segnalazione di contenuti e attività illegali, e non si estende ai contenuti che violano solo le condizioni d'uso o gli standard della *community*. Tuttavia, le piattaforme possono comunque decidere

[326] Ai sensi dell'art. 16, par. 2, DSA: «I meccanismi di cui al paragrafo 1 sono tali da facilitare la presentazione di segnalazioni sufficientemente precise e adeguatamente motivate. A tal fine i prestatori di servizi di memorizzazione di informazioni adottano le misure necessarie per consentire e facilitare la presentazione di segnalazioni contenenti tutti gli elementi seguenti: a) una spiegazione sufficientemente motivata dei motivi per cui la persona o l'ente presume che le informazioni in questione costituiscano contenuti illegali; b) una chiara indicazione dell'ubicazione elettronica esatta di tali informazioni, quali l'indirizzo o gli indirizzi URL esatti e, se necessario, informazioni supplementari che consentano di individuare il contenuto illegale adeguato al tipo di contenuto e al tipo specifico di servizio di memorizzazione di informazioni; c) il nome e l'indirizzo di posta elettronica della persona o dell'ente che presenta la segnalazione, tranne nel caso di informazioni che si ritiene riguardino uno dei reati di cui agli articoli da 3 a 7 della direttiva 2011/93/UE; d) una dichiarazione con cui la persona o l'ente che presenta la segnalazione conferma la propria convinzione in buona fede circa l'esattezza e la completezza delle informazioni e delle dichiarazioni ivi contenute».

[327] Art. 16, par. 6, DSA.

volontariamente di applicare tale procedura anche a questi casi, ancorché il legislatore europeo non ha imposto tale estensione.

Dunque, l'art. 16 DSA assume così un ruolo centrale, poiché istituzionalizza un meccanismo fondamentale per il funzionamento del *private enforcement*, consentendo a utenti ed enti di collaborare con le piattaforme nel contrasto ai contenuti illeciti. Questo consente agli utenti di affiancare e supportare i fornitori nella complessa e onerosa attività di controllo e repressione dei contenuti illeciti. Considerata, infatti, la vastità dei contenuti *online* non è realistico aspettarsi che i fornitori riescano da soli a individuare ogni contenuto illegale.

L'art. 17 DSA[328] completa il quadro procedurale prevedendo per gli *hosting provider* l'obbligo di fornire una motivazione chiara e specifica agli utenti rispetto alle misure adottate nei loro confronti nell'ambito della moderazione dei contenuti.

Le sanzioni per cui è richiesta tale motivazione, elencate al par. 1 dell'art. 17 DSA, comprendono interventi che vanno dalla semplice limitazione della visibilità di un contenuto, alla sospensione o interruzione del servizio, fino alla chiusura definitiva dell'account dell'utente.

Il par. 3 dell'art. 17 DSA fornisce ulteriori chiarimenti rilevanti sul contenuto dell'obbligo di motivazione. In primo luogo, è necessario specificare il tipo di sanzione adottata, indicando anche l'ambito territoriale in cui essa si applica e la sua durata.

Inoltre, devono essere illustrati i fatti e le circostanze che hanno portato alla decisione, precisando – se opportuno – se la misura sia stata presa in seguito a una segnalazione ricevuta tramite il meccanismo di *notice and action* oppure se derivi da un'indagine avviata autonomamente dalla piattaforma. Solo se strettamente necessario, può essere rivelata anche l'identità del soggetto che ha effettuato la segnalazione.

È altresì richiesto che venga chiarito se la decisione si basi sull'illegalità del contenuto o sulla sua incompatibilità con le condizioni d'uso del servizio, specificando in entrambi i casi la norma giuridica o la clausola contrattuale violata, e spiegando perché il contenuto è ritenuto in contrasto con tali disposizioni. Infine, il prestatore deve indicare se la decisione è stata presa con l'ausilio di strumenti

[328] Art. 17 DSA – "Informazioni da fornire ai destinatari del servizio".

automatizzati, anche per quanto riguarda l'individuazione del contenuto sanzionato, e deve fornire informazioni chiare e facilmente comprensibili sui mezzi di ricorso disponibili. Questi includono il sistema interno di gestione dei reclami, la possibilità di ricorrere a un organismo di risoluzione extragiudiziale delle controversie e il ricorso per via giudiziaria.

L'ampiezza dell'obbligo motivazionale, pur comportando in capo ai soggetti regolati notevoli oneri gestionali e organizzativi, risulta giustificata alla luce dei diritti fondamentali che l'attività di moderazione può coinvolgere. Inoltre, l'obbligo di motivazione fornisce all'utente una base informativa essenziale per poter esercitare in modo consapevole ed efficace i propri diritti attraverso i meccanismi di reclamo[329].

A completare il sistema di segnalazione dell'art. 16 DSA è l'art. 22 DSA[330], che introduce i c.d. "segnalatori attendibili" (*trusted flaggers*). Si tratta di soggetti – generalmente organizzazioni o gruppi di esperti – ufficialmente riconosciuti da uno Stato membro dell'Ue per la loro competenza specifica nel rilevare contenuti illeciti in Rete. Infatti, la loro figura è stata prevista con l'obiettivo rendere più efficiente l'individuazione e la rimozione di contenuti illegali o dannosi sulle piattaforme digitali[331].

2.7. Le condizioni che escludono la responsabilità del *Provider*

Si è già osservato in precedenza che, sebbene il Regolamento (UE) 2022/2065 contenga una revisione del quadro normativo relativo alla responsabilità dei *provider*, i principi cardine rimangono sostanzialmente in linea con quelli stabiliti dalla *Direttiva E-Commerce*.

Per tale motivo, appare opportuno ripercorrere, in modo sintetico, i principi fondamentali della Direttiva 2000/31/CE, la quale ha rappresentato per oltre vent'anni la normativa di riferimento in materia di responsabilità degli *Internet Service Provider*.

---

[329] In tal senso BIRRITTERI, *Contrasto alla disinformazione*, cit., 60 ss.
[330] Art. 22 DSA – "Obbligo di fornire motivazioni".
[331] Cfr. FOTI, *Regolamentazione digitale*, cit., 3.

Questa normativa ha notevolmente limitato i casi in cui gli ISP possono essere ritenuti responsabili, sia in sede civile che penale, poiché ha riconosciuto diverse forme di esenzione da responsabilità a loro favore.

Anzitutto, l'art. 12 della Direttiva regola l'attività del prestatore che si limita a trasmettere informazioni fornite da un utente o a fornire accesso alla Rete (*mere conduit*). Il *provider* che svolge questo tipo di attività non può essere ritenuto responsabile, né civilmente né penalmente, per i contenuti trasmessi, a condizione che non sia lui a generare la trasmissione, non scelga il destinatario della comunicazione e non intervenga in alcun modo nella selezione o modifica delle informazioni trasmesse.

La disposizione successiva (art. 13 della Direttiva) disciplina l'attività di caching, ossia la memorizzazione automatica, temporanea e intermedia dei dati effettuata per rendere più efficiente la loro successiva trasmissione. In questo caso, l'ISP per beneficiare dell'esenzione della responsabilità deve astenersi dal modificare le informazioni memorizzate, rispettare le condizioni di accesso stabilite per quei dati e attenersi alle regole di aggiornamento indicate secondo modalità comunemente riconosciute e adottate nel settore. Inoltre, non deve ostacolare l'uso legittimo di tecnologie diffuse e utilizzate per monitorare l'impiego delle informazioni. Infine, è tenuto a intervenire tempestivamente per rimuovere i dati o bloccarne l'accesso non appena venga effettivamente a conoscenza del fatto che le informazioni sono state eliminate dalla rete di origine, che l'accesso è stato disattivato, oppure che un'autorità giudiziaria o amministrativa ne ha ordinato la rimozione o l'inaccessibilità.

Infine, l'art. 14 della Direttiva, relativo all'attività di *hosting*, stabilisce che il *provider* non può essere ritenuto responsabile per i contenuti illeciti caricati da terzi, a condizione che non sia effettivamente a conoscenza del carattere illecito dell'attività o dell'informazione ospitata e, nel caso di richieste di risarcimento, non sia a conoscenza di elementi che rendano evidente l'illegalità. Parimenti, qualora venga a conoscenza di tali circostanze, il *provider* deve intervenire tempestivamente per rimuovere i contenuti o impedirne l'accesso. Il secondo

comma dell'art. 14 chiarisce che l'esenzione da responsabilità non vale se l'utente agisce sotto la direzione o il controllo dell'*hosting provider*[332].

Il Regolamento sui servizi digitale introduce una disciplina peculiare in materia di responsabilità dei prestatori. Infatti, non elenca in modo specifico i casi in cui gli ISP possono essere ritenuti responsabili, ma definisce le condizioni in cui tale responsabilità è esclusa[333]. Sul punto, è interessante notare come gli artt. 4, 5 e 6 del DSA ricalcano sostanzialmente gli artt. 12, 13 e 14 della Direttiva 2000/31/CE[334].

Il DSA, oltre a ribadire l'assenza, in capo ai *provider*, di un obbligo generale di sorveglianza sui contenuti trasmessi o memorizzati, né devono attivamente ricercare elementi indice di attività illecite, ai considerando 21 e 22 precisa che un prestatore può usufruire dell'esenzione da responsabilità per i servizi di semplice trasmissione o memorizzazione temporanea solo se non ha alcun coinvolgimento nei contenuti trasmessi o accessibili tramite il servizio. A tal fine, è essenziale che il prestatore non alteri le informazioni trasmesse o rese accessibili. Tuttavia, sono ammesse modifiche di natura tecnica effettuate durante la trasmissione o l'accesso, purché non compromettano l'integrità dei dati.

Per quanto riguarda i servizi di memorizzazione, l'esenzione si applica solo se il prestatore interviene tempestivamente per rimuovere o bloccare l'accesso a contenuti o attività illecite non appena ne abbia effettiva conoscenza o consapevolezza[335].

Costituisce, invece, una novità l'introduzione del c.d. "principio del Buon Samaritano". L'art. 7 del Regolamento stabilisce che gli intermediari non perdono automaticamente il regime di esenzione di responsabilità previsto dagli artt. 4, 5, 6 del DSA, solo perché, agendo in buona fede e con diligenza, svolgono indagini volontarie o adottano misure per individuare e rimuovere contenuti illegali. Lo stesso vale per le azioni intraprese per rispettare gli obblighi previsti dal diritto

---

[332] Così CEDROLA, *La responsabilità penale dell'*Internet Service Provider *(ISP)*, in *Ius in It.*, 2018, 3 ss.
[333] In tal senso MOROTTI, *Luci e ombre delle piattaforme di* crowdfunding donation, in *Pers. mer.*, 2024, 4, 1314.
[334] V. VICINANZA, *La responsabilità delle piattaforme*, cit., 10.
[335] Così DI CERBO, *La tutela dell'identità nell'ambiente digitale alla luce delle norme europee*, in *EJPLT*, 2023, 2, 263.

dell'Unione o dalle normative nazionali che vi si conformano, incluso quanto stabilito dal DSA[336].

L'art. 7 è stato pensato per incoraggiare le piattaforme ad agire in modo proattivo. Tuttavia, se tali interventi vengono effettuati senza la dovuta attenzione e portano alla conoscenza di elementi che rendono evidente l'illegalità di un contenuto o di un'attività, l'immunità può venire meno[337].

2.8. La responsabilità degli *Internet Service Provider* in materia di dati personali: due approcci giurisprudenziali

Negli ultimi anni, la giurisprudenza europea e italiana ha affrontato in più occasioni il tema della responsabilità degli *Internet Service Provider*, offrendo spesso interpretazioni diverse. I Tribunali, caso per caso, valutano se questi soggetti possono essere considerati responsabili per ciò che viene pubblicato dagli utenti.

In questo paragrafo si intendono esaminare due casi giurisprudenziali che hanno affrontato il tema della responsabilità degli ISP relativamente alla tutela dei dati personali, giungendo in sostanza a conclusioni giuridiche opposte.

Nel primo caso, la Corte di Cassazione ha escluso la responsabilità di Google per contenuti pubblicati da terzi su una sua piattaforma; nel secondo, deciso dalla Corte di Giustizia dell'Unione europea, Google è stato invece ritenuto responsabile per non aver rimosso riferimenti a dati personali presenti sui propri *server*, violando così un obbligo di cancellazione[338].

La prima questione, nota come "caso Google-ViviDown", ha avuto origine da un'accusa rivolta a Google da parte di un'associazione impegnata nella tutela delle persone con autismo.

Ripercorrendo i fatti, l'8 settembre 2006 sulla piattaforma Google-Video veniva caricato un video che ritraeva uno studente con evidenti disabilità mentre subiva aggressioni fisiche e offese verbali da parte di alcuni compagni.

Inoltre, nel video veniva menzionata l'associazione italiana impegnata nella ricerca scientifica e nella tutela delle persone con sindrome di Down.

---

[336] Art. 7, Reg. (UE) 2022/2065.
[337] Cfr. CAGGIANO, *La proposta di* Digital Service Act, cit., 18.
[338] V. NOTARI, *La controversa responsabilità dell'*Internet Service Provider *in materia di* privacy *nella giurisprudenza europea e interna: il caso Google*, in *Amm. camm.*, 2016, 1 s.

Il video offensivo, sorprendentemente, riuscì a diventare il più visualizzato nella categoria "video divertenti" di Google-Video. Solo a distanza di due mesi dalla pubblicazione del video, a seguito di una segnalazione da parte di un cittadino indignato e dell'intervento della polizia postale italiana, Google procedette infine alla sua rimozione.

Dopo la pubblicazione del video, si aprirono tre procedimenti distinti: il primo riguardava gli studenti autori del filmato e responsabili del suo caricamento; il secondo coinvolgeva l'insegnante e l'istituto scolastico per non aver impedito l'accaduto; il terzo procedimento, oggetto di questa analisi, era rivolto contro il Gruppo Google, la sua filiale italiana (Google Italy s.r.l.) e quattro suoi dirigenti.

A questi ultimi la Procura della Repubblica di Milano contestava due reati: il concorso nella diffamazione dell'Associazione ViviDown e del ragazzo disabile e la mancata correttezza nel trattamento dei dati personali di quest'ultimo[339].

Così, nel 2010, il giudice di primo grado si pronunciava condannando i dirigenti della piattaforma alla reclusione per violazione della normativa sulla protezione dei dati personali. Gli stessi, tuttavia, furono assolti dall'accusa di diffamazione[340].

Per quanto riguarda il primo capo d'imputazione, relativo al reato di diffamazione, l'accusa aveva attribuito la responsabilità non solo agli studenti che avevano realizzato e caricato il video, ma anche ai dirigenti di Google, sostenendo che vi fosse un'omissione rilevante ai sensi dell'art. 40 c.p.

Infatti, la ricostruzione fattuale-giuridica secondo l'accusa, Google avrebbe potuto impedire la diffamazione se si fosse conformata alle disposizioni del Codice della *privacy*.

Tuttavia, il giudice, pur riconoscendo il contenuto diffamatorio del video, ha escluso la responsabilità della società, rilevando che la normativa vigente non prevede nessun obbligo generale di controllo preventivo da parte degli ISP.

Nel secondo capo d'accusa, il giudice riconosceva la violazione dell'art. 167 del Codice della privacy, rilevando che il video trattava dati sensibili relativi alla

---

[339] V. GRANDINETTI, *La responsabilità dell'*internet provider *tra* privacy *e diritto d'autore*, in BOMBI, ORIOLES (a cura di), *Nuovi valori dell'italianità nel mondo. Tra identità e imprenditorialità*, Udine, 2011, 142.

[340] Cfr. Tribunale di Milano, sez. IV pen., 12 aprile 2010, n.1972.

salute di un minore e che il consenso al trattamento non era stato né richiesto né ottenuto. Di conseguenza, il giudice riteneva che fossero presenti tutte le condizioni per configurare un trattamento illecito di dati sensibili, imputabile sia agli autori del video sia a Google.

Pur ammettendo che un ISP non ha l'obbligo di sorveglianza generale sui contenuti caricati da terzi, il giudice aveva contestato a Google Italia la mancata fornitura di un'informativa chiara e specifica agli utenti, come previsto dall'art. 13 del Codice della *privacy*.

Inoltre, veniva sottolineato l'elemento soggettivo del dolo, cioè l'intento di trarre profitto dal trattamento dei dati: Google Video, secondo il giudice, non si limitava a ospitare i contenuti, ma li gestiva attivamente a fini commerciali, assumendo così il ruolo di *content provider*.

Per questo motivo, il Tribunale di Milano condannava in primo grado i dirigenti di Google a sei mesi di reclusione per trattamento illecito di dati sensibili[341].

La sentenza di primo grado è stata oggetto di appello davanti alla Corte di Milano[342], la quale modificava la sentenza del Tribunale di Milano assolvendo i dirigenti dall'accusa del trattamento illecito dei dati ai sensi dell'art. 167 del Codice della *privacy*.

Il giudice d'appello aveva criticato l'impostazione seguita dal giudice di primo grado, secondo cui Google avrebbe dovuto avvisare in modo esplicito gli studenti che caricavano il video della necessità di ottenere il consenso scritto della persona ripresa e delle responsabilità penali derivanti dalla mancata acquisizione.

La Corte, infatti, sosteneva che tale obbligo non fosse previsto dal Codice della *privacy*, in particolare dall'art. 13, e che quindi non potesse configurarsi una violazione. Sostiene che l'art. 167 richiede che l'autore del reato agisca violando specifiche disposizione del Codice, ma nessuna di queste impone agli ISP di informare gli utenti sui contenuti della normativa sulla *privacy*. Di conseguenza, la condanna risultava giuridicamente infondata.

---

[341] Sul punto NOTARI, *La controversa responsabilità dell'*Internet Service Provider, cit., 3 ss.
[342] V. Corte d'Appello di Milano, sez. I pen., 21 dicembre 2012, n. 8611.

La Corte, inoltre, escluse che Google avesse un obbligo di sorveglianza preventiva sui contenuti caricati dagli utenti, vista l'enorme quantità di dati che circolano *online*. Un controllo del genere sarebbe stato possibile solo attraverso un sistema di filtraggio preventivo, vietato dalla normativa vigente.

La Corte riconosceva soltanto che, pur ammettendo un ISP più attivo, non si può attribuire loro un obbligo generalizzato di monitoraggio, indipendentemente dal loro grado di intervento.

Infine, la Corte aveva chiarito i rapporti tra la disciplina della *privacy* e quella del commercio elettronico. In particolare, il giudice distingueva in quella sede il ruolo dell'*host provider* (Google Video), l'*uploader* (coloro che caricano i contenuti) e i soggetti terzi i cui dati personali sono presenti nel video. Secondo la Corte, Google Video non era il titolare dei dati contenuti nel video oggetto del procedimento. Pertanto, il rapporto tra il provider e le persone i cui dati erano trattati nei contenuti caricati dagli utenti doveva essere regolato dalla normativa sul commercio elettronico, che esclude la responsabilità dei provider per i contenuti caricati dagli utenti, salvo conoscenza effettiva.

Si delineava così, dunque, una doppia relazione giuridica: da un lato, quella tra l'*host provider* e l'*uploader*, regolata dal Codice della *privacy*, in cui il provider assume il ruolo di responsabile del trattamento dei dati personali dell'*uploader* stesso; dall'altro, quella tra l'*host provider* e i soggetti terzi i cui dati vengono trattati nei contenuti caricati dagli utenti, disciplinata invece dal d.lgs. 70/2003.

Oltre alla mancanza dell'elemento oggettivo del reato, la Corte aveva rilevato anche l'assenza dell'elemento soggettivo, ossia il dolo specifico, poiché non vi era prova che i dirigenti di Google fossero a conoscenza del video e del suo contenuto. Inoltre, non si riteneva dimostrato alcun vantaggio economico derivante dalla pubblicazione del video, anche perché Google Video era un servizio gratuito e il filmato in questione non conteneva pubblicità associata[343].

La vicenda veniva definitivamente conclusa con la sentenza n. 5107 del 2014, con cui la Corte di Cassazione confermava l'assoluzione dei dirigenti di Google per l'accusa di trattamento illecito di dati personali.

[343] Così NOTARI, *La controversa responsabilità dell'*Internet Service Provider, cit., 6 s.

Con tale decisione sono stati altresì sanciti dei principi fondamentali in materia di responsabilità degli ISP. La Suprema Corte escluse la responsabilità di Google per il trattamento illecito dei dati, affermando che solo il titolare del trattamento — cioè, chi ha potere decisionale sui dati — può essere soggetto a sanzioni. Google Video, in quanto *host provider*, non aveva questo ruolo e godeva delle limitazioni di responsabilità previste dal d.lgs. 70/2003, che non impone un obbligo generale di controllo sui contenuti. Inoltre, Google aveva adempiuto ai propri doveri segnalando tempestivamente il video alle autorità competenti. L'eventuale illecito, quindi, era da attribuire esclusivamente agli utenti che avevano caricato il contenuto.

La Corte di Cassazione non ha riconosciuta alcuna incompatibilità tra la normativa sul commercio elettronico e quella sulla *privacy*, contrariamente dal ricorrente che si era basato sull'art. 1 del d.lgs. 70/2003.

I giudici di legittimità, inoltre, avevano respinto la qualificazione di Google Video come *host* attivo: anche se Google svolgeva un ruolo attivo nel fornire la piattaforma, non si trattava di un *content provider*, cioè di un soggetto che crea o controlla direttamente i contenuti e che, per questo, può essere ritenuto responsabile per eventuali illeciti.

Google, in quel contesto, si limitava a offrire uno spazio per il caricamento dei video da parte degli utenti, senza intervenire sul contenuto, e pertanto continuava a rientrare nella categoria degli host provider, beneficiando delle limitazioni di responsabilità previste dagli articoli 16 e 17 del D.lgs. 70/2003.

Le tre argomentazioni sviluppate dalla Corte di Cassazione sono considerate principi fondamentali in materia di responsabilità degli *Internet Service Provider*. Sulla base delle stesse è stato concluso definitivamente il caso Google-ViviDown ma, allo stesso tempo, sono diventate un punto di riferimento essenziale per definire l'equilibrio tra libertà di espressione, controllo dei contenuti online e protezione dei dati personali e sensibili[344].

Il secondo caso giurisprudenziale, il "caso Google-Spain", deciso dalla Corte di Giustizia dell'Unione europea, ha condotto a una decisione completamente diversa rispetto a quella adottata dalla magistratura italiana appena analizzata.

---

[344] V. NOTARI, *La controversa responsabilità dell'*Internet Service Provider, cit., 8 ss.

La vicenda iniziava nel 2010, quando un cittadino spagnolo aveva presentato un reclamo all'Agenzia spagnola per la protezione dei dati personali (AEPD) contro il quotidiano *online* "La Vanguardia", Google Spain e Google Inc.

Il ricorrente contestava il fatto che, tramite il motore di ricerca Google, fosse possibile accedere a *link* che rimandavano a pagine del giornale contenenti un annuncio del 1998 relativo alla vendita all'asta di alcuni suoi immobili, disposta a seguito di un pignoramento per debiti previdenziali. Poiché il debito era stato da tempo saldato, il ricorrente chiedeva che il quotidiano eliminasse o modificasse quelle pagine e che Google rimuovesse o rendesse non accessibili i suoi dati personali dai risultati di ricerca.

L'AEPD respingeva il reclamo nei confronti de "La Vanguardia", ritenendo legittima la pubblicazione dei dati, avvenuta su disposizione del Ministero del Lavoro per garantire la trasparenza della procedura di vendita.

Tuttavia, l'AEPD accoglieva il reclamo contro Google Spain e Google Inc., sostenendo che i motori di ricerca potessero essere obbligati a rimuovere o limitare l'accesso a dati personali qualora la loro diffusione risultasse lesiva del diritto fondamentale alla protezione dei dati.

Google Spain e Google Inc. impugnarono la decisione presentando due ricorsi distinti, poi riuniti, dinanzi all'*Audiencia Nacional*. Quest'ultima sospese il procedimento e sottopose la questione alla Corte di Giustizia dell'Unione europea tramite rinvio pregiudiziale, chiedendo di chiarire quali obblighi gravassero sui motori di ricerca quando indicizzano e rendono accessibili informazioni personali pubblicate da terzi, alla luce della Direttiva 95/46/CE e del diritto alla protezione dei dati personali sancito dall'art. 8 della Carta di Nizza[345].

L'*Audiencia Nacional* ha presentato una serie di questioni pregiudiziali, tra cui la questione relativa alla natura dell'attività del motore di ricerca e sulla sua qualifica giuridica. La Corte di Giustizia ha stabilito che, secondo l'art. 2 della Direttiva *privacy*, le operazioni di indicizzazione e memorizzazione svolte da Google costituiscono a tutti gli effetti un trattamento di dati. Di conseguenza, Google Spain è stato considerato responsabile del trattamento, distinto da quello

[345] V. FLOR, *Dalla* data retention *al diritto all'oblio. Dalle paure Orwelliane alla recente giurisprudenza della Corte di Giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive* de jure condendo, *in Dir. inf.*, 2014, 4, 227 ss.

effettuato dal sito del quotidiano, poiché agiva autonomamente nella gestione dei dati indicizzati.

La CGUE ha altresì affrontato le questioni relative all'estensione della responsabilità dei motori di ricerca.

A differenza della posizione assunta dalla Corte di Cassazione nel caso "Google-Vividown", la CGUE ha riconosciuto che anche Google può essere ritenuto responsabile per i contenuti pubblicati da terzi. In particolare, ha affermato che, il gestore del motore di ricerca è tenuto a rimuovere dai risultati i *link* che rimandano a pagine contenenti informazioni personali, anche se tali pagine non sono state eliminate e la loro pubblicazione è legittima[346].

[346] Cfr. NOTARI, *La controversa responsabilità dell'*Internet Service Provider, cit., 11 ss.

CAPITOLO III

L'IPS NEGLI USA: UN'ANALISI NORMATIVA E GIURISPRUDENZIALE

3.1. Le responsabilità dei *Provider* secondo la normativa statunitense

Sia negli Stati Uniti che in Europa, le prime regole dello spazio digitale sono state concepite con un approccio prevalentemente improntato al liberalismo, ove la priorità era incentivare la libera circolazione delle informazioni e sostenere lo sviluppo dei servizi digitali. L'obiettivo principale era eliminare le barriere che ostacolavano lo sviluppo del commercio elettronico e favorire la diffusione della società dell'informazione.

Sul punto, negli Stati Uniti, il Congresso ha introdotto nel 1996 la celebre sezione 230 del *Title 47* dello *U.S. Code*, che ha escluso gli ISP da qualsiasi responsabilità per i contenuti pubblicati da terzi[347].

Tuttavia, negli ultimi anni l'interesse si è progressivamente evoluto, passando dalla semplice promozione della libertà di navigazione *online* all'adozione di misure normative volte a proteggere gli utenti digitali[348].

A riguardo, si osservano significative differenze tra l'approccio statunitense e l'approccio europeo per plurimi ordini di motivi. In particolare, la differente visione è dovuta sia alle diverse tradizioni giuridiche – più liberista negli Stati Uniti e più garantista in Europa – sia a considerazioni geopolitiche. Infatti, la maggior parte delle aziende – tra cui Apple, Microsoft, Alphabet, Amazon, Nvidia, Meta e Tesla – con la maggiore capitalizzazione di mercato al mondo appartengono al settore tecnologico e sono tutte statunitensi; pertanto, è facile intuire perché gli USA tendano a difendere la loro storica supremazia tecnologica. L'Unione europea, invece, si confronta ancora con il problema della dipendenza e della scarsa sovranità tecnologica.

---

[347] Sul tema v. infra § 3.2.1.

[348] Sul punto FABIANO, *Il liberal-protezionismo digitale statunitense fra difesa della* leadership *nel mercato tecnologico e sicurezza nazionale*, in *DPCE online*, 2023, 3, 2335 s.

Queste differenze si riflettono inevitabilmente nelle scelte politiche dei due Paesi: gli Stati Uniti puntano soprattutto sulle opportunità offerte dalla digitalizzazione, privilegiando l'obiettivo strategico di conservare una posizione di *leadership* globale in ambito tecnologico, considerata fondamentale per l'espansione economica e il predominio militare. Al contrario, l'Unione europea sembra orientata a promuovere un modello globale basato sull'uso etico delle tecnologie, adottando un approccio improntato sul principio di precauzione e incentrato sulla tutela dei diritti fondamentali[349].

Dunque, l'esperienza americana si è contraddistinta per un approccio fortemente liberale nella regolamentazione di Internet. Questa visione ha trovato conferma anche nella giurisprudenza costituzionale statunitense, che ha dichiarato incostituzionali alcune disposizioni del *Telecommunication Act* del 1996 – in particolare quelle previste dal *Communications Decency Act* – per violazione del Primo Emendamento[350], nella parte in cui prevedevano sanzioni penali e amministrative per la diffusione tramite Internet di contenuti osceni e offensivi della decenza a minorenni[351].

Inoltre, l'importanza attribuita alla libertà di espressione ha spinto i giudici statunitensi, nell'interpretazione della Sezione 230 del *Communications Decency Act*, a garantire una tutela particolarmente ampia ai *provider* che ospitano contenuti accessibili al pubblico, anche quando la diffusione di tali contenuti costituisca un comportamento illecito da parte dell'utente che li ha caricati in Rete. Infatti, limitare l'immunità dei fornitori comporterebbe il rischio di una censura che potrebbe comprimere la libertà di espressione, poiché gli ISP, per timore di eventuali sanzioni, sarebbero indotti a rimuovere anche contenuti leciti, temendo di essere ritenuti responsabili[352].

---

[349] V. FABIANO, *Il liberal-protezionismo digitale statunitense*, cit., 2338 s.

[350] Primo Emendamento, Cost. USA 1791: «Il Congresso non potrà emanare leggi per il riconoscimento di una religione o per proibirne il libero culto, o per limitare la libertà di parola o di stampa o il diritto dei cittadini di riunirsi in forma pacifica e d'inviare petizioni al governo per la riparazione dei torti subiti».

[351] Così PERDONÒ, *Le responsabilità penali collegate all'uso di Internet fra comparazione e prospettive di riforma*, in *Dir. Inf.*, 2007, 335.

[352] In argomento SARTOR, VIOLA DE AZEVEDO CUNHA, *Il caso Google e i rapporti regolatori USA/EU*, in *Dir. inf.*, 2014, 660.

Con il CDA, il legislatore statunitense ha inteso tutelare gli ISP, escludendoli da responsabilità civili derivanti dalla pubblicazione *online* di contenuti illeciti da parte degli utenti. Nello specifico, la Sezione 230 del CDA ha introdotto una vera e propria esenzione da responsabilità civile per i *provider*, stabilendo al paragrafo (c) che «nessun provider o utente di un servizio informatico interattivo può essere considerato come editore o autore di informazioni fornite da terzi»[353].

Questa disposizione richiama, in parte, quanto previsto dalla Direttiva 2000/31/CE e, oggi, dal *Digital Services Act*, poiché nell'ordinamento dell'Unione delinea un regime di irresponsabilità condizionata e orizzontale, applicabile tanto in sede civile quanto in sede penale; al contrario, il CDA statunitense si occupa esclusivamente della responsabilità civile, senza affrontare la questione della responsabilità penale dei *provider* per eventuali reati commessi dagli utenti. Infatti, l'inapplicabilità del CDA in materia penale è espressamente prevista alla Sezione 230 (e)[354], confermando così che l'esenzione di responsabilità prevista per gli ISP riguarda esclusivamente l'ambito civile e non quello penale[355].

Rispetto al confronto tra l'ipotesi di totale deresponsabilizzazione del *provider* e quella di una sua responsabilizzazione eccessiva, l'applicazione del diritto statunitense ha mostrato un andamento oscillante tra i diversi modelli di imputazione. Passando, in particolare, dalla *vicarious liability* – cioè la responsabilità per fatto altrui – alla *strict liability* – ossia la responsabilità oggettiva – fino a giungere al modello del *contributory infringement*, il quale si fonda sull'effettivo contributo fornito dal *provider* alla realizzazione dell'evento dannoso[356].

3.1.1. *Direct liability*

Nel sistema giuridico statunitense, un ISP può essere ritenuto responsabile direttamente, per violazioni di legge, oppure in forma secondaria, per atto o

[353] Sezione 230 (c)(1) CDA.
[354] Sezione 230 (e)(1) CDA: «Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute».
[355] In tal senso ACCINNI, *Profili di responsabilità penale dell'*hosting provider *"attivo"*, in Arch. Pen., 2017, 2, 16.
[356] Cfr. PERDONÒ, *Le responsabilità penali collegate all'uso di Internet*, cit., 334.

omissione di terzi. Questa forma di responsabilità secondaria include la *contributory liability*, intesa quale responsabilità per aver contribuito nella commissione dell'illecito, e la *vicarious liability*, ovverosia responsabilità per l'azione di un terzo.

La responsabilità diretta (*direct liability*) si configura quando il *provider* compie personalmente la condotta illecita e non occorre dimostrare l'intenzione o la consapevolezza da parte dello stesso di aver realizzato la condotta illecita (*mens rea*)[357].

Sul punto, nel 1993, nella decisione *Playboy Enterprises, Inc. v. Frena*[358] – considerato il caso giuridico di riferimento per questo paradigma di responsabilità – è stata riconosciuta un'ipotesi di responsabilità diretta del *provider*.

Nel caso di specie, è stata contestata la diffusione su un BBS (*bulletin board systems*[359]) di fotografie appartenenti a Playboy Inc., e il gestore del BBS è stato ritenuto responsabile a titolo di responsabilità diretta per la violazione del *copyright*.

Tuttavia, questa forma di responsabilità non è stata valutata in base ad un comportamento attivo o intenzionale da parte dell'ISP, ma – come si evince chiaramente dalla motivazione della sentenza[360] – la responsabilità è stata attribuita al gestore per aver "ospitato e permesso", inconsapevolmente, la pubblicazione *online* di immagini protette dal diritto d'autore, caricate dagli utenti della piattaforma.

In questo contesto, l'interpretazione adottata dai Giudici appare forzata: viene valutata come responsabilità diretta una situazione in cui il *provider* è

---

[357] Così BHATTACHARYA, ROY, *Contributory Liability Vis-a-Vis Strict Liability: Analyzing World Trends in ISP Liability Regime with Respect to the Indian Position*, in *GNLU L. Rev.*, 2012, 79 e 81 s.

[358] V. Playboy v. Frena, 839 F. supp. 1552 (M.D. Flo. 1993).

[359] «Le BBS erano sistemi a cui diversi utenti potevano collegarsi usando computer e modem per accedere, grazie a un apposito software, a diversi servizi, soprattutto scambi di messaggi e di programmi» Cfr. NOSENGO, voce *Telematica*, in *Enc. dei ragazzi Treccani*, Roma, 2006.

[360] Cfr. Playboy v. Frena, 839 F. supp. 1552 (M.D. Flo. 1993) «There is irrefutable evidence of direct copyright infringement in this case. It does not matter that Defendant Frena may have been unaware of the copyright infringement. Intent to infringe is not needed to find copyright infringement. Intent or knowledge is not an element of infringement, and thus even an innocent infringer is liable for infringement; rather, innocence is significant to a trial court when it fixes statutory damages, which is a remedy equitable in nature».

coinvolto solo per il fatto che contenuti illeciti siano stati pubblicati sulla sua piattaforma da terzi.

Di conseguenza, così operando, si finisce per imporre al fornitore un obbligo di controllo sostanzialmente irrealizzabile sui contenuti generati dagli utenti, trasformando, di fatto, la responsabilità diretta in una forma di responsabilità oggettiva[361].

Alla luce di queste considerazioni, i tribunali e le Corti che si sono successivamente interessati della responsabilità degli *Internet Service Provider* hanno scelto di non aderire a questo precedente.

Tra tutti, il caso *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*[362] rappresenta un esempio significativo in cui la Corte distrettuale degli Stati Uniti per il distretto settentrionale della California ha escluso la possibilità di attribuire una responsabilità diretta all'ISP. In particolare, nel caso di specie i Giudici hanno evidenziato che le copie del materiale protetto dal diritto d'autore generate da *Netcom* erano indispensabili per il corretto funzionamento della rete e che venivano prodotte in modo automatico[363].

Di conseguenza, seguendo questa interpretazione, i fornitori di servizi *online* non dovrebbero essere considerati direttamente responsabili per le violazioni commesse dai loro utenti, considerato che, affinché si possa parlare di *direct liability*, è necessario che vi sia un nesso di causalità, cioè un'azione concreta del *provider*. I Giudici, sul punto, hanno precisato che questo nesso causale manca del tutto quando il *provider* si limita a offrire l'accesso al cyberspazio o a mettere a disposizione una piattaforma pubblica per lo scambio di informazioni e opinioni parte di cittadini.

In questi casi, infatti, coerentemente con la dottrina e la giurisprudenza prevalente, risulta più appropriato fare riferimento a un modello basato sulla *contributory liability*, che offre un'impostazione giuridica più adatta per dirimere

---

[361] Sul punto BUGIOLACCHI, *Principi e questioni aperte in materia di responsabilità extracontrattuale dell'*Internet provider*. Una sintesi di diritto comparato*, in *Dir. inf.*, 2000, 838.
[362] V. *Religious Tech. Center v. Netcom On-Line Comm.*, 907 F. Supp. 1361 (N.D. Cal. 1995).
[363] Così IMPERADORI, *La responsabilità dell'*Internet Service Provider *per violazione del diritto d'autore: un'analisi comparata*, in *Lawtech*, 2014, 11.

le criticità relative a questo genere di condotte *online*[364]. Da queste premesse muove l'analisi delle responsabilità contributiva, oggetto del paragrafo seguente.

3.1.2. *Contributory liability*

Le teorie della responsabilità secondaria – ossia la *contributory* e la *vicarious infringement* – originariamente sviluppate per situazioni interessate dal mondo *offline*, sono state successivamente estese anche agli ISP.

Queste teorie giuridiche sono state sviluppate e affinate nel tempo dai Tribunali americani e, in particolare, nel caso *Gershwin Publishing Corp. v. Columbia Artists Management, Inc.*[365]. *In questa decisione, infatti, la Corte d'appello degli Stati Uniti per il secondo circuito ha delineato i confini della responsabilità contributiva, precisando che un soggetto può essere ritenuto responsabile se, consapevole dell'attività illecita compiuta da terzi, partecipa alla condotta altrui inducendola, causandola o contribuendo significativamente alla sua realizzazione*[366].

Secondo questa concezione, in base al principio della responsabilità contributiva, affinché un ISP possa essere ritenuto responsabile devono essere soddisfatte tre condizioni fondamentali. Anzitutto, è necessario che si sia verificata una *direct infringement* da parte di un soggetto principale. Inoltre, il *provider* deve essere a conoscenza o, quantomeno, avrebbe dovuto essere a conoscenza di tale violazione. Infine, l'ISP deve aver fornito un contributo significativo alla realizzazione dell'illecito[367].

I criteri della *knowledge* e del *material contribution* permettono, quindi, di delineare tre distinte situazioni in cui un ISP può essere ritenuto responsabile per *contributory liability*, in relazione a un illecito commesso da uno dei suoi utenti.

---

[364] V. BERNTHOL, *Copyright Infringement in Cyberspace: On-line Service Provider Liability on the Cyberfrontier*, in *Intell. Prop. L. Bull.*, 1997, 21.
[365] Cfr. *Gershwin Publishing Corporation, Plaintiff-appellee, v. Columbia Artists Management, Inc.*, Defendant-appellant, Andcommunity Concerts, Inc., Defendant, 443 F.2d 1159 (2d Cir. 1971).
[366] In argomento LADEIA, *The Internet Service Provider Secondary Liability: A Comparative Analysis of Brazilian and United States Legislation and Case Law*, in *J. Int'l Media & Ent. L.*, 2016, 2, 201.
[367] In tal senso HUA, *Establishing Certainty of Internet Service Provider Liability and Safe Harbor Regulation*, in *NTU L. Rev.*, 2014, 1, 14.

Nel primo caso, si potrebbe ipotizzare che la sola fornitura del servizio Internet da parte dell'ISP configuri una forma di responsabilità contributiva, in quanto, avendo numerosi utenti, è probabile che alcuni di essi commettano violazioni. Di conseguenza, si potrebbe sostenere che il *provider* sia consapevole del fatto che il proprio servizio viene impiegato anche per attività illecite e che tale offerta rappresenti un contributo materiale.

Tuttavia, sul punto, secondo l'orientamento espresso dalla Corte Suprema[368], il grado di consapevolezza implicito nella mera erogazione del servizio non è sufficiente a soddisfare il requisito della conoscenza necessario per attribuire responsabilità contributiva, ma occorre una conoscenza effettiva delle violazioni, nonché un contributo materiale alla loro realizzazione.

Nel secondo caso, l'ISP viene informato o acquisisce prove certe che un utente specifico stia commettendo una violazione. Questo può accadere, ad esempio, quando il titolare dei diritti fornisce una documentazione chiara e inequivocabile relativa a una violazione su una pagina web precisa, oppure quando l'ISP, nel corso di verifiche tecniche – come può essere l'analisi di un traffico anomalo – scopre che il problema è dovuto alla diffusione non autorizzata di contenuti protetti. In tali circostanze, la consapevolezza dell'illecito è evidente, e, secondo l'orientamento giurisprudenziale prevalente[369], continuare a fornire il servizio equivale a un contributo materiale.

Nella terza ipotesi può accadere che che l'ISP riceva segnalazioni che indicano (ma non provano in modo definitivo) che un abbonato stia commettendo una violazione o, alternativamente, l'ISP potrebbe indagare su un reclamo e scoprire che l'utente ha utilizzato contenuti di pubblico dominio, ha evitato la violazione o ha agito nell'uso legittimo. In questi casi, l'ISP potrebbe sostenere che, in assenza di una conoscenza effettiva dell'illecito, non si possa configurare una responsabilità contributiva. Al contrario, i titolari dei contenuti potrebbero obiettare, però, che questa interpretazione rischia di incentivare gli ISP a ignorare consapevolmente le

---

[368] V. *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).
[369] Cfr. *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 264 (9th Cir. 1996); *Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc.*, 907 F. Supp. 1361, 1375 (N.D. Cal. 1995); *Screen Gems-Columbia Music, Inc. v. Mark-Fi Records, Inc., 256 F. Supp. 399, 404-05 (S.D.N.Y. 1966)*.

violazioni commesse dagli utenti non perfettamente dettagliate. Di conseguenza, secondo questa visione, anche informazioni che generano un sospetto ragionevole di violazione dovrebbero essere considerate sufficienti per attivare la responsabilità del *provider*. Altrimenti, pretendere prove più evidenti darebbe agli ISP la possibilità di trascurare tutte le segnalazioni ad eccezione di quelle estremamente precise e corredate da documentazione completa[370].

3.1.3. *Vicarious liability*

La teoria della *vicarious liability* è una forma di responsabilità indiretta sviluppata nella dottrina di *common law* – insieme alla teoria della *contributory liability* – per contrastare le diffuse violazioni poste in essere dagli utenti finali nell'ambito dell'utilizzo di opere protette da copyright, considerando che la normativa sul diritto d'autore emanata dal Congresso non prevede che un soggetto possa essere ritenuto responsabile per le violazioni compiute da altri[371].

Il paradigma della responsabilità vicaria si configura quando il soggetto convenuto trae vantaggio dalla condotta illecita e intrattiene con l'autore della violazione un rapporto talmente stretto da consentire alla legge di assimilarli e trattarli come se fossero sullo stesso piano.

Questo modello segue il principio del *respondeat superior*, secondo cui il datore di lavoro può essere ritenuto responsabile per gli atti illeciti compiuti dai propri dipendenti. Questa impostazione costituisce il fondamento della normativa statunitense in materia di marchi e diritto d'autore ed è stata introdotta dalla giurisprudenza nel noto caso *Shapiro, Bernstein and Co. v. H.L. Green Co.*[372]

È possibile, dunque, attribuire responsabilità a un soggetto diverso dall'autore materiale dell'illecito, come il *provider*, quando da un lato possiede il potere e la facoltà di controllare l'attività realizzata dell'agente che ha commesso la violazione e, dall'altro, è presente un interesse economico connesso all'illecito all'interno del rapporto che li lega. Ne consegue che tale forma di responsabilità

---

[370] In argomento YEN, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, in *Geo. L.J.*, 2000, 1873 ss.
[371] Ai sensi del 17 U.S.C. § 501 (a), la responsabilità sorge solo a carico della parte che viola direttamente i diritti esclusivi del titolare del diritto d'autore.
[372] V. *Shapiro, Bernstein & Co. v. H. L. Green Co.*, 316 F.2d 304, 307 (2d Cir. 1963).

può essere riconosciuta anche in assenza di una consapevolezza diretta da parte del *provider* riguardo all'attività illecita[373].

Sebbene questo paradigma di responsabilità richieda generalmente uno standard probatorio più rigoroso rispetto alla *contributory liability*, talvolta – quando mancano prove chiare o complete della consapevolezza dell'illecito – la responsabilità vicaria può rappresentare l'unica base giuridica concretamente applicabile[374].

Con riferimento agli ISP, affinché possa configurarsi la responsabilità vicaria vi deve essere la compresenza di tre elementi essenziali. Nello specifico, deve esserci stata una violazione diretta da parte dell'autore principale dell'illecito; l'ISP deve aver tratto un vantaggio economico diretto dall'attività illecita svolta da quest'ultimo; infine, il *provider* deve avere il potere e la capacità di monitorare o esercitare controllo sull'attività svolta dall'autore dell'illecito[375].

Sul concetto di controllo (*control prong*) i Tribunali[376] hanno elaborato due standard concorrenti: il controllo effettivo e il controllo legale.

Il primo implica che il soggetto sia concretamente in grado di distinguere tra comportamenti leciti e illeciti. Pertanto, questo approccio richiede qualcosa in più del semplice potere teorico di interrompere tutte le attività indistintamente, del diritto di bloccare operazioni non direttamente collegate alla violazione o, ancora, della possibilità di intervenire solo dopo che la violazione è evidente.

Al contrario, il controllo legale si basa esclusivamente sulla facoltà contrattuale di limitare o sospendere qualsiasi attività, indipendentemente dalla sua natura. In questo senso, è sufficiente che il soggetto disponga di una capacità tecnica di intervenire sull'infrazione. Pertanto, il controllo viene riconosciuto in ogni rapporto in cui il soggetto abbia un potere tecnico – ad esempio consentendo l'accesso a un prodotto o a un'attività – anche se, nella pratica, risulta difficile distinguere tra comportamenti leciti e illeciti ed eliminare soltanto questi ultimi.

---

[373] In argomento CAMARELLA, *La responsabilità dell'*Internet Service Provider *alla luce della nuova direttiva sul diritto d'autore nel mercato unico digitale*, in *LawTech*, 2020, 63.
[374] Sul punto HIRNING, *Contributory and Vicarious Copyright Infringement in Computer Software*, in *Chi-Kent J. Intell. Prop.*, 2006, 1, 11 s.
[375] Così HUA, *Establishing Certainty of Internet Service Provider Liability*, cit., 14.
[376] Cfr. *Shapiro, Bernstein & Co. v. H. L. Green Co.*, 316 F.2d 304, 307 (2d Cir. 1963); *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 263 (9th Cir. 1996); *Demetriades v. Kaufmann*, 690 F. Supp. 289, 293 (S.D.N.Y. 1988).

Secondo un approccio intermedio, basato sulla deterrenza[377], il requisito del controllo dovrebbe essere inteso in modo restrittivo come la possibilità di esercitare il controllo a costi ragionevoli, collocandosi in una posizione intermedia tra il controllo effettivo e il controllo legale. In questa prospettiva, non è necessario dimostrare che il controllo sia stato effettivamente già esercitato o che sia in atto, ma è sufficiente che il soggetto si trovi in una condizione tale da poter prevenire le violazioni senza sostenere oneri eccessivi.

Nel caso della responsabilità degli ISP, ciò implicherebbe la capacità di distinguere, a costi ragionevoli, i contenuti illeciti da quelli leciti. In questo modo, se il *provider* può scoraggiare le violazioni a costi contenuti, non avrà motivo di adottare misure sproporzionate, anche in assenza di un guadagno economico diretto dai contenuti caricati dagli utenti. Infatti, un controllo eccessivo rischierebbe di compromettere la sua reputazione, mentre un'azione efficace di prevenzione rafforzerebbe l'immagine dell'ISP e potrebbe generare vantaggi economici indiretti, come l'ampliamento della base degli utenti[378].

Il secondo requisito, quello del vantaggio economico, viene interpretato in modi diversi nelle aule dei Tribunali, oscillando tra letture restrittive – come nel caso *Artists Music*[379] – e letture più ampie – come nel caso *Polygram*[380].

Una parte della dottrina[381] ritiene che una lettura restrittiva di questo criterio sia preferibile, poiché riduce il rischio che la responsabilità vicaria produca un'eccessiva deterrenza dei confronti degli ISP.

---

[377] V. SCHWARTZ, *The Hidden and Fundamental Issue of Employer Vicarious Liability,* in *S. Cal. L. Rev.*, 1996, 1756; SYKES, *The Economics of Vicarious Liability*, in *Yale L.J.*, 1984, 1246 ss.

[378] In tal senso WAN, *Monopolistic Gatekeepers' Vicarious Liability for Copyright Infringement*, in *Regent U. L. Rev.*, 2010, 75 s.

[379] Cfr. *Artists Music Inc. v. Reed Publ'g (USA) Inc.*, 31 U.S.P.Q.2d 1623, 1627 (S.D.N.Y. 1994): il giudice ha stabilito che l'organizzatore di una fiera riceveva un compenso fisso dagli espositori in base alla dimensione dello *stand*, indipendentemente dal fatto che venisse riprodotta musica. Pertanto, ha respinto l'idea che la musica fosse determinante per il successo dell'evento, ritenendo che i ricorrenti non avessero dimostrato alcun beneficio economico derivante dalle esecuzioni non autorizzate.

[380] V. *Polygram Int'l Publ'g, Inc. v. Nev./TIG, Inc.*, 855 F. Supp. 1314, 1332 (D. Mass. 1994): il tribunale ha adottato una visione meno restrittiva, riconoscendo che la musica poteva essere uno strumento utile per interagire con i visitatori della fiera. Di conseguenza, se la musica facilita la comunicazione e contribuisce al successo dell'evento, allora può rappresentare un vantaggio finanziario sufficiente a soddisfare il criterio della responsabilità vicaria.

[381] Cfr. HAMDANI*, Who's Liable for Cyberwrongs?*, in *Cornell L. Rev.*, 2002, 947.

Infatti, in linea teorica, gli ISP – che traggono beneficio da ogni contenuto caricato – sono in grado di bilanciare autonomamente costi e benefici di monitoraggio e non avrebbero quindi motivo di esercitare controlli eccessivi.

Tuttavia, nel contesto digitale, gli ISP ricevono costantemente numerose segnalazioni da parte dei titolari dei diritti d'autore e non riescono facilmente a distinguere tra contenuti leciti e illeciti. Di conseguenza, pur traendo vantaggio dalla presenza di nuovi materiali sulle loro piattaforme, è probabile che rinuncino a parte di questi benefici economici diretti per evitare il rischio di pesanti sanzioni legate alla violazione del *copyright*[382].

La teoria della responsabilità vicaria è stata presa in considerazione dalla Corte d'Appello del Nono Circuito degli Stati Uniti nel caso *Napster*[383], in cui il tribunale ha stabilito che *Napster* – un servizio Internet che consentiva ai propri utenti di condividere e conservare file audio digitali[384] – aveva un interesse economico diretto nell'attività illecita, in quanto i suoi guadagni erano strettamente collegati alla presenza di contenuti non autorizzati sulla piattaforma.

La Corte ha rilevato che *Napster* aveva la possibilità di controllare l'accesso al proprio sistema e, almeno in linea teorica, era in grado di identificare i contenuti illeciti grazie alle sue funzionalità di ricerca.

Di conseguenza, si è concluso che *Napster* disponeva sia del potere sia della capacità di monitorare le attività illecite. Pertanto, la Corte ha ritenuto che i fornitori di contenuti avessero buone probabilità di ottenere un risarcimento da *Napster* sulla base della responsabilità vicaria per violazione del *copyright*[385].

3.2. Il *Communications Decency Act* (CDA) del 1996

Negli ultimi anni, Internet è diventato il mezzo di comunicazione con la crescita più rapida e con il potenziale di diffusione più ampio mai registrato.

Diversamente da qualsiasi altra forma di comunicazione, il suo utilizzo e accesso hanno conosciuto uno sviluppo esponenziale. I legislatori, tuttavia, faticano

---

[382] Così WAN, *Monopolistic Gatekeepers' Vicarious Liability*, cit., 76 s.
[383] Cfr. *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).
[384] V. ZEPEDA, *A&M Records, Inc. v. Napster, Inc.*, in *Berkeley Tech. L.J.*, 2002, 72.
[385] In argomento FANCHER, DUNN, *The Trend Toward Limited Internet Service Provider (ISP) Liability for Third Party Copyright Infringement on the Internet: A United States and Global Perspective*, in *Bus. L. Int.*, 2002, 146 s.

a stare al passo con questa evoluzione e fino al 1996 esistevano pochissime norme in grado di regolamentarne l'uso. L'introduzione del *Communications Decency Act* (CDA), infatti, ha segnato un punto di svolta in questo scenario.

Mentre gli altri strumenti di comunicazione celebravano una progressiva riduzione dell'intervento statale, Internet è stato oggetto, per la prima volta in questa occasione, di una regolamentazione federale volta a censurare i contenuti *online*. In particolare, il Titolo V del *Telecommunications Act* del 1996[386] comprende il *Communication Decency Act* (CDA), che impone limitazioni alla diffusione di contenuti osceni o indecenti attraverso la rete *online*.

Il CDA è stato redatto dal senatore James Exon[387], che si è fatto promotore della sua approvazione condannando le minacce legate alla diffusione della pornografia in rete, andando così a rappresentare il primo intervento legislativo volto a regolamentare i contenuti *online* negli Stati Uniti.

Il suo obiettivo dichiarato era proteggere i minori dall'esposizione a materiali osceni e indecenti, cercando di eliminarne la presenza *online*. Sebbene la tutela dei minori da contenuti inappropriati sia sempre stato un obiettivo importante, le modalità con cui il Congresso ha cercato di perseguirla – in particolare criminalizzando la pubblicazione di tali materiali – hanno sollevato non poche controversie e critiche[388].

Quando il senatore Exon ha presentato il CDA, il disegno di legge ha incontrato una forte opposizione da parte di diversi gruppi politici, ciascuno con una visione differente sul grado di regolamentazione da applicare a Internet.

Alcuni senatori, tra cui Patrick Leahy[389], ritenevano che la proposta fosse eccessivamente restrittiva e minacciasse la libertà di espressione. Quest'ultimo, infatti, aveva avanzato una proposta alternativa che prevedeva l'assenza totale di

---

[386] Il *Telecommunications Act* ha modificato il *Communications Act* del 1934, introducendo una significativa deregolamentazione nel settore delle telecomunicazioni. Uno dei suoi principali obiettivi era garantire il c.d. "servizio universale", assicurando che anche i residenti nelle zone rurali potessero accedere ai servizi radiotelevisivi con le stesse condizioni di chi vive nelle aree urbane. Inoltre, la legge ha promosso la concorrenza, obbligando le grandi compagnie televisive e via cavo ad aprire il mercato alle imprese locali più piccole. Queste misure sono state accolte positivamente da chi sostiene una diffusione mediatica più locale e decentralizzata.

[387] James Exton è stato un senatore democratico per lo Stato del Nebraska.

[388] Sul punto MERCIER, *The Communications Decency Act, Congress' First Attempt to Censor Speech over the Internet*, in *Loy. Consumer L. Rev.*, 1997, 3, 274 s.

[389] Patrick Leahy è stato un senatore del Partito Democratico per lo Stato del Vermont.

interventi governativi nel cyberspazio. All'estremo opposto, il senatore Grassley[390] sosteneva che il CDA non fosse abbastanza incisivo nel contrastare la diffusione di contenuti pornografici *online*. Il disegno di legge di Exon si è trovato, quindi, al centro di un acceso dibattito nel Congresso, con posizioni polarizzate su come lo strumento di Internet doveva essere regolamentato.

La versione proposta da Exon includeva alcune difese legali per gli ISP, che, in determinate circostanze espressamente previste dalla legge, avrebbero potuto evitare responsabilità penali. Questo aspetto era particolarmente criticato dal gruppo di Grassley, che riteneva le esenzioni troppo permissive, mentre il gruppo di Leahy si opponeva a qualsiasi forma di regolamentazione da parte del governo.

Al contrario di quanto accaduto al Senato, le discussioni alla Camera sono state meno accese e di breve durata. Di conseguenza, il disegno di legge proposto è stato approvato rapidamente dai suoi membri e successivamente trasmesso al Presidente Clinton, che lo ha promulgato l'8 febbraio 1996.

Le previsioni normative proposte in chiave di tutela dal senatore Exon per tutelare gli ISP[391] sono state pensate per proteggere i *provider* da responsabilità penali in relazione a contenuti non creati direttamente da loro.

Questa idea nasceva dal fatto che secondo il Congresso sarebbe stato praticamente impossibile per un ISP controllare ogni singola immagine caricata quotidianamente sulla rete. Pertanto, salvo che il *provider* risulti coinvolto attivamente nella diffusione di materiale pornografico, non può essere ritenuto responsabile ai sensi del CDA[392].

Tuttavia, il *Communications Decency Act*, sin dalla sua entrata in vigore, ha sollevato diverse questioni di legittimità costituzionale.

La legge, nella sua formulazione, presentava alcuni tratti peculiari e, in particolare, tre rilevanti criticità di natura costituzionale. In primo luogo, la normativa non operava una distinzione chiara tra i concetti giuridici di oscenità e indecenza, trattandoli in modo uniforme; inoltre, la stessa non teneva conto delle caratteristiche peculiari di Internet come mezzo di comunicazione a sé, distinto

[390] Charles Ernest Grassley è un membro del Partito Repubblicano, senatore per lo Stato dell'Iowa.
[391] Sul tema v. infra § 3.2.2.
[392] Cfr. MERCIER, *The Communications Decency Act*, cit., 277 ss.

dagli altri; e infine, quest'ultima utilizzava un linguaggio eccessivamente generico e prevedeva un'applicazione delle sue disposizioni in modo troppo ampio[393].

L'entrata in vigore del CDA ha causato una forte reazione da parte della comunità telematica: numerose organizzazioni impegnate nella difesa delle libertà civili, come l'ACLU[394] e la EFF[395], sostenute anche dalle principali aziende del settore tecnologico, hanno promosso un'azione legale contestando la compatibilità del provvedimento con il Primo Emendamento della Costituzione statunitense[396].

In particolare, i ricorrenti hanno sollevato diverse obiezioni che mettevano in luce l'ambiguità della legge: gli stessi hanno evidenziato come fosse problematico applicare una normativa nazionale, ovverosia quella statunitense, a un mezzo di comunicazione globale come Internet e, inoltre, hanno sottolineato l'assenza di definizioni precise per il concetto di "materiale indecente", evidenziando il rischio di interpretazioni arbitrarie e incerte dell'espressione.

Un altro punto particolarmente controverso riguardava la punizione della trasmissione di contenuti considerati osceni o indecenti, secondo cui veniva equiparata l'indecenza all'illegalità. Questo approccio, secondo i ricorrenti, violava il Primo Emendamento, che protegge la libertà di espressione, compresa quella che può risultare scomoda o provocatoria.

Infine, gli stessi hanno sottolineato la mancanza di considerazione della volontà dell'utente: non veniva riconosciuto il diritto di un individuo adulto di scegliere consapevolmente di accedere a contenuti destinati a un pubblico maturo[397].

Le obiezioni sollevate hanno trovato esplicazione in una delle decisioni più importanti della Corte Suprema in materia di libertà di espressione nel *cyberspace*: la sentenza *Reno v. American Civil Liberties Union* del 1997[398].

---

[393] V. MERCIER, *The Communications Decency Act*, cit., 284.
[394] L'*American Civil Liberties Union* è un'organizzazione non governativa, operante negli Stati Uniti, la cui missione è realizzare la promessa contenuta nella Costituzione e ampliare l'effettiva tutela dei diritti che essa garantisce.
[395] L'*Electronic Frontier Foundation* è la principale organizzazione senza scopo di lucro impegnata nella tutela della privacy digitale, della libertà di espressione e dell'innovazione.
[396] La normativa, dapprima oggetto di ricorso da parte dell'ALCU, è stata successivamente dichiarata incostituzionale dalla Corte Suprema nel caso *Reno v. ACLU* (1997), in quanto ritenuta lesiva del diritto alla libertà di espressione garantito dal Primo Emendamento della Costituzione.
[397] In argomento ZICCARDI, *La libertà di espressione in* Internet *al vaglio della Corte Suprema degli Stati Uniti*, in *Quad cost.*, 1998, 1, 126 s.
[398] V. *Reno v. ACLU*, 521 U.S. 844 (1997).

Questa pronuncia, infatti, ha rappresentato una netta risposta della Corte Suprema al primo tentativo del Governo degli Stati Uniti di disciplinare l'accesso *online* a contenuti non adatti ai minori.

Come detto, con il *Communications Decency Act* il legislatore aveva introdotto restrizioni volte a colpire contenuti considerati indecenti o esplicitamente offensivi, nella convinzione che su Internet fosse impossibile replicare i meccanismi di *zoning*[399] e *age verification*[400] che esistono nel mondo fisico, i quali impediscono ai minori di accedere a materiali vietati.

Tuttavia, la Corte Suprema ha dichiarato incostituzionali queste disposizioni normative poiché emanate in violazione del Primo Emendamento. Come indicato nella pronuncia, le norme del CDA risultavano eccessivamente vaghe e generiche, in contrasto con il principio dello *strict scrutiny*[401]. In sostanza, la Corte ha espresso il principio di diritto secondo cui le restrizioni ai contenuti su Internet possono essere normativamente previste ma devono essere sempre precise, proporzionate e non possono sacrificare la libertà di espressione degli adulti nel tentativo di proteggere i minori e, nel caso di specie, a parere della Corte le restrizioni alla c.d. *free speech* non apparivano giustificate da una reale e proporzionata esigenza di tutela dei minori[402].

3.2.1. Origine e finalità della *Section 230* del CDA

Per comprendere pienamente il significato e l'impatto della *Section* 230 del *Communications Decency Act,* è necessario esaminare il dibattito legislativo sulle comunicazioni digitali sviluppatosi negli anni '90.

Nel corso del tempo la Sezione 230 del CDA è stata definita in vari modi, differenti tra loro: da un lato, è stata definita come «la legge più rilevante per la

---

[399] Le attività di *zoning* consistono nell'imposizione di restrizioni o trattamenti differenziati a specifici soggetti riguardo all'accesso a spazi, contenuti o servizi, basandosi su criteri variabili e non uniformi. Cfr. Lessig, Resnick, *Zoning Speech on the Internet: A Legal and Technical Model*, in *The Berkman Center for Internet & Society Research Publication*, 1999.

[400] Il sistema di *age verification* è progettato per determinare l'età dell'utente che accede a un servizio *online*, con l'obiettivo di impedire ai minori di usufruire di contenuti o funzionalità potenzialmente dannose o non adeguate alla loro fascia d'età.

[401] Il principio dello *strict scrutiny* è uno standard di giudizio utilizzato dalle corti costituzionali, in particolare negli Stati Uniti, per valutare la legittimità di una legge che limita diritti fondamentali o introduce discriminazioni basate su categorie sospette.

[402] Così POLLICINO, *La prospettiva costituzionale sulla libertà di espressione nell'era di* Internet, in *MediaLaws*, 2018, 1, 69 s.

tutela della libertà di espressione su Internet»[403] e «la normativa più determinante per lo sviluppo dell'innovazione *online*»[404]; dall'altro, invece, è stata anche definita come «una sorta di Magna Carta dell'impunità per le imprese»[405].

Tuttavia, dall'analisi dell'*iter* parlamentare che ne ha portato l'approvazione, emerge come la protezione riconosciuta agli intermediari dalla Sezione 230 non sia nata con l'obiettivo primario di rafforzare la libertà di espressione nel contesto digitale, bensì dimostra come la stessa si sia inserita in un disegno normativo di segno opposto, volto a introdurre limitazioni alla circolazione di contenuti *online*.

Il dibattito legislativo che ha portato all'introduzione della Sezione 230 del CDA ha avuto origine nel 1994, con l'intento di evitare – come si è visto – che Internet passasse dall'essere uno strumento di diffusione dell'informazione a diventare prevalentemente un mezzo per la circolazione di contenuti pornografici. In particolare, al fine di tutelare la salute e lo sviluppo dei minori, all'interno della vasta riforma delle telecomunicazioni approvata nel 1996 sono state inserite due disposizioni penali che punivano la pubblicazione *online* di materiali considerati indecenti o esplicitamente offensivi rivolti ai minori.

Il legislatore mirava a realizzare una sorta di c.d. "zonizzazione" (*rectius* pianificazione) degli spazi digitali, creando aree virtuali riservate esclusivamente agli adulti, in modo da evitare che i minori potessero accidentalmente entrare in contatto con contenuti potenzialmente dannosi per il loro sviluppo fisico e mentale.

In questo contesto, caratterizzato da un approccio restrittivo alla regolamentazione della libertà di espressione, che è stata proposta quella che sarebbe poi diventata la Sezione 230 del CDA.

L'approvazione di questa norma si inserisce dunque in un contesto giurisprudenziale piuttosto incerto, se non addirittura ostile, nei confronti degli

---

[403] V. KAMDAR, *CDA 230: The Most Important Law Protecting Internet Speech*, in *Electronic Frontier Found.*, 2012; AMMORI, *The "New" New York Times: Free Speech Lawyering in the age of Google and Twitter*, in *Harv. L. Rev.*, 2014, 8, 2290.

[404] V. GOLDMAN, *Online User Account Termination and 47 U.S.C. § 230 (c)(2)*, in *U.C. Irvine L. Rev.*, 2012, 67; KOSSEFF, *The Gradual Erosion of the Law that Shaped the Internet: Section 230's Evolution over Two Decades*, in *Colum. Sci. & Tech. L. Rev.*, 2016, 1, 1.

[405] V. PASQUALE, *Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power*, *Theoretical Inquiries L.*, 2016, 24, 494.

operatori della rete. Questo clima, in assenza di un intervento, avrebbe potuto ostacolare lo sviluppo del potenziale comunicativo di Internet.

La norma, infatti, è nata come risposta alle difficoltà incontrate dalla giurisprudenza nel gestire i conflitti tra privati generati dall'uso delle infrastrutture digitali, in assenza di una regolamentazione specifica; le differenti decisioni dei Tribunali che si sono susseguite nel corso degli anni sono state percepite come un segnale di allarme preoccupante, prova di un sistema normativo ancora instabile, che rischiava di compromettere la crescita del Web.

Per questi motivi, la formulazione della Sezione 230 è stata profondamente condizionata dalle prime e contrastanti decisioni giurisprudenziali, aventi ad oggetto prevalentemente casi di diffamazione *online* e in cui venivano applicati i principi del diritto civile tradizionale[406].

Il testo della Sezione 230 del CDA, infatti, è stato concepito in risposta a precise esigenze di politica del diritto e, in particolare, quella di costruire un accordo strategico tra gli intermediari e l'ordinamento. In base a questo accordo, agli operatori della rete veniva affidato il compito di favorire la libertà di espressione e contribuire a uno sviluppo equilibrato delle comunicazioni *online*, mentre il legislatore garantiva loro ampie protezioni da responsabilità legali per i contenuti generati dagli utenti[407].

La disposizione contenuta nella Sezione 230, ancora oggi vigente, rappresenta la concreta traduzione dello spirito libertario ispirato al Primo Emendamento, che veniva esaltato con l'avvento di Internet.

In linea con questa impostazione, la norma solleva i fornitori di servizi digitali da qualsiasi responsabilità legata alla moderazione di contenuti potenzialmente diffamatori, sia nel caso in cui decidano di rimuovere un contenuto, sia nel caso in cui scelgano di mantenerlo *online*, non potranno essere ritenuti responsabili, salvo alcune eccezioni specifiche.

---

[406] Nello specifico, si fa riferimento ai procedimenti *Cubby v. CompuServe* (Cfr. *Cubby v. CompuServe*, in *F. Supp.*, 135 - S.D.N.Y. 1992) e *Stratton v. Prodigy* (Cfr. *Stratton v. Prodigy,* in *WL 323710* - N.Y. Sup. 1995) nei quali i tribunali statunitensi hanno dovuto stabilire se fosse opportuno applicare alle condotte diffamatorie avvenute in rete le regole già esistenti per i tradizionali mezzi di comunicazione oppure se fosse necessario elaborare un nuovo insieme di norme specificamente pensato per le caratteristiche uniche della comunicazione digitale.

[407] In argomento PETRUSO, *La responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, Torino, 2019, 3 ss e 9.

Questa tutela, particolarmente favorevole per gli operatori digitali, fonda le proprie radici nell'obiettivo di eliminare le ambiguità nella loro qualificazione giuridica, risolvendo il dilemma che aveva impegnato la giurisprudenza americana nel tentativo di inquadrarli come *distributors* o *publishers*.

La scelta adottata rappresenta, inoltre, un potenziamento delle garanzie già offerte dal Primo Emendamento ed è stata motivata dalla necessità di evitare che pratiche positive di moderazione e controllo dei contenuti da parte dei siti potessero comportare l'applicazione di un regime di responsabilità troppo severo nei confronti di soggetti che, di fatto, non esercitano un controllo diretto sui contenuti pubblicati[408].

Nei primi anni successivi all'entrata in vigore della legge, la giurisprudenza[409] ha messo in luce l'intento originario del Congresso, ossia favorire la libertà di espressione a livello globale, integrarla con il progresso tecnologico e permettere al mercato digitale di svilupparsi liberamente. Questo obiettivo non escludeva l'introduzione di misure di tutela per gli utenti, ma prevedeva al contempo una protezione per i fornitori di servizi, nota come *intermediary immunity*.

Alla luce della citata giurisprudenza[410], era già stato stabilito che una piattaforma non potesse essere ritenuta responsabile per contenuti diffamatori pubblicati da terzi se non era a conoscenza della loro natura offensiva. Tuttavia, la responsabilità può emergere nel momento in cui la piattaforma decide di intervenire sui contenuti, modificandoli o rimuovendo parti ritenute inappropriate.

Il legislatore federale ha armonizzato questi orientamenti giurisprudenziali[411], codificandoli nella Sezione 230 (c) e prevedendo solo tre eccezioni: l'applicazione della legge penale federale, la tutela della proprietà intellettuale e la normativa sulla *privacy* nelle comunicazioni elettroniche[412].

---

[408] In tal senso POLLICINO, *Regolazione e innovazione tecnologica nell'"ordinamento della rete"*, in *AIC*, 2025, 2, 134 s.
[409] Cfr. *Cubby v. CompuServe*, in *F. Supp.*, 135 (S.D.N.Y. 1992); *Stratton v. Prodigy,* in *WL 323710* (N.Y. Sup. 1995).
[410] *Ibid*.
[411] *Ibid*.
[412] Sul punto FERRARI, *L'*executive order *sulla prevenzione della censura* online*: quali effetti sull'autonomia dei* social network*?*, in *DPCE*, 2020, 2, 1150.

Tra queste, la prima eccezione è di particolare importanza sotto il profilo penale. Questa, infatti, consente di perseguire penalmente gli ISP nei casi in cui non si limitino a svolgere un ruolo di semplici intermediari, ma prendano parte attiva a condotte illecite, come la diffusione di materiale pedopornografico, la distribuzione di *malware* o il sostegno a reti di criminalità organizzata *online*.

In tal senso, pur garantendo un ampio margine di immunità in ambito civile, la Sezione 230 lascia aperto un margine di intervento penale, evitando così la creazione di aree in cui la prevenzione e la repressione dei reati informatici risulterebbero compromesse.

3.2.2. Le immunità dei *Provider* secondo il CDA

Il *Communications Decency Act* stabiliva tre principali forme di tutela per gli *Internet Service Provider*.

Nello specifico, il provvedimento prevedeva che gli ISP che offrivano un semplice servizio di accesso alla rete non potevano essere ritenuti responsabili, purché non fossero coinvolti nella creazione dei contenuti trasmessi. In secondo luogo, i datori di lavoro non rispondevano delle azioni compiute dai propri dipendenti, a meno che non avessero approvato esplicitamente tali condotte o le avessero ignorate con negligenza. Infine, il CDA riconosceva una protezione basata sulla buona fede per quei fornitori che si impegnavano attivamente a rispettare le normative vigenti. Però, queste garanzie si applicavano esclusivamente agli ISP e non si estendevano agli utenti[413].

Queste disposizioni, tuttavia, sono state dichiarate parzialmente incostituzionali dalla Corte Suprema[414], in una pronuncia emessa nella seconda metà degli anni ’90. Questa decisione rifletteva il clima di grande ottimismo sulle potenzialità offerte da Internet e si inseriva in un contesto normativo caratterizzato da un orientamento prevalentemente libertario.

Fin da subito, però, la decisione ha suscitato critiche da parte di chi riteneva che la Corte Suprema avesse sopravvalutato la capacità degli utenti di proteggersi

[413] Così MERCIER, *The Communications Decency Act*, cit., 279.
[414] V. *Reno v. ACLU*, 521 U.S. 844 (1997).

autonomamente, scegliendo consapevolmente tra contenuti appropriati e inappropriati.

Inoltre, è apparso evidente fin da subito che la decisione *Reno* fosse coerente con l'impostazione libertaria adottata dal Congresso l'anno precedente, quando è stata introdotta la Sezione 230 del Titolo 47 dello *U.S. Code*. Tale norma stabiliva l'esonero totale di responsabilità per i *provider* rispetto ai contenuti pubblicati da terzi, grazie alla c.d. clausola del *Good Samaritan* (Buon Samaritano).

Emblematica è la sentenza *Zeran v. America Online*[415], con la quale la Corte d'Appello del Quarto Circuito ha chiarito l'ampiezza della protezione offerta dalla Sezione 230, stabilendo che essa si applica anche nei casi in cui il *provider* sia stato informato della presenza di contenuti illeciti sulla propria piattaforma. Questa interpretazione ha esteso ulteriormente l'immunità dei *provider* rispetto a quanto già riconosciuto nel precedente caso *CompuServe*[416]. Infatti, nella decisione *Zeran*, la Corte ha affermato che la Sezione 230 non solo esclude la possibilità di considerare i *provider* come editori, ma impedisce anche di attribuire loro la responsabilità prevista per i distributori di contenuti che rispondono solo se consapevoli della natura illecita del materiale diffuso.

L'ampiezza dell'immunità prevista dalla Sezione 230 è stata ulteriormente confermata da successive pronunce giurisprudenziali statunitensi, le quali hanno stabilito che tale protezione si applica anche quando l'autore dei contenuti diffamatori è legato al *provider* tramite un contratto di collaborazione autonoma[417], oppure nei casi in cui il terzo abbia compiuto un illecito penale evidente[418]. In entrambi gli scenari, la responsabilità del *provider* resta esclusa, a dimostrazione della portata particolarmente estesa della tutela offerta dalla norma[419].

La regolamentazione tradizionale degli intermediari digitali nei paesi occidentali si fonda sul principio di una generale esclusione di responsabilità per i contenuti diffusi da terzi attraverso le loro piattaforme. Questo approccio, adottato negli Stati Uniti, nell'Unione europea e in numerosi altri paesi, si ispira a una

[415] Cfr. *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997).
[416] V. *Cubby v. CompuServe*, in *F. Supp.*, 135 (S.D.N.Y. 1992).
[417] V. *Blumenthal v. Drudge and America Online, Inc.*, 992 F. Supp. 44 (D.C.C. 1998).
[418] Cfr. *Doe v. America Online, Inc.*, No. 97-2587, 1998 WL 712764 (Fla. Ct. App. Oct. 14, 1998).
[419] In argomento FABIANO, *Il liberal-protezionismo digitale statunitense*, cit., 2342 ss.

visione che privilegia la tutela della libertà di espressione, realizzata attraverso l'istituzione del c.d. *safe harbor*.

La normativa statunitense fonda sulla Sezione 230 del CDA, che si articola attorno a due principi chiave. Il primo stabilisce che i fornitori di servizi informatici interattivi non devono essere considerati responsabili come autori – *speaker* – o editori – *publisher* – dei contenuti generati da terzi. Il secondo principio esclude la responsabilità civile per quei fornitori che, agendo in buona fede, decidano volontariamente di limitare l'accesso a materiali ritenuti osceni, indecenti, violenti, offensivi o comunque inappropriati.

La prima parte della Sezione 230, nello specifico, protegge i fornitori da qualsiasi responsabilità diretta o indiretta per i contenuti pubblicati da altri utenti, mentre la seconda, ossia la clausola del Buon Samaritano, rafforza ulteriormente questa immunità, anche nel caso in cui il fornitore eserciti un certo grado di controllo sui contenuti attraverso attività di moderazione. L'intento della norma era quello di promuovere lo sviluppo di Internet come uno spazio aperto e libero, dove chiunque potesse condividere contenuti, garantendo al tempo stesso ai fornitori la possibilità di intervenire responsabilmente per limitare l'accesso a contenuti problematici, favorendo così forme di autoregolazione.

Questa protezione è, inoltre, giustificata dalle difficoltà tecniche legate a un controllo capillare dei contenuti, in quanto il rischio di non riuscire a gestirli efficacemente avrebbe potuto scoraggiare nuovi operatori dal partecipare al mercato digitale e ostacolare l'innovazione.

Si evince pertanto che la Sezione 230 non offre protezione nei casi che riguardano il diritto penale o la proprietà intellettuale, ambiti regolati separatamente – per esempio, le questioni legate al *copyright* sono disciplinate dal *Digital Millennium Copyright Act*, che adotta un approccio più vicino a quello dell'Unione europea. Diversamente, il sistema giuridico europeo prevede un'immunità che si estende a tutte le forme di responsabilità, senza distinzioni tra ambito civile, penale o di altro tipo[420].

[420] Sul punto VICINANZA, *La responsabilità delle piattaforme digitali nei confronti dei contenuti illegali: dal caso* Telegram *al* Digital Services Act, in *Quaderni AISDUE*, 2025, 1, 6 s.

Difatti, la Sezione 230 delinea cinque eccezioni all'immunità dalla stessa prevista. In particolare, un imputato non può invocare tale immunità per ottenere l'archiviazione di un procedimento penale federale, né per opporsi a qualsiasi causa intentata ai sensi delle leggi sulla proprietà intellettuale, delle leggi statali coerenti con la Sezione 230, di talune leggi sulla privacy delle comunicazioni elettroniche o di alcune leggi sul traffico sessuale.

La prima eccezione all'esenzione da responsabilità riguarda «[…] any other Federal criminal statute»[421], ciò significa un imputato in un processo penale federale non può invocare la protezione offerta dalla Sezione 230.

Ad esempio, questa norma non ostacola l'azione penale per la diffusione consapevole di contenuti osceni su Internet, né ha impedito il processo federale contro le società legate a Backpage.com per reati di cospirazione e riciclaggio di denaro[422]. Tuttavia, questa eccezione vale solo per il diritto penale federale, non per quello statale, e la Sezione 230 è stata interpretata come un ostacolo ai procedimenti penali statali che risultino in contrasto con essa. Inoltre, la maggior parte delle corti ha ritenuto che la Sezione 230(e)(1) consentisse esclusivamente azioni penali, escludendo le cause civili basate su violazioni di norme penali federali.

Alcuni ricorrenti hanno sostenuto che, nei casi in cui una legge federale prevede sia sanzioni penali che civili per lo stesso comportamento, impedire le azioni civili in base alla Sezione 230 potrebbe indebolire l'efficacia della normativa penale. Tuttavia, diversi tribunali hanno respinto questa tesi, ribadendo la distinzione tra responsabilità penale e civile e affermando che, menzionando solo le leggi penali nella Sezione 230(e)(1), il Congresso ha inteso escludere le azioni civili dalla deroga all'immunità[423].

3.3. Il *Digital Millennium Copyright Act (*DMCA) del 1998

Il *Digital Millennium Copyright Act* (DMCA) del 1998 nasce dall'esigenza di garantire una tutela efficace ai titolari dei diritti d'autore e si inserisce in un

[421] Sezione 230 (e) (1) CDA.
[422] V. Press Release, U.S. Dep't of Justice, *Backpage's Co-founder and CEO, As Well As Several Backpage-Related Corporate Entities, Enter Guilty Pleas*, Apr. 12, 2018.
[423] In tale senso BRANNON, *Section 230: an overview*, in *Congressional Research Service*, 2024, 26 s.

contesto di progressiva trasformazione dall'ambiente analogico a quello digitale, favorito dalla rapida evoluzione della tecnologia informatica e dai processi di digitalizzazione.

Tale transizione verso un'economia digitale comportava nuove modalità di riproduzione e diffusione delle opere protette da *copyright*, ma portava con sé anche nuove minacce.

Infatti, nel *White Paper*[424] dell'amministrazione del Presidente Clinton veniva sottolineato che la *National Information Infrastructure* (NII)[425] poteva offrire benefici agli autori e ai consumatori, riducendo drasticamente i tempi tra la creazione e la diffusione delle opere. Tuttavia, era sufficiente un singolo caricamento non autorizzato su una piattaforma digitale per provocare danni significativi sul mercato dell'opera, ben più gravi rispetto alle copie isolate nel contesto analogico-cartaceo.

Dunque, il Congresso ha ritenuto il DMCA una misura per affrontare questi rischi emergenti, considerandolo indispensabile per garantire ai titolari dei diritti di sfruttare le potenzialità delle nuove tecnologie e di diffondere le proprie opere con il pubblico, senza dover affrontare continuamente la minaccia della pirateria digitale[426].

In questa prospettiva, il DMCA vieta la creazione e la diffusione di tecnologie, strumenti o servizi che possano essere utilizzati per eludere le protezioni poste a tutela delle opere coperte da *copyright*, e introduce sanzioni più severe per le violazioni del diritto d'autore commesse *online*[427].

In particolare, il DMCA si articola in cinque Titoli (*sections*), ciascuno dedicato a un ambito specifico. Il suo obiettivo dichiarato era duplice: da una parte, rafforzare la tutela dei diritti d'autore nell'ambiente digitale; dall'altra, promuovere

---

[424] Information Infrastructure Task Force, *The Report of the Working Group on Intellectual Property Rights, Intellectual Property and the National Information Infrastructure: The White Paper* (Sept. 1995).

[425] La *National Institute of Standards and Technology* (NIST) definisce la *National Information Infrastructure* (NII) come l'«Interconnessione a livello nazionale di reti di comunicazione, computer, database ed elettronica di consumo che rende disponibili agli utenti enormi quantità di informazioni. Include reti pubbliche e private, Internet, la rete pubblica commutata e le comunicazioni via cavo, wireless e satellitari».

[426] Così JEANNERET, *The Digital Millennium Copyright Act: Preserving the Traditional Copyright Balance*, in *Fordham Intell. Prop., Media & Ent. L.J.*, 2002, 1, 162 s.

[427] V. D'URSO, *I profili informatici nella valutazione della responsabilità dell'*Hosting Provider, in *RIID*, 2021, 1, 83.

lo sviluppo e la diffusione di contenuti protetti da *copyright*, definendo criteri internazionali chiari e condivisi in materia di protezione della proprietà intellettuale.

Il Titolo I introduce modifiche alla normativa sul *copyright* per allinearla agli accordi internazionali stabiliti dalla *World Intellectual Property Organization* (WIPO). Inoltre, in questo Titolo sono incluse le norme contro l'elusione delle misure di protezione, che rafforzano i diritti dei titolari di *copyright*, permettendo loro di limitare l'accesso ai contenuti e di ricorrere a sanzioni civili o penali in caso di violazioni.

Proseguendo, il Titolo II prevede delle "zone franche", note come *safe harbors*, destinate ai fornitori di servizi *online*. Queste disposizioni limitano la loro responsabilità in caso di violazioni del *copyright* legate a specifiche attività, come l'archiviazione di contenuti su richiesta degli utenti, il collegamento a materiali ospitati su altri siti, o il semplice passaggio di dati tra utenti. Tali esenzioni, previste in questa sezione, si affiancano alle garanzie già offerte da altre normative.

Il Titolo III stabilisce, invece, che i fornitori di servizi non sono responsabili per la copia di un *software* effettuata durante l'avvio di un *computer*, qualora tale operazione sia necessaria per interventi di manutenzione o riparazione.

In seguito, il Titolo IV raccoglie norme che riguardano soprattutto i c.d. *webcasters*, cioè fornitori di contenuti in streaming, le biblioteche, gli archivi e l'istruzione a distanza. I *webcasters* sono tenuti a pagare i diritti di licenza alle etichette discografiche per l'utilizzo dei brani.

Le biblioteche e gli archivi, invece, hanno la possibilità di effettuare un numero ristretto di copie, nel rispetto di precise limitazioni.

Inoltre, sono altresì previsti approfondimenti e analisi per sviluppare regolamenti che favoriscano l'espansione dell'istruzione a distanza.

Infine, il Titolo V garantisce una tutela temporanea ai *design* innovativi degli scafi delle imbarcazioni, riconoscendo loro una protezione legale contro la copia non autorizzata[428].

3.3.1. La clausola di sicurezza per gli *ISP*

[428] Sul punto HILTON, *An ethics analysis of the Digital Millennium Copyright Act*, in *Issues in Information System*, 2004, 2, 495 s.

Il *Digital Millennium Copyright Act*, tra le varie disposizioni, si occupa della responsabilità degli *Internet Service Provider* in relazione alla diffusione di materiali che violano le norme a tutela del diritto d'autore.

Al fine di limitare la discrezionalità del giudice nella valutazione della *contributory liability*, la Sezione 512 del *Title* 17 dello *United States Code* – rubricata «Limitations on liability relating to material online»[429] – stabilisce regole di esonero della responsabilità per quei fornitori che si limitano a svolgere un ruolo tecnico di intermediazione tra gli utenti coinvolti nell'illecito, senza avervi preso parte in modo volontario[430].

Tuttavia, la disciplina contenuta nella Sezione 512 costituisce una parziale eccezione rispetto all'impostazione generale del *DMCA*. Mentre quest'ultimo mira a trovare un equilibrio tra il diritto di accesso alle opere e alle informazioni e la protezione del diritto d'autore, nel contesto digitale si è iniziato a tutelare alcuni soggetti potenzialmente responsabili di violazioni nei confronti del diritto d'autore.

In particolare, agli ISP viene riconosciuta una forma di immunità non solo per le infrazioni commesse dagli utenti, ma anche per quelle che potrebbero essere imputate direttamente a loro[431].

Prima dell'entrata in vigore del DMCA, il regime di responsabilità degli ISP per le violazioni del *copyright* commesse dai propri utenti non era definito con chiarezza.

Successivamente, con l'adozione del DMCA, il legislatore ha formalizzato l'orientamento giurisprudenziale prevalente[432] dell'epoca, introducendo una clausola di esonero – il c.d. *Safe Harbor* – che limita la responsabilità degli ISP in specifiche circostanze. Secondo questa norma, un soggetto può essere esonerato dal risarcimento dei danni o dall'obbligo di rispettare ingiunzioni, a condizione che

[429] V. U.S.C, Title 17, Chapter 5, Section 512 – *Limitations on liability relating to material online*.
[430] In argomento DI CIOMMO, *Programmi-filtro e criteri di imputazione/esonero della responsabilità* on-line*. A proposito della sentenza Google/Vivi Down*, in *Dir. inf.*, 2010, 843.
[431] In tal senso PASSAGLIA, *Cenni* sull'Online Copyright Infringement Liability Limitation Act *statunitense*, in PASSAGLIA (a cura di), *Tutela del diritto d'autore e oscuramento dei siti* web, Corte cost., Servizio Studi – Area di diritto comparato, 2015, 95.
[432] Cfr. H.R. Rpt. 105-551, at 11 (May 22, 1998).

rientri nella definizione di *service provider*[433] e che adotti le misure previste per rimuovere tempestivamente i contenuti illeciti.

Per poter beneficiare delle protezioni previste dal DMCA, è necessario che il *provider* non intervenga o modifichi i contenuti che transitano attraverso i propri sistemi. Inoltre, è tenuto a adottare una *policy* efficace per la disconnessione nei confronti degli utenti recidivi.

Il DMCA consente al *provider* di limitare la propria responsabilità in tre principali situazioni. La prima riguarda le comunicazioni transitorie – come, ad esempio, le *email* – che attraversano i sistemi del *provider* senza essere memorizzate.

La seconda situazione è quella del *caching* temporaneo, ovverosia un processo tecnico automatico che consente di conservare dati provenienti da fonti esterne per un periodo limitato, fino a quando l'utente destinatario non li elimina.

Infine, vi è il caso dei contenuti caricati direttamente dagli utenti, in cui il *provider* può andare esente da responsabilità solo se interviene tempestivamente per rimuovere il contenuto illecito, seguendo procedure rigorose e ben definite.

Al fine di ottenere la protezione dalla responsabilità prevista dal DMCA in caso di archiviazione di contenuti illeciti, il fornitore di servizi deve rispettare tre condizioni fondamentali.

La prima è che non deve essere a conoscenza, né in modo diretto né indiretto, dell'attività illecita; e, qualora venga informato di una violazione, è tenuto a intervenire prontamente per rimuovere il materiale.

La seconda condizione impone che il *provider* non tragga alcun vantaggio economico direttamente collegato all'attività illecita. Infine, una volta ricevuta una segnalazione formale di violazione del *copyright*, il *provider* deve agire rapidamente per rimuovere o bloccare l'accesso al contenuto contestato[434].

---

[433] Ai sensi della sezione 512 (k) (1) del DMCA il "*service provider*" è definito come «an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received»; nonché come «a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A)».

[434] Sul punto BENCHELL, *The Digital Millennium Copyright Act: a review of the law and the court's interpretation*, in *J. Marshall J. Computer & Info. L.*, 2002, 38 s.

È stato il legislatore statunitense ad introdurre per la prima volta nel DMCA le c.d. procedure di *notice and take down*, segnando così il primo intervento normativo volto a tutelare il diritto d'autore in Internet.

In particolare, il modello procedurale previsto dalla normativa statunitense stabilisce che per poter beneficiare dell'esonero da responsabilità in caso di violazioni del *copyright*, il *provider* deve innanzitutto designare un referente incaricato – noto come *designated agent* – di ricevere le segnalazioni da parte dei titolari dei diritti d'autore[435]. Questo soggetto deve essere facilmente individuabile dal pubblico, grazie alla presenza di *link* ben visibili e accessibili sulla *homepage* della piattaforma.

La *notification* consiste in una comunicazione formale, redatta per iscritto, che deve includere una serie di informazioni[436] ed essere trasmessa al *designated agent*.

La Sezione 512(g) stabilisce, inoltre, una presunzione generale di non responsabilità per il *provider* che, agendo in buona fede, abbia rimosso contenuti o bloccato l'accesso ad attività *online* sulla base di elementi che ne indicavano una possibile illiceità, anche qualora successivi approfondimenti non confermassero tale impressione.

Tuttavia, questa tutela non si applica se il *provider* non assicura un minimo di confronto tra il titolare dei diritti d'autore presumibilmente violati e la persona responsabile dei contenuti o delle attività segnalate. Pertanto, il *provider* è tenuto a informare tempestivamente quest'ultima della rimozione, affinché possa presentare una contronotifica (c.d. *counter notification*).

Chi presenta una *replica* deve firmare una dichiarazione con cui accetta di sottoporsi alla giurisdizione del competente *Federal District Court* e autorizza l'agente designato a trasmettere la contronotifica alla parte che ha effettuato la

[435] Sezione 512(c)(2) del Titolo 17 dello U.S. Code

[436] Ai sensi della Sezione 512 (c)(3) la notifica di presunta violazione deve includere: i) la firma autografa o elettronica del soggetto interessato o del legale rappresentante; ii) l'indicazione dell'opera protetta che si ritiene violata; iii) l'identificazione del materiale che si ritiene violato o oggetto di attività illecita e che deve essere rimosso o il cui accesso deve essere disabilitato, e le informazioni sufficienti per consentire al fornitore di servizi di individuare il materiale; iv) le informazioni ragionevolmente sufficienti sull'identità del presunto autore della violazione, che consentano al provider di contattarlo; v) una dichiarazione in cui il ricorrente afferma di agire in buona fede a tutela dei propri diritti; vi) un'ulteriore dichiarazione che comprovi l'accuratezza delle informazioni fornite, nonché la legittimazione ad agire avverso le condotte oggetto del reclamo.

segnalazione. Una volta ricevuta la *counter notification*, l'agente è tenuto a informare immediatamente il segnalante, comunicandogli che, salvo diversa indicazione, provvederà entro dieci giorni al ripristino dei contenuti precedentemente rimossi[437].

Con l'introduzione nell'ordinamento statunitense del concetto di *Safe Harbor*, inteso come un insieme di condizioni che consentono agli ISP di essere esonerati da responsabilità civile, il legislatore non ha però fatto alcun riferimento alla responsabilità penale.

Da ciò sono emersi numerosi dubbi in dottrina sull'eventuale possibilità di estensione della tutela prevista dalla Sezione 512 anche agli illeciti di natura penale.

Sebbene una parte autorevole della dottrina[438] abbia criticato l'idea che una condotta non sanzionabile sul piano civile possa comunque comportare conseguenze penali, altri studiosi[439], analizzando la Sezione 512(c), hanno sostenuto la necessità di distinguere i due ambiti. Secondo questa interpretazione, l'applicazione della norma richiede che il *provider* non sia a conoscenza dell'illecito, condizione che, in ambito penale, equivale all'assenza di intenzionalità.

Di conseguenza, l'unica difesa che il *provider* può invocare per evitare la responsabilità penale consiste nel dimostrare di non aver agito intenzionalmente. La prova di questa mancanza di volontarietà sarebbe sufficiente per escludere la *criminal liability*, senza che sia necessario dimostrare anche gli altri requisiti previsti dal *safe harbor*. In tal senso, la difesa basata sulla non-intenzionalità risulterebbe persino più ampia rispetto alla protezione offerta dal DMCA stesso.

Negli Stati Uniti, inoltre, si è discusso a lungo sull'opportunità di utilizzare strumenti penali per tutelare il *copyright*. Sebbene l'analisi economica abbia evidenziato l'efficacia deterrente delle sanzioni penali contro la pirateria digitale, la presenza di un articolato sistema di rimedi civili a disposizione dei titolari dei

---

[437] In tal senso SICA, D'ANTONIO, *La procedura di de-indicizzazione*, in *Dir. Inf.*, 2014, 719 ss.
[438] Cfr. NIMMER, *Nimmer on Copyright*, così come citato da NEWHALL, *Criminal Copyright Enforcement Against Filesharing Services*, in *North Carolina Journal of Law and Technology*, 2013, 124.
[439] V. NEWHALL, *Criminal Copyright Enforcement Against Filesharing Services*, cit., p. 128.

diritti d'autore suggerisce la necessità di riconsiderare l'uso delle sanzioni penali, tenendo conto della loro natura di *extrema ratio*[440].

3.3.2. Un confronto con il modello europeo: Direttiva e-commerce e Digital Services Act

L'impianto normativo statunitense di protezione del diritto d'autore in Internet costituisce un valido punto di partenza circa l'*enforcement* della normativa in ambito europeo e italiano. Difatti, la Commissione europea, durante la formulazione della Direttiva 2000/31/CE relativa ai servizi della società dell'informazione, sembra essersi ispirata a questo modello normativo.

Seguendo l'impostazione del DMCA, la Direttiva ha riconosciuto nella responsabilità degli operatori digitali la base su cui costruire meccanismi rapidi ed efficaci per la rimozione dei contenuti illeciti e la disabilitazione del loro accesso. Tuttavia, nella versione definitiva, la normativa europea si è poi distanziata in modo significativo dal modello statunitense[441].

Anzitutto, occorre sottolineare che il DMCA si concentra esclusivamente sulla tutela del diritto d'autore e sulla responsabilità per la sua violazione, seguendo un'impostazione c.d. verticale, cioè limitata a un ambito specifico. Al contrario, la Direttiva europea adotta una prospettiva orizzontale, affrontando in modo più ampio la responsabilità degli ISP in relazione a qualsiasi tipo di contenuto illecito caricato dagli utenti.

Gli articoli 12, 13 e 14 della Direttiva – corrispondenti oggi agli artt. 4, 5 e 6 del *Digital Services Act* – stabiliscono infatti che, in linea generale, gli ISP non siano ritenuti responsabili per le informazioni trasmesse o memorizzate, indipendentemente dal tipo di illecito. Ciò include violazioni del diritto d'autore, pubblicità ingannevole, infrazioni relative a marchi o brevetti, diffamazione o altre condotte penalmente rilevanti. Inoltre, tale approccio viene ulteriormente confermato dalla Direttiva 2001/29/CE sul *copyright*, la quale, nel considerando

[440] In argomento IMPERADORI, *La responsabilità dell'*Internet Service Provider, cit., 44 s.
[441] Così DELSIGNORE, *Il sistema U.S.A.*, in *AIDA*, 2014, 1, 3.

16[442], chiarisce esplicitamente di non modificare le regole sulla responsabilità degli ISP[443].

Il DMCA è intervenuto sulle violazioni digitali del diritto d'autore attraverso l'adozione della procedura basata sulla segnalazione e sulla rimozione successiva dei contenuti illeciti (*notice and take down*)[444].

Questo modello di rimozione dei contenuti illeciti *online* delineato dal DMCA evidenzia alcuni principi essenziali che dovrebbero orientare qualsiasi procedura simile, soprattutto quando la gestione iniziale è affidata direttamente al *provider*.

Uno degli aspetti centrali è la necessità di garantire costantemente il confronto tra tutte le parti coinvolte nella disputa sul contenuto *online*. In questo senso, il DMCA prevede che il fornitore di servizi svolga un ruolo attivo nel facilitare il dialogo tra le parti in conflitto, attraverso il sistema di notifica **e** contro-notifica. Per l'ISP, assicurare il contraddittorio non è solo un principio astratto, ma un obiettivo concreto da perseguire, poiché in caso contrario potrebbe essere ritenuto responsabile per eventuali danni derivanti da rimozioni ingiustificate.

Un altro elemento distintivo del sistema statunitense è la forte responsabilizzazione degli utenti coinvolti nel processo. Il rischio di censurare contenuti legittimi o di abusare dello strumento è ridotto grazie a misure dissuasive che gravano sia su chi richiede la rimozione, sia su chi si oppone. Entrambi, nel momento in cui presentano una notifica o una contro-notifica, sono informati del

---

[442] Direttiva 2001/29/CE, Considerando 16: «La responsabilità per le attività in rete riguarda, oltre al diritto d'autore e ai diritti connessi, una serie di altri ambiti, come la diffamazione, la pubblicità menzognera o il mancato rispetto dei marchi depositati, ed è trattata in modo orizzontale nella direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico")(4) che chiarisce ed armonizza vari aspetti giuridici riguardanti i servizi della società dell'informazione, compresi quelli riguardanti il commercio elettronico. La presente direttiva dovrebbe essere attuata in tempi analoghi a quelli previsti per l'attuazione della direttiva sul commercio elettronico, in quanto tale direttiva fornisce un quadro armonizzato di principi e regole che riguardano tra l'altro alcune parti importanti della presente direttiva. Questa direttiva lascia impregiudicate le regole relative alla responsabilità della direttiva suddetta».

[443] V. DELSIGNORE, *Il sistema U.S.A.*, cit., 8 s.

[444] Cfr. USMAN, *Guideline on Internet Service Providers' (ISPS) Liability Regime in the United States*, in AHMADU (a cura di), *Perspectives on Nigerian Law*, Sokoto, 2017, 3.

fatto che assumono precise responsabilità nel caso in cui le dichiarazioni rese siano false o inesatte, o qualora si tenti di usare il procedimento in modo improprio[445].

In Europa, la Direttiva e-commerce, pur ispirandosi al DMCA non ha recepito integralmente la procedura di *notice and take down*. Tuttavia, la Direttiva ha introdotto il concetto di "conoscenza effettiva" quale presupposto per far scattare l'obbligo di rimozione di contenuti illeciti[446]. Questo ha generato dubbi sul valore delle segnalazioni fatte dai titolari dei diritti d'autore, poiché non esisteva un meccanismo chiaro che obblighi i *provider* a rimuovere i contenuti segnalati.

In Italia, prima dell'entrata in vigore del DSA, la giurisprudenza[447] è stata particolarmente severa, poiché considerava "effettiva" solo la conoscenza la notizia proveniente da un'autorità pubblica**,** come un giudice o un ente amministrativo, escludendo le segnalazioni private come base sufficiente per agire.

Inoltre, la Direttiva[448] si è limitata a incoraggiare l'adozione di sistemi condivisi tra le parti interessate senza imporre obblighi specifici[449].

Il quadro normativo europeo delineato dalla Direttiva 2000/31/CE è cambiato con l'introduzione del *Digital Services Act*. Questo regolamento europeo, pur mantenendo il principio secondo cui la responsabilità del *provider* può essere esclusa solo se non ha conoscenza effettiva dei contenuti illeciti, e pur non richiedendo un intervento diretto da parte delle autorità per attivare gli obblighi di rimozione, impone ai fornitori di servizi di *hosting* di predisporre strumenti che

---

[445] In tal senso SICA, D'ANTONIO, *La procedura di de-indicizzazione*, cit., 722.

[446] L'Art. 14 della Dir. 2000/31/CE prevede che il prestatore «a) non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività, o b) non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso».

[447] V. Cass. civ., sez I, 19 marzo 2019, n. 7708.

[448] Direttiva 2000/31/CE, Considerando 40: «Le attuali o emergenti divergenze tra le normative e le giurisprudenze nazionali, nel campo della responsabilità dei prestatori di servizi che agiscono come intermediari, impediscono il buon funzionamento del mercato interno, soprattutto ostacolando lo sviluppo dei servizi transnazionali e introducendo distorsioni della concorrenza. In taluni casi, i prestatori di servizi hanno il dovere di agire per evitare o per porre fine alle attività illegali. La presente direttiva dovrebbe costituire la base adeguata per elaborare sistemi rapidi e affidabili idonei a rimuovere le informazioni illecite e disabilitare l'accesso alle medesime. Tali sistemi potrebbero essere concordati tra tutte le parti interessate e andrebbero incoraggiati dagli Stati membri. È nell'interesse di tutte le parti attive nella prestazione di servizi della società dell'informazione istituire e applicare tali sistemi. Le disposizioni dalla presente direttiva sulla responsabilità non dovrebbero impedire ai vari interessati di sviluppare e usare effettivamente sistemi tecnici di protezione e di identificazione, nonché strumenti tecnici di sorveglianza resi possibili dalla tecnologia digitale, entro i limiti fissati dalle direttive 95/46/CE e 97/66/CE».

[449] Così DELSIGNORE, *Il sistema U.S.A.*, cit., 11.

permettano a chiunque – persona fisica o ente – di segnalare la presenza di contenuti ritenuti illegali.

Questi strumenti devono essere facilmente accessibili e utilizzabili, consentendo l'invio di segnalazioni esclusivamente in formato elettronico. Devono inoltre facilitare la presentazione di notifiche chiare, dettagliate e ben motivate, in modo che un operatore economico responsabile possa riconoscere l'illegalità dei contenuti[450].

Il meccanismo di *notice and action*, codificato nell'art. 16 del DSA, si rivela particolarmente significativo, in quanto istituzionalizza un meccanismo essenziale. Attraverso questo meccanismo, enti e persone fisiche contribuiscono a rendere più efficace il controllo privato da parte degli operatori digitali, offrendo un supporto in processi che, già di per sé, risultano complessi sotto il profilo organizzativo e gestionale. Inoltre, sarebbe irrealistico attendersi che le piattaforme siano in grado, da sole, di individuare ogni contenuto illegale diffuso tramite i loro servizi.

Tuttavia, è fondamentale sottolineare che il meccanismo di *notice and action* deve essere obbligatoriamente predisposto per le segnalazioni di attività o contenuti illegali, e non anche per quelli lesivi unicamente delle condizioni generali d'uso o dei c.d. *standard* della *community*. Resta comunque inteso che le piattaforme hanno sempre la possibilità di ampliare volontariamente l'ambito di applicazione di tali procedure, permettendo l'attivazione anche per contenuti che, pur non essendo illegali, violano le condizioni d'uso del servizio o riguardano attività non consentite[451].

Questo aspetto rappresenta uno dei punti chiave della normativa europea, in quanto la responsabilità del fornitore, nel momento in cui carica contenuti *online*, è legata all'adozione di sistemi di segnalazione e rimozione, simili a quelli introdotti negli Stati Uniti con il DMCA del 1998. Infatti, il DSA mostra una maggiore somiglianza con il modello americano rispetto a quanto previsto dalla precedente Direttiva sul commercio elettronico[452].

---

[450] V. Reg. (UE) 2022/2065, art. 16, par. 1.

[451] Sul punto BIRRITTERI, *Contrasto alla disinformazione,* Digital Services Act *e attività di* private enforcement*: fondamento, contenuti e limiti degli obblighi di* compliance *e dei poteri di autonormazione degli operatori*, in *MediaLaws*, 2023, 2, 61.

[452] Sul punto PURPURA, *Osservazioni sul* Digital Services Act*: responsabilità e gestione del rischio nella prestazione di servizi intermediari*, in *Comp. dir. civ.*, 2022, 3, 1055 s.

3.4. La giurisprudenza sulla responsabilità dei *provider* negli USA

La giurisprudenza americana ha svolto un ruolo particolarmente centrale nel definire il quadro della responsabilità degli *Internet Service Provider*. La peculiarità del contesto statunitense risiede nell'introduzione di normative dedicate, come la Sezione 230 del *Communications Decency Act* (CDA) e il *Digital Millennium Copyright Act* (DMCA), che hanno profondamente modellato l'approccio dei tribunali e fornito agli ISP un significativo scudo di immunità.

Gli ISP, in qualità di soggetti attraverso i quali possono transitare eventuali contenuti illeciti, si trovano spesso in una posizione vulnerabile nell'ambito di azioni giudiziarie, poiché risultano più facilmente individuabile rispetto agli utenti che popolano il *cyberspace*, i quali operano spesso in condizioni di anonimato.

Diverse decisioni giudiziarie[453], infatti, sia prima che dopo l'introduzione delle suddette normative, hanno contribuito a definire i limiti della responsabilità dei *provider*, tracciando l'evoluzione del modello statunitense[454].

Sul piano legislativo – come anticipato – il *CDA* del 1996 e il *DMCA* del 1998 offrono agli ISP una forma di immunità rispetto a responsabilità che, secondo i principi del *common law*, sarebbero altrimenti riconoscibili, finendo per ridurre drasticamente l'esposizione degli ISP a responsabilità.

La Sezione 230 del CDA, in particolare, è diventata una disposizione chiave secondo cui un ISP non deve essere trattato come editore o autore di alcuna informazione fornita da un utente o da un'altra fonte. Le decisioni dei Tribunali americani hanno spesso interpretato questa norma in modo estensivo, ampliando l'immunità a tutte le forme di responsabilità e a tutti i tipi di informazione[455].

---

[453] Cfr. *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991); *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 23 Media L. Rep. 1794 (N.Y. Sup. Ct. 1995); *Zeran v. America Online*, Inc., 958 F. Supp. 1124 (E.D. Va. 1997); *Blumenthal v. Drudge*, 992 F. Supp. 44 (D.D.C. 1998); *Gucci America, Inc. v. Hall & Associates*, 135 F. Supp. 2d 409 (S.D.N.Y. 2001); *Lunney v. Prodigy Servs. Co.*, 94 N.Y. 2d 242 (N.Y. Ct. App. 1999).

[454] In argomento BERNSTEIN, RAMCHANDANI, *Don't Shoot the Messenger! A Discussion of ISP Liability*, in *Canadian Journal of Law and Technology*, 2002, 2, 77 s.

[455] Sul punto LICHTMAN, POSNER, *Holding Internet Service Providers Accountable*, in *Sup. Ct. Econ. Rev.*, 2006, 248.

Nel contesto di illeciti come la diffamazione, l'approccio giuridico tradizionale ha sempre distinto tra chi crea e pubblica il contenuto e chi lo distribuisce.

In particolare, gli autori e gli editori delle comunicazioni sono considerati responsabili, mentre librai, biblioteche e altri soggetti che si limitano a distribuire il materiale godono di immunità, a condizione che non fossero a conoscenza dell'illecito.

Prima dell'introduzione del CDA, i Tribunali avevano tentato di estendere il modello di responsabilità tradizionale anche agli ISP. In particolare, nel caso *Cubby v. Compuserve*[456] la Corte distrettuale degli Stati Uniti per il distretto meridionale di New York aveva stabilito che l'ISP non poteva essere ritenuto responsabile per contenuti diffamatori trasmessi attraverso la sua infrastruttura. Questa decisione si basava sul fatto che l'ISP agiva come semplice distributore delle informazioni, senza svolgere un ruolo attivo nella loro selezione o pubblicazione, e quindi non poteva essere equiparato a un editore.

Poco tempo dopo, in un caso simile – *Stratton Oakmont v. Prodigy Services*[457] – un altro Tribunale è giunto a una conclusione opposta, ritenendo che l'ISP doveva essere considerato un editore. Secondo la Corte Suprema di New York, il fatto che il *provider* impiegasse attivamente strumenti tecnologici e personali per rimuovere messaggi dalle proprie bacheche elettroniche dimostrava che esercitava un controllo sui contenuti. Questo intervento, secondo il giudice, equivaleva a un'attività editoriale vera e propria.

Tuttavia, questo sviluppo giurisprudenziale ha portato a una conseguenza prevedibile, in quanto le norme sulla responsabilità finivano per disincentivare gli ISP dall'intervenire per moderare contenuti problematici. Infatti, un ISP che sceglieva di non adottare misure di controllo veniva trattato secondo il modello delineato dal caso *Cubby*, godendo di un'ampia immunità come semplice distributore passivo. Al contrario, un ISP che cercava di filtrare o rimuovere contenuti rischiava di essere considerato responsabile, come nel caso *Stratton Oakmont*, assumendo quindi il ruolo di editore.

---

[456] V. *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991).
[457] Cfr. *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 23 Media L. Rep. 1794 (N.Y. Sup. Ct. 1995).

Di conseguenza, risultava più sicuro e conveniente non intervenire affatto, anche di fronte ad abusi evidenti e, proprio per correggere questo problema, il Congresso ha approvato il *Communications Decency Act* nel 1996.

Il fulcro del CDA è rappresentato dalla Sezione 230, la quale stabilisce che gli ISP non possono essere considerati responsabili come editori o autori delle informazioni fornite dagli utenti o da terze parti. Tuttavia, sin dalla sua entrata in vigore, questa norma ha suscitato un ampio dibattito circa la responsabilità degli ISP e, in particolare, veniva discusso se la disposizione costituisse per gli ISP un'immunità totale rispetto a responsabilità per diffamazione e altri illeciti simili oppure se la stessa consenta comunque di considerarli responsabili in qualità di semplici distributori.

Sul punto emblematica è la sentenza *Zeran v. America Online*[458], nella quale la Corte d'Appello del Quarto Circuito ha stabilito che la Sezione 230 garantisce ai *provider* un'immunità federale da qualsiasi azione legale basata su contenuti generati da terzi, a prescindere dal ruolo assunto dall'ISP, sia esso quello di editore o di semplice distributore. Secondo la Corte, infatti, la responsabilità del distributore non è altro che una forma di responsabilità editoriale e, pertanto, rientra anch'essa nell'ambito di esclusione previsto dalla norma.

La Corte ha motivato questa interpretazione anche sulla base di considerazioni di ordine pratico e politico: attribuire agli ISP una responsabilità da distributori significherebbe costringerli a intervenire ogni volta che ricevono una segnalazione di contenuti potenzialmente diffamatori, obbligandoli a condurre verifiche tempestive e complesse e a prendere decisioni editoriali immediate. Un simile onere, secondo questa prospettiva, nel contesto dinamico e vasto di Internet, risulterebbe insostenibile. Inoltre, ciò rischierebbe di generare un effetto repressivo sulla libertà di espressione *online*, inducendo i *provider* a rimuovere automaticamente qualsiasi contenuto segnalato, anche in assenza di una reale violazione della legge[459].

[458] V. *Zeran v. America Online, Inc.*, 958 F. Supp. 1124 (E.D. Va. 1997).
[459] In tal senso LICHTMAN, POSNER, *Holding Internet Service Providers Accountable*, cit., 249 ss.

La Sezione 230, pur garantendo una sostanziale immunità civile agli ISP, ne esclude espressamente l'applicazione in ambito penale[460], lasciando aperta la possibilità di configurare una responsabilità penale ai *provider*.

Ciononostante, ad oggi non si ravvisano precedenti concreti che abbiano effettivamente applicato questo principio. Soltanto attraverso un'analisi approfondita dei singoli casi giurisprudenziali gli interpreti possono comprendere concretamente come il diritto vivente si orienti rispetto alla responsabilità degli ISP, soprattutto alla luce di un quadro normativo ormai superato e del ruolo sempre più centrale dei processi automatizzati nelle decisioni editoriali adottate dai *provider online*.

Affidare il controllo dei contenuti esclusivamente all'intervento umano risulta ormai impraticabile, data l'impossibilità materiale di controllare l'enorme flusso di utenti nel cyberspazio. Pertanto, è necessario ripensare ai modelli di responsabilità penale, data la progressiva marginalizzazione della presenza dell'uomo – che, quantomeno, potrebbe essere ritenuto responsabile a titolo di colpa – e del sempre più rilevante ruolo assunto da sistemi automatizzati nella selezione e nel filtraggio dei contenuti.

L'ordinamento statunitense, con il caso *Force v. Facebook*[461], è stato il primo ad affrontare questa problematica. In questa vicenda, il *social network* è stato accusato di aver indirettamente collaborato con Hamas nella realizzazione di attentati terroristici in Israele, che hanno causato la morte di cittadini americani. Il caso affrontato dai giudici di New York solleva, per la prima volta, il tema delle decisioni algoritmiche che operano dietro la piattaforma, invitando a rivedere il ruolo tradizionalmente attribuito a *Facebook* come semplice intermediario neutrale. Secondo l'accusa, infatti, la piattaforma eserciterebbe una forma di manipolazione dei contenuti proprio attraverso l'impiego di sistemi automatizzati, offrendo così spunti rilevanti per la riflessione sul contributo causale degli algoritmi[462].

3.4.1. Il caso *Cubby v. Compuserve Inc.* (1991)

[460] *Title* 47 *U.S. Code* § 230 (2)(e)(1).
[461] Cfr. *Force v. Facebook, Inc.*, No. 18-397 (2d Cir. 2019).
[462] In argomento BACCIN, *Responsabilità penale dell'*internet service provider *e concorso degli algoritmi negli illeciti* online*: Il caso* Force v. Facebook, in *Sist. pen.*, 2020, 5, 78 s.

La questione della responsabilità degli intermediari *online* è emersa nel 1991 con il caso *Cubby v. Compuserve Inc.*[463], che è considerato uno dei primi interventi giudiziari sulla responsabilità dei fornitori di servizi internet per i contenuti pubblicati da terzi[464].

In questo caso assumeva un ruolo centrale il fornitore di servizi online *Compuserve*, che all'epoca rappresentava il secondo più grande sistema BBS[465] commerciale negli Stati Uniti ed era stato un punto di riferimento nel settore.

Tra i vari servizi offerti dalla Società vi era il *Journalism Forum*, noto come "JFORUM", pensato per favorire lo scambio di informazioni nel mondo del giornalismo. Proprio all'interno di JFORUM veniva distribuita agli utenti una *newsletter* chiamata *Rumorville Usa*, elemento centrale della disputa legale nel caso *Cubby*.

Rumorville, fondata nel 1983, era una *newsletter* disponibile esclusivamente in formato digitale tramite JFORUM, pubblicata da *Don Fitzpatrick Associates* (DFA), un'azienda specializzata nel supporto alla collocazione di professionisti nel campo dell'informazione televisiva, della programmazione e della distribuzione. Dietro pagamento di un abbonamento, *Rumorville* offriva notizie e indiscrezioni riguardanti il mondo del giornalismo radiotelevisivo e i suoi protagonisti, rivolgendosi principalmente a organizzazioni professionali del settore.

Nel 1990, *Cubby, Inc.* e Robert Blanchard avevano ideato *Skuttlebut*, una *newsletter* elettronica pensata per competere con *Rumorville*. Successivamente, *Cubby* e Blanchard avviarono una causa contro *Compuserve* e DFA, accusando *Rumorville* di aver diffuso informazioni false e diffamatorie riguardanti *Skuttlebut* e Blanchard. Gli attori accusavano *CompuServe* e DFA di diffamazione nei confronti di Blanchard, oltre che di concorrenza sleale e denigrazione commerciale nei confronti di *Skuttlebut*, facendo riferimento alla normativa dello Stato di New York.

Compuserve chiedeva il rigetto delle accuse, sostenendo di essere solo un distributore di informazioni e non il loro editore. Secondo la sua posizione, in

---

[463] V. *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991).
[464] Così KOSSEFF, *Twenty Years of Intermediary Immunity: The US Experience*, in *Scripted*, 2017, 1, 10.
[465] V. nota 13.

quanto mero distributore, non poteva essere ritenuta responsabile per le presunte dichiarazioni diffamatorie, poiché non ne era a conoscenza né aveva motivo di esserlo[466].

Il giudice accoglieva la richiesta di *Compuserve*, richiamando un principio giuridico consolidato nel diritto dello Stato di New York, secondo cui un distributore di contenuti diffamatori non può essere ritenuto responsabile se non è a conoscenza – né ha motivo di esserlo – della natura diffamatoria del materiale. Il tribunale ha ritenuto che l'attività della *Compuserve* poiché non esercitava alcun controllo editoriale preventivo sui contenuti pubblicati da terzi.

La decisione nel caso *Cubby* si fondava anche sulle tutele offerte dal Primo Emendamento a soggetti come librai, edicolanti e bibliotecari. In particolare, si richiamava il precedente *Smith*[467], in cui la Corte Suprema degli Stati Uniti aveva annullato un'ordinanza comunale che attribuiva responsabilità oggettiva al titolare di una libreria per il possesso di un libro osceno, anche se non ne conosceva il contenuto.

La Corte aveva sottolineato che, se i librai e gli edicolanti fossero costretti a controllare personalmente ogni pubblicazione, la loro attività diventerebbe insostenibile. Pur trattandosi nel caso *Smith* di responsabilità penale, il tribunale nel caso *Cubby* ha ritenuto che le protezioni costituzionali garantite da quel precedente si estendessero anche al contesto civile della diffamazione[468].

3.4.2. Il caso *Stratton Oakmont Inc. v. Prodigy Services Co.* (1995)

Il caso *Stratton Oakmont Inc. v. Prodigy Services Co.*[469] si inserisce in un contesto di rapida evoluzione tecnologica e crescente consapevolezza pubblica riguardo ai danni reputazionali; riflette una nuova realtà in cui le comunicazioni, essendo simultanee, interattive, mirate e accessibili a un vasto pubblico, possono causare danni economici e personali significativi.

---

[466] Sul punto CONNER, *Cubby v. Compuserve, Defamation Law on the Electronic Frontier*, in *Geo. Mason Indep. L. Rev.*, 1993, 1, 232 s.
[467] V. *Smith v. California*, 361 U.S. 147 (1959).
[468] Così CONNER, *Cubby v. Compuserve, Defamation Law on the Electronic Frontier*, cit., 233 s.
[469] V. *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 23 Media L. Rep. 1794 (N.Y. Sup. Ct. 1995).

La sentenza offre un importante punto di riferimento per gli ISP che intendono prevenire o limitare il rischio di azioni legali in materia di diffamazione. Nello specifico, questa decisione un cambiamento nell'approccio giuridico al ruolo dei fornitori di servizi digitali, andando oltre il solo tema della diffamazione *online* e aprendo la strada a una più ampia riflessione sulle responsabilità in rete[470].

Nell'ottobre del 1994, la società di investimento bancario *Stratton Oakmont* e il suo presidente Daniel Porush citavano in giudizio la Società *Prodigy* accusandola di aver diffuso messaggi anonimi ritenuti diffamatori tramite la bacheca elettronica *Money Talk*. Secondo i querelanti, Prodigy avrebbe dovuto impedirne la pubblicazione e, quindi, ne era responsabile.

Sul punto, il giudice della Corte Suprema di New York ha qualificato *Prodigy* come editore e ha ritenuto che Epstein operava come agente della società e, allo stesso tempo, ha stabilito che, in generale, i servizi *online* dovrebbero essere considerati distributori di contenuti, analoghi a librerie, biblioteche o reti televisive affiliate e, quindi, soggetti a una responsabilità limitata per le dichiarazioni di terzi.

Tuttavia, nel caso di *Prodigy*, la Corte ha ritenuto applicabile uno standard di responsabilità più rigoroso, simile a quello previsto per giornali e altri editori, motivando tale scelta con il fatto che le politiche aziendali, le tecnologie adottate e le decisioni organizzative di *Prodigy* la avvicinavano maggiormente al ruolo di editore piuttosto che a quello di semplice distributore.

La società *Prodigy* nel corso del giudizio sosteneva che, al momento della presunta diffamazione, i suoi sistemi di controllo non erano più rigorosi come in passato e che, considerando l'elevato numero di messaggi pubblicati ogni giorno sulle bacheche, un monitoraggio completo era di fatto impossibile.

Tuttavia, il giudice rilevava che la Società non aveva presentato alcuna prova concreta di tali modifiche né aveva informato gli utenti del servizio e, conseguentemente, ha riconosciuto la responsabilità del *provider*[471].

---

[470] In argomento CHARLES, ZAMANSKY, *Liability for Online Libel after Stratton Oakmont, Inc. v. Prodigy Services Co.*, in *Conn. L. Rev.*, 1996, 1174 e 1176 s.

[471] Sul punto JOHNSON, *Defamation in Cyberspace: A Court Takes a Wrong Turn on the Information Superhighway in Stratton Oakmont, Inc. v. Prodigy Services Co.*, in *Ark. L. Rev.*, 1996, 3, 595 ss.

Nel loro insieme, le sentenze *Cubby* e *Stratton Oakmont* hanno contribuito a delineare l'idea secondo cui gli intermediari *online* possono essere ritenuti giuridicamente responsabili per i contenuti generati dagli utenti solo nel caso in cui intervengano attivamente per controllarli, ad esempio attraverso la moderazione dei forum o l'imposizione di regole comportamentali. Al contrario, se mantengono una posizione completamente neutrale e si astengono dall'intervenire sui contenuti pubblicati da terzi, non possono essere considerati responsabili. Di conseguenza, queste pronunce hanno finito per scoraggiare gli intermediari dall'esercitare qualsiasi forma di controllo sui contenuti degli utenti, al fine di evitare implicazioni legali.

Queste decisioni hanno attirato rapidamente l'attenzione dell'opinione pubblica. Negli anni '90, mentre Internet passava da essere uno strumento riservato a istituzioni accademiche e governative a un mezzo sempre più diffuso nelle case e negli ambienti di lavoro, crescevano le preoccupazioni tra politici e attivisti per i diritti civili. Si temeva che sentenze come quelle dei casi *Cubby* e *Stratton Oakmont* avrebbero potuto trasformare il Web in uno spazio privo di regolamentazione, popolato da contenuti offensivi e inadatti ai minori. Il Congresso avrebbe potuto rispondere introducendo norme più rigide a carico degli intermediari, imponendo loro di intervenire sui contenuti generati dagli utenti. Tuttavia, misure di questo tipo rischiavano di incontrare una forte opposizione da parte dei provider e degli altri attori del settore. Pertanto, il Congresso ha deciso di affrontare il tema della moderazione dei contenuti attraverso la Sezione 230 del *Communications Decency Act* del 1996.

Le disposizioni contenute del CDA incarnano il duplice intento del Congresso di promuovere, da un lato, la moderazione volontaria dei contenuti da parte delle piattaforme *online*, e, dall'altro, di favorire l'innovazione e la crescita dell'allora emergente Internet commerciale. Infatti, nella relazione allegata alla legge, i promotori del provvedimento hanno dichiarato esplicitamente l'intenzione di annullare l'effetto di decisioni giudiziarie come quella del caso Stratton Oakmont, ritenendo che tali sentenze ostacolassero in modo significativo

l'obiettivo federale di permettere ai genitori di controllare i contenuti accessibili ai propri figli attraverso i servizi digitali interattivi[472].

3.4.3. Effetti del CDA: sentenza *Zeran v. American Online Inc.* (1997)

La storia che ha portato all'approvazione della Sezione 230 mostra chiaramente l'intenzione originaria di promuovere una moderazione in buona fede da parte degli ISP. Tuttavia, l'interpretazione successiva da parte dei tribunali[473] ha attribuito a questi soggetti un'immunità quasi assoluta, andando ad ostacolare, di fatto, l'incentivo ad adottare misure ragionevoli di tutela dei contenuti.

Nel 1996 – anno in cui è stato approvato l'emendamento – Internet era ancora agli albori e le dimensioni e l'influenza che avrebbe assunto non erano immaginabili. Infatti, l'intento della Sezione 230 non era quello di agevolare attività illecite *online*, bensì contribuire a rendere il Web un ambiente più sicuro.

Ed infatti, a solo un anno dall'entrata in vigore della Sezione 230, il caso *Zeran v. American Online Inc.*[474] (AOL) ha segnato la prima applicazione della norma in ambito giudiziario. Questo caso evidenzia come la Sezione 230 non abbia spinto le piattaforme digitali ad intervenire in "buona fede" o ad assumere il ruolo di "buoni samaritani", ma abbia piuttosto legittimato un atteggiamento passivo, da mero spettatore.

Se fosse stato imposto un obbligo i fornitori *online* sarebbero stati incentivati a gestire attivamente i rischi presenti sulle loro piattaforme.

Tuttavia, le Corti[475] hanno interpretato la Sezione 230(c)(1) come una norma che garantisce ai *provider* un'immunità assoluta per i contenuti generati da terzi, anche quando operano in modo simile a un editore tradizionale[476].

---

[472] In tal senso KOSSEFF, *Twenty Years of Intermediary Immunity*, cit., 10 s. e 13.
[473] Cfr. CITRON, WITTES, *The Problem Isn't Just Backpage: Revising Section 230 Immunity*, in *Geo. L. Tech. L. Rev.*, 2018, 7, 465: «The broad sweeping interpretation of Section 230's immunity eliminates incentives for better behavior by those in the best position to minimize harm».
[474] V. *Zeran v. America Online, Inc.*, 958 F. Supp. 1124 (E.D. Va. 1997).
[475] Cfr. *Shiamili v. Real Estate Group of New York*, 17 N.Y.3d 281, 284-85 (N.Y. App Ct. 2011); *Phan v. Pham*, 182 Cal.App.4th 323, 325-26 (Cal. App. Ct. 2010); *Jones v. Dirty World Entertainment Recordings*, LLC, 755 F.3d 398, 401-02 (6th Cir. 2014); *Hinton v. Amazon*, 72 F. Supp. 3d 685, 687 (S.D. Miss. 2014).
[476] Sul punto CABRERA, *Analysis of Section 230 under a Theory of Premises Liability: A Focus on Herrick v. Grindr and Daniel v. Armslist*, in *U. Miami Bus. L. Rev.*, 2021, 2, 63 ss.

Nel caso di specie, pochi giorni dopo l'attentato di Oklahoma City nel 1995, un utente anonimo pubblicava su una bacheca *online* di *American Online* un messaggio promozionale per magliette con slogan offensivi sull'accaduto. Nel post veniva indicato di contattare un soggetto di nome "Ken" presso l'abitazione di Zeran per effettuare l'acquisto. A seguito della pubblicazione, Zeran cominciò a ricevere numerose telefonate minacciose, ma non poteva cambiare numero di telefono a causa di esigenze lavorative.

Così Zeran contattava la Società lo stesso giorno e un dipendente gli assicurava che il messaggio sarebbe stato rimosso, precisando però che, per politica aziendale, AOL non avrebbe pubblicato alcuna rettifica. Nonostante la rimozione del post iniziale, nei giorni successivi sono comparsi nuovi messaggi, con identificativi leggermente diversi che continuavano a invitare gli utenti a chiamare Zeran.

La situazione è peggiorata drasticamente quando una radio locale ha trasmesso i contenuti dei messaggi in diretta, causando un'ondata di telefonate nei confronti del soggetto e costringendo la polizia a sorvegliare costantemente la casa di Zeran.

Nell'aprile 1996, Zeran intentò causa contro AOL, accusandola di negligenza per non aver gestito adeguatamente i post falsi e dannosi dopo essere stata informata della loro natura. La sua azione si basava sulla teoria della responsabilità del distributore, secondo cui chi distribuisce contenuti può essere ritenuto responsabile se è a conoscenza – o dovrebbe esserlo – del loro carattere diffamatorio.

AOL, in sua difesa, ha chiesto l'archiviazione della causa sostenendo che il CDA escludeva la possibilità di avanzare richieste di responsabilità come quella formulata da Zeran.

Il tribunale distrettuale ha rigettato la causa intentata da Zeran, ritenendo che fosse incompatibile con quanto previsto dalla Sezione 230 del CDA. In particolare, il giudice ha esaminato se la richiesta di Zeran, basata sul diritto statale e relativa alla distribuzione negligente di contenuti diffamatori, violava il principio

del CDA che impedisce di considerare i fornitori di servizi Internet come "editori" o "autori" dei contenuti pubblicati da terzi[477].

Pertanto, secondo il tribunale, la responsabilità del distributore è una forma di responsabilità editoriale, richiamando la Sezione 577 del *Restatement (Second) of Torts*, che definisce la pubblicazione come l'atto di comunicare contenuti diffamatori, ma include anche la mancata rimozione di tali contenuti da spazi sotto il proprio controllo.

Applicando questa definizione, il tribunale ha concluso che Zeran, nel cercare di attribuire ad AOL una responsabilità da distributore, stava di fatto cercando di trattarla come un editore. Tuttavia, la sezione 230(c)(1) del CDA stabilisce chiaramente che i fornitori di servizi interattivi non possono essere considerati responsabili come editori per i contenuti generati da altri.

Di conseguenza, il tribunale ha stabilito che AOL non poteva essere ritenuta responsabile per la pubblicazione dei messaggi diffamatori e ha respinto la richiesta di Zeran.

La Corte d'Appello del Quarto Circuito[478] ha confermato tale decisione, affermando che la Sezione 230 impedisce ai tribunali di accogliere azioni legali che implicherebbero trattare un fornitore di servizi informatici come se fosse l'editore dei contenuti.

La Corte, tenendo conto sia del testo della legge che delle intenzioni del legislatore, ha concluso che AOL rientrava pienamente nella definizione di editore e, per questo motivo, godeva della protezione garantita dalla Sezione 230 del CDA[479].

In definitiva, il caso *Zeran v. AOL* è divenuto un punto di riferimento centrale nella giurisprudenza sulla Sezione 230, essendo citato in oltre 1.400 sentenze e influenzando così quasi tutte le decisioni successive in materia. La Corte ha interpretato la norma in modo particolarmente ampio, superando quanto strettamente necessario per perseguire gli obiettivi originari del Congresso, ossia

---

[477] Sezione 230(c)(1).
[478] V. *Zeran v. America Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997).
[479] In argomento PANTAZIS, *Zeran v. America Online, Inc.: Insulating Internet Service Providers from Defamation Liability*, in *Wake Forest L. Rev.*, 1999, 532 ss.

scongiurare l'effetto della sentenza Stratton Oakmont e tutelare il diritto dei genitori di controllare i contenuti accessibili ai propri figli.[480].

3.4.4. Il *caso Force v. Facebook* (2019)

L'organizzazione terroristica palestinese Hamas, tra il 2014 e il 2016, ha compiuto una serie di attacchi in Israele, causando la morte di cinque cittadini statunitensi. I familiari delle vittime, indicati collettivamente come *Force*, hanno avviato un'azione legale contro Facebook, accusando la piattaforma di aver facilitato la diffusione di contenuti che incitavano direttamente a tali atti terroristici. Secondo *Force*, gli algoritmi di Facebook avrebbero identificato utenti potenzialmente sensibili al messaggio di Hamas e avrebbero inserito quei contenuti nei loro *feed* personalizzati, permettendo così all'organizzazione di raggiungere il pubblico mirato e di compiere le operazioni comunicative fondamentali per i propri attacchi.

In particolare, *Force* sosteneva che Facebook era civilmente responsabile ai sensi della Sezione 2333 dell'*Anti-Terrorism Act*[481], accusandolo di aver fornito supporto materiale a un'organizzazione terroristica, quale è Hamas.

A riguardo, la U*nited States District Court for the Eastern District of New York* ha stabilito la Sezione 230(c)(1) impediva a *Force* di sostenere che Facebook dovesse essere considerato editore o autore dei contenuti pubblicati da Hamas, e ha così respinto le richieste.

Successivamente, *Force* ha presentato una nuova richiesta per ottenere il permesso di depositare una seconda memoria emendata, in cui si sosteneva che Facebook avesse nascosto il proprio coinvolgimento nel fornire supporto materiale a Hamas. Tuttavia, anche questa istanza è stata respinta dalla Corte, che ha ribadito che la Sezione 230(c)(1) garantisce a Facebook l'immunità rispetto alle accuse, rendendo superflua la nuova memoria.

---

[480] In tal senso LUKMIRE, *Can the Courts Tame the Communications Decency Act?: The Reverberations of Zeran v. American Online*, in *N.Y.U. Ann. Surv. Am. L.*, 2010, 2, 385.

[481] 18 U.S.C., Sezione 2333 (a): «Any national of the United States injured in his or her person, property, or business by reason of an act of international terrorism, or his or her estate, survivors, or heirs, may sue therefor in any appropriate district court of the United States and shall recover threefold the damages he or she sustains and the cost of the suit, including attorney's fees».

In fase di appello, il *Second Circuit* ha confermato la decisione del tribunale di primo grado, riconoscendo a Facebook l'immunità civile prevista dalla Sezione 230(c)(1) e qualificando la piattaforma come editore dei contenuti. Inoltre, ha chiarito che la creazione dell'algoritmo da parte di Facebook non equivaleva alla creazione dei contenuti che esso suggeriva, sottolineando che la selezione e la distribuzione di contenuti di terzi rientrano pienamente nelle funzioni editoriali della piattaforma[482].

Il caso *Force v. Facebook*[483] solleva un interesse comparatistico significativo, non solo per la possibilità di istituire un parallelismo tra gli ordinamenti giuridici italiano e statunitense in materia di responsabilità degli ISP, ma anche per la profonda riflessione che ha innescato riguardo agli algoritmi. Infatti, in questa controversia un elemento essenziale di novità, rispetto alle precedenti decisioni delle Corti statunitensi, è stata proprio la discussione incentrata sugli algoritmi come fonte di responsabilità per l'*interactive computer service*. Tanto che gli attori hanno sostenuto che l'utilizzo degli algoritmi era il discrimine essenziale per escludere l'applicazione della Sezione 230.

Nonostante l'esito negativo del processo per gli attori, che ha sancito l'irrilevanza dell'utilizzo di strumenti intelligenti nella gestione della piattaforma, è evidente che il passaggio dal tema della responsabilità del *social network* per contenuti inappropriati, all'analisi dell'influenza degli algoritmi nelle interazioni tra utenti ha spinto i giudici a riconsiderare la portata applicativa della Sezione 230.

Secondo l'argomentazione proposta dagli attori del giudizio, Facebook, avendo permesso a degli algoritmi di associazione e filtraggio di gestire i contenuti immessi da terzi sulla piattaforma, sarebbe andato ben oltre la sua funzione di semplice editore. Il *social network* avrebbe assunto così un ruolo attivo, proseguendo l'azione dell'autore originario e diventando un elemento causale essenziale nella diffusione del contenuto illecito.

---

[482] Così DALZELL, *Telecommunications Law – Facebook Immunized from Civil Liability Under Communications Decency Act Despite Using Algorithms to Recommend Content – Force v. Facebook, 934 F.3d 53 (2d Cir. 2019), cert. denied, 140 S. Ct. 2761*, in *Suffolk U. L. Rev.*, 2021, 600 ss.

[483] V. *Force v. Facebook, Inc.*, No. 18-397 (2d Cir. 2019).

Il concetto di *hosting provider* attivo è ben formulato anche nella giurisprudenza italiana ed europea[484] ed esclude l'applicabilità del regime di esenzione previsto dall'art. 16 D.lgs. 70/2003 – oggi ripreso dagli artt. 6 e 8 del *Digital Services Act* – che prevede l'esclusione della responsabilità se il prestatore non è a conoscenza dell'illiceità o agisce prontamente per rimuovere i contenuti.

Questa impostazione, seppur inizialmente contestata da alcune pronunce[485], è stata definitivamente confermata dalla Cassazione civile[486], che ha riconosciuto l'idea che l'*hosting provider* attivo sia presumibilmente a conoscenza dei contenuti illeciti, considerando le frequenti attività svolte dagli intermediari per migliorare i propri servizi e promuovere la diffusione dei contenuti.

Anche nel contesto penale, la conoscenza effettiva del contenuto è un elemento cruciale. Sebbene la giurisprudenza penale abbia avuto approcci diversi[487], passando dalla responsabilità per mancata rimozione di contenuto diffamatorio alla successiva esclusione di un obbligo di controllo *ex ante*, è evidente che il combinato disposto delle giurisprudenze civile e penale in ambito di *hosting provider* attivi possa portare a una forma di responsabilità quasi oggettiva per i *provider* che utilizzano strumenti automatizzati.

Infatti, se si assume che l'*hosting provider* abbia automaticamente conoscenza dei contenuti illeciti ogni volta che svolge un ruolo attivo nella gestione delle informazioni, e considerando che la maggior parte di questi operatori utilizza algoritmi per ottimizzare le prestazioni delle proprie piattaforme, si giunge a riconoscere un loro coinvolgimento diretto nella realizzazione dell'illecito.

Il caso *Force v. Facebook* ha evidenziato il rischio elevatissimo e imprevedibile che le macchine, attivate per scopi leciti, possano veicolare informazioni illecite o lesive a causa del *machine learning*, cioè dell'apprendimento autonomo. Ciò solleva la questione di come costruire un modello di responsabilità penale adeguato, capace di affrontare situazioni in cui l'algoritmo commette

---

[484] V. Trib. Milano, Sez. Spec. Propr. Ind. e Intellettuale, 9/09/2011, n. 10893, in cui l'*hosting provider* attivo viene definito come «il prestatore dei servizi della società dell'informazione il quale svolge un'attività che esula da un servizio di ordine meramente tecnico, automatico e passivo, e pone, invece, in essere una condotta attiva, concorrendo con altri nella commissione dell'illecito».
[485] Cfr. Trib. Torino, I Sez. Civ., 7/04/2017, n. 1928; Trib. Napoli Nord, ord. 3/11/2016.
[486] V. Cass. civ., Sez. I, 19 marzo 2019, n. 7708.
[487] Cfr. Cass. pen., Sez. V, 27/12/2016, n. 54946; Cass. pen., Sez. V, 8/11/2018, n. 12546.

autonomamente l'illecito, senza che l'essere umano ne sia consapevole o abbia la possibilità di intervenire.

Di fronte a queste problematiche, il caso *Force v. Facebook* rappresenta un campanello d'allarme e impone una riflessione urgente. In particolare, il giudice invita il legislatore a rivedere la Sezione 230, ritenendola ormai inadeguata[488].

Il ragionamento della Corte nel caso *Force* evidenzia quanto estesa sia divenuta l'applicazione dell'immunità prevista dal CDA a favore degli ISP, e sottolinea l'urgenza di rivedere il modo in cui questa norma viene interpretata e applicata nei tribunali.

Un'interpretazione più restrittiva del CDA sarebbe più coerente con le intenzioni originarie del legislatore, che mirava a tutelare il ruolo degli editori tradizionali, senza prevedere le sofisticate capacità algoritmiche che le piattaforme moderne oggi possiedono. Eppure, una semplice rilettura restrittiva potrebbe non bastare, in quanto potrebbe essere necessario aggiornare la Sezione 230 per adeguarla all'evoluzione tecnologica e alle nuove funzioni delle piattaforme *social*.

Il *Second Circuit* è uno dei diversi tribunali che si sono trovati ad affrontare il problema dell'applicazione del CDA ai *social media*. In particolare, ha valutato se Facebook potesse essere ritenuta responsabile per aver presumibilmente agevolato un'organizzazione terroristica nel compiere attacchi, e, adottando una lettura ampia del CDA che ha riconosciuto a Facebook l'immunità, si è allineato all'orientamento prevalente. Tuttavia, questa interpretazione non rispecchia lo spirito originario della norma, poiché oggi Internet ha capacità molto più avanzate nel connettere individui e gruppi. Le piattaforme *social*, sfruttando queste potenzialità, hanno superato il ruolo degli editori tradizionali e, per questo, non dovrebbero continuare a beneficiare della stessa immunità prevista dal CDA[489].

---

[488] In tal senso BACCIN, *Responsabilità penale dell'*internet service provider, cit., 96 ss e 102.

[489] Così ELEEY, *Internet Regulation – Second Circuit Follows Majority of Courts in Broad Application of Communications Decency Act Immunity – Force v. Facebook, Inc., 934 F.3d 53 (2d Cir. 2019),* in *Sufflok J. Trial & App. Advoc.*, 2021, 1, 178 ss.

CONCLUSIONI

Il presente elaborato ha esplorato il rapporto esistente tra diritto penale e responsabilità degli *Internet Service Provider* (ISP), proponendo una ricostruzione del quadro normativo e giurisprudenziale vigente a livello nazionale, europeo e in ottica comparata.

Anzitutto, dal lavoro di ricerca è emerso che la figura dell'*Internet Service Provider* rappresenta oggi un attore indispensabile per il funzionamento stesso della rete: senza gli ISP, infatti, non sarebbe possibile accedere a Internet né fruire delle modalità e dei servizi oggi conosciuti. La loro evoluzione storica mostra come, a partire dagli anni Novanta, questi siano passati dall'essere considerati meri fornitori di accesso alla rete a soggetti centrali, in grado di offrire non soltanto connettività, ma anche una pluralità di servizi collegati.

In particolare, l'*hosting provider*, da soggetto chiamato a svolgere un'attività di ordine meramente tecnico, automatico e passivo, ha iniziato a intervenire attivamente sui contenuti, portando così la giurisprudenza a elaborare la nozione di *hosting provider* attivo, a testimonianza del fatto che tali figure abbiano oramai assunto un ruolo che le rende potenzialmente partecipi nella prevenzione e/o nella realizzazione degli illeciti.

Inoltre, si è rilevato come il tema della responsabilità penale degli ISP risulti particolarmente complesso, non registrandosi un modello unitario di imputazione della responsabilità nei diversi sistemi giuridici, posto che i vari ordinamenti sono alla ricerca, in questa materia, di un equilibrio tra la tutela dei diritti fondamentali e l'esigenza di prevenire e reprimere i reati *online*.

È pacifico che, al pari di qualsiasi soggetto che realizzi una condotta penalmente rilevante, anche il *provider* possa essere chiamato a rispondere penalmente per reati commessi in forma diretta o in concorso. Al contempo, però, si registrano difficoltà interpretative e applicative nell'inquadrare giuridicamente le condotte tipiche nell'ambiente digitale.

Con specifico riferimento alla responsabilità omissiva degli ISP, infatti, si evidenzia una netta distinzione tra il controllo preventivo dei contenuti e l'intervento successivo alla loro pubblicazione.

Se da un lato la giurisprudenza e la dottrina prevalenti escludono che gravi sugli ISP un obbligo generale di sorveglianza preventiva – poiché questo comporterebbe forme di censura alla libertà di espressione e oneri eccessivamente gravosi per gli operatori – dall'altro, la Corte di Cassazione in alcune pronunce ha riconosciuto che i *provider* possono essere ritenuti responsabili ove consapevolmente non rimuovano contenuti manifestamente illeciti, concorrendo così con la propria inerzia alla prosecuzione dell'illecito. Altresì, come evidenziato, la recente evoluzione normativa dimostra come oggi possano configurarsi, in taluni settori, forme di responsabilità omissiva propria e non solo basate sull'art. 40, co. 2, c.p.

È stata poi analizzata l'ipotesi di responsabilità concorsuale *ex* art. 110 c.p., nel caso in cui l'attività del *provider* fornisca un contributo causale alla commissione di un illecito da parte degli utenti. Affinché si configuri il concorso nel reato, come noto, è necessario tanto un contributo oggettivo, che faciliti la realizzazione del reato, quanto la consapevole volontà di contribuire alla commissione dello stesso. Su questo punto, quanto al *provider*, sono emerse due posizioni opposte: da un lato, un orientamento maggioritario che ritiene applicabili i criteri generali del concorso di persone nel reato, riconoscendo che l'ISP possa concorrere penalmente qualora il suo apporto incida effettivamente sulla realizzazione dell'illecito; dall'altro, un approccio più garantista che sottolinea come l'attività del *provider* – che in linea di principio ha natura neutra e lecita – possa diventare penalmente rilevante solo in presenza di un dolo specifico e di una concreta possibilità di impedire il reato.

Accanto alle ipotesi di concorso commissivo, dunque, si è aperta una riflessione sulle ipotesi di concorso omissivo, nei casi in cui il *provider*, pur essendo a conoscenza del contenuto illecito, non provveda alla sua rimozione. Nel corso della ricerca è emerso come questa impostazione incontri dei limiti strutturali, considerato che la responsabilità per omissione presuppone che il reato non sia ancora consumato, mentre in ipotesi come la diffamazione *online* l'illecito si perfeziona nel momento stesso della pubblicazione del contenuto, rendendo più complessa l'imputazione omissiva all'ISP.

L'attività di ricerca in chiave comparatistica proposta nel presente lavoro ha messo inoltre in luce come negli Stati Uniti, originariamente, si fosse seguito il modello normativo europeo e, dunque, fosse stato adottato un approccio alla regolamentazione del *cyberspace* di tipo liberalista, volto cioè a favorire lo sviluppo del commercio elettronico e la diffusione della società dell'informazione.

Tuttavia, la situazione è mutata e le divergenze tra i due modelli sono, con il tempo, aumentate.

Negli Stati Uniti l'impianto normativo si caratterizza per una visione fortemente liberale, che privilegia la tutela della libertà di espressione e la protezione degli operatori digitali. Questa impostazione ha condotto all'adozione della *Section* 230 del *Communications Decency Act* del 1996, che ha introdotto un'ampia esenzione da responsabilità civile per gli ISP, anche in presenza di contenuti illeciti pubblicati dagli utenti.

Al contrario, l'Unione europea ha seguito un approccio più garantista e multilivello, ispirato al principio di precauzione e alla salvaguardia dei diritti fondamentali.

Un ulteriore elemento distintivo tra i due modelli riguarda l'ambito di applicazione della normativa: mentre la Direttiva *E-Commerce* e l'attuale *Digital Services Act* prevedono un regime di irresponsabilità condizionata e orizzontale, esteso tanto all'ambito civile quanto all'ambito penale, la *Section 230* limita espressamente la sua applicabilità alla responsabilità civile, escludendo ogni estensione al campo penale.

Inoltre, il confronto con il *Digital Millennium Copyright Act* e la disciplina europea mette in luce un altro rilevante divario: mentre negli USA il legislatore ha adottato un approccio settoriale, limitato alla tutela del diritto d'autore e basato sulla procedura di *notice and takedown*, l'Unione europea ha introdotto un sistema più ampio e generalista, applicabile a qualsiasi contenuto illecito.

La Direttiva *E-commerce*, tuttavia, non ha previsto un sistema compiuto di *notice and takedown*, ma ha introdotto il concetto di conoscenza effettiva come presupposto per imporre al *provider* l'obbligo di rimuovere i contenuti illeciti, generando così profonde incertezze interpretative. Con l'adozione del *Digital Services Act* il quadro europeo si è evoluto: pur mantenendo il principio della

conoscenza effettiva, il Regolamento ha introdotto l'obbligo per i *provider* di predisporre strumenti accessibili a chiunque per la segnalazione di contenuti illegali.

Da ciò è emerso che le nuove procedure devono essere digitali, semplici e dettagliate, così da consentire una rimozione dei contenuti illeciti più rapida ed efficace. In questo senso, all'esito dell'analisi comparatistica svolta, si può affermare che il DSA presenta alcune affinità con il modello statunitense del *Digital Millennium Copyright Act*, in quanto introduce una vera e propria procedura di *notice and action,* superando così le lacune del precedente impianto normativo.

BIBLIOGRAFIA

ABALDO, *Una prospettiva di regolamentazione degli ISP attraverso il* Digital Service Act, in *MediaLaws*, 2022, 1.

ACCINNI, *Profili di responsabilità penale dell'*hosting provider *"attivo"*, in *Arch. pen.*, 2017, 1.

AJMONE MARSAN, GUADAGNI, LENZINI, (2011), *Le reti a pacchetto*, in CANTONI, FALCIASECCA, PELOSI (a cura di) *Storia delle telecomunicazioni*, Firenze, 2011, 239.

ALÙ, *I problemi giuridici di* Internet*: il dibattito sul diritto all'uguaglianza digitale*, in *Agenda Digitale*, 2015,1.

ALÙ, *La* Governance *di* Internet *oltre gli Stati? Gli inediti tratti del futuro ecosistema digitale*, in *RIID*, 2022, 251.

ALLEGRI, Ubi Social, Ibi Ius*. Fondamenti costituzionali dei* social network *e profili giuridici della responsabilità dei* provider, Milano, 2018.

ALLEGRI, *Il diritto all'oblio e la libertà di informazione nel bilanciamento operato dalla Corte di giustizia*, in *Riv. it. inf. dir.*, 2022, 1.

ALMA, *Offesa alla reputazione del movimento LGBT e configurabilità del delitto di diffamazione*, in *Sist. pen.*, 2024, 5, 101.

AMMORI, *The "New" New York Times: Free Speech Lawyering in the age of Google and Twitter*, in *Harv. L. Rev.*, 2014, 8, 2259.

ANRÒ, Online hate speech*: la prospettiva dell'Unione europea. Tra regolamentazione della condotta dei prestatori dei servizi intermediari e ricorso al diritto penale*, in *Osservatorio sulle fonti*, 2023, 14.

ARENA, *La Convenzione di Budapest del Consiglio d'Europa sulla repressione della criminalità informatica*, in *CRIO Papers*, 2021, 3.

BACCIN, *Responsabilità penale dell'*Internet Service Provider *e concorso degli algoritmi negli illeciti* online*: Il caso* Force v. Facebook, in *Sist. pen.*, 2020, 5, 75.

BAFFA, MASSARO, *Pedopornografia* online*: strumenti di prevenzione e contrasto,* Roma, 2020.

BASSINI, *La rilettura giurisprudenziale della disciplina sulla responsabilità degli* Internet service provider*. Verso un modello di responsabilità 'complessa'?*, in *Federalismi.it*, 2015, 3, 2.

BASSINI, *La Cassazione e il simulacro del* provider *attivo:* mala tempora currunt, in *MediaLaws*, 2019, 2, 248.

BASSINI, *La libertà di espressione e* social network*, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione*, in *RIID*, 2021, 2, 43.

BENATTI, PORTONERA, *La responsabilità di diritto civile degli* Internet Service Providers. *Spunti dalla comparazione con la giurisprudenza statunitense*, in *NGCC*, 2024, 2, 476.

BENCHELL. *The Digital Millennium Copyright Act: A Review of the Law and the The Digital Millennium Copyright Act: A Review of the Law and the Court's Interpretation*, in *J. Marshall J. Computer & Info. L.*, 2022, 30.

BERNSTEIN, RAMCHANDANI, *Don't Shoot the Messenger! A Discussion of ISP Liability*, in *Canadian Journal of Law and Technology*, 2002, 2, 77.

BERNTHOL, *Copyright Infringement in Cyberspace: On-line Service Provider Liability on the Cyberfrontier*, in *Intell. Prop. L. Bull.*, 1997, 3.

BETZU, *Poteri pubblici e poteri privati nel mondo digitale*, in *Riv. GdP*, 2021, 2, 166.

BHATTACHARYA, ROY, *Contributory Liability Vis-a-Vis Strict Liability: Analyzing World Trends in ISP Liability Regime with Respect to the Indian Position*, in *GNLU L. Rev.*, 2012, 75.

BIASIN, *La neutralità della rete*, in *LawTech*, 2016, 12.

BIRRITTERI, *Contrasto alla disinformazione,* Digital Services Act *e attività di* private enforcement*: fondamento, contenuti e limiti degli obblighi di* compliance *e dei poteri di autonormazione degli operatori*, in *MediaLaws*, 2023, 2, 52.

BLENGINO, *I reati della rete e la costruzione dei rischi nello spazio digitale*, in *Antigone,* 2008, 3, 104.

BOLISANI, GOTTARDI, *Nascita ed evoluzione di* Internet, in GARRONE, MARIOTTI (a cura di), *L'economia digitale*, Bologna, 2001, 360.

BRANNON, *Section 230: An Overview*, in *Congressional Research Service*, 2024, 1.

BRASCHI, Social media *e responsabilità penale dell'*Internet Service Provider, in *MediaLaws*, 2020, 3, 157.

BRASCHI, *Il nuovo Regolamento sui servizi digitali: quale futuro per la responsabilità degli* Internet Service Provider?*,* in *Dir. pen. proc.*, 2023, 3, 367.

BRIGANTI, *Commercio elettronico: il Dlgs 70/2003 di attuazione della direttiva europea*, in *Altalex*, 2010, 1.

BUCCARELLA, *Il Secondo Protocollo addizionale alla Convenzione di Budapest e le nuove frontiere della cooperazione internazionale in ambito digitale. Quali rischi per la protezione dei dati personali nell'Unione europea?*, in *Quaderni AISDUE*, 2023, 8, 184.

BUGIOLACCHI, *Principi e questioni aperte in materia di responsabilità extracontrattuale dell'*Internet provider*. Una sintesi di diritto comparato*, in *Dir. inf.*, 2000, 829.

CABRERA, *Analysis of Section 230 under a Theory of Premises Liability: A Focus on Herrick v. Grindr and Daniel v. Armslist*, in *U. Miami Bus. L. Rev.*, 2021, 2, 53.

CADOPPI, VENEZIANI (a cura di), *Elementi di diritto penale. Parte generale*, Padova, 2023.

CAGGIANO, *La proposta* di Digital Service Act *per la regolazione dei servizi e delle piattaforme* online *nel diritto dell'Unione europea*, in *Quaderni AISDUE*, 2021, 1, 1.

CAMARELLA, *La responsabilità dell'*Internet Service Provider *alla luce della nuova direttiva sul diritto d'autore nel mercato unico digitale*, in *LawTech*, 2020, 1.

CAMISA, SIMONCINI, *Il fattore umano e la regolazione della* cybersecurity, in *Mondo Digitale*, 2024, 1.

CEDROLA, *La responsabilità penale dell'*Internet Service Provider *(ISP)*, in *Ius in Itinere*, 2018, 1.

CHARLES, ZAMANSKY, *Liability for Online Libel after Stratton Oakmont, Inc. v. Prodigy Services Co.*, in *Conn. L. Rev.*, 1996, 1173.

CISTERNA, *Il contrasto al terrorismo* online *e la tutela delle infrastrutture informatiche*, in *Dir. pen. proc.*, 2023, 11, 1431.

CITRON, WITTES, *The Problem Isn't Just Backpage: Revising Section 230 Immunity*, in *Geo. L. Tech. L. Rev.*, 2018, 7, 453.

COLLETTI, *Il compromesso tra diritto all'oblio e responsabilità dell'*internet service provider *nell'ottica dell'individuazione di rimedi diversi dalla deindicizzazione*, in *Dirittifondamentali.it*, 2024, 1, 339.

CONNER, *Cubby v. Compuserve, Defamation Law on the Electronic Frontier*, in *Geo. Mason Indep. L. Rev.*, 1993, 1, 227.

COSTA, *La responsabilità dell'*Internet Service Provider *per i reati in materia di diritto d'autore*, in *Giur. pen.*, 2022, 2, 1.

D'AGOSTINO, *Disinformazione e responsabilità delle piattaforme. Obblighi di attivazione e misure di compliance*, in *DPC.*, 2021, 4, 282.

D'ALTERIO, *ISP: la responsabilità per le pubblicazioni degli utenti. I criteri di imputazione delle responsabilità civile e penale a carico degli* Internet Service Provider *in base al d.lgs. n. 70/2003*, in *Altalex*, 2021, 1.

DALZELL, *Telecommunications Law - Facebook Immunized from Civil Liability under Communications Decency Act Despite Using Algorithms to Recommend Content - Force v. Facebook, 934 F.3d 53 (2d Cir. 2019), cert. denied, 140 S. Ct. 2761*, in *Suffolk U. L. Rev.*, 2021, 599.

DE GIOIA, *La responsabilità degli* internet service providers *in caso di pratiche commerciali scorrette*, in *NJus*, 2021, 1.

DE GREGORIO, *Il regime di responsabilità degli ISP alla luce della sentenza della Corte di Cassazione n. 54946/2016*, in *MediaLaws*, 2017, 1.

DE NATALE, *La responsabilità dei fornitori di informazioni in* Internet *per i casi di diffamazione* online, in *Riv. trim. dir. pen. ec.*, 2009, 509.

DE NATALE, *Responsabilità penale dell'*internet service provider*, per omesso impedimento e per concorso nel reato di pedopornografia*, in GRASSO, PICOTTI, SICURELLA (a cura di), *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011, 295.

DELSIGNORE, *Il sistema U.S.A.*, in *AIDA*, 2014, 1, 3.

DI CERBO, *La tutela dell'identità nell'ambiente digitale alla luce delle norme europee*, in *EJPLT*, 2023, 2, 253.

DI CIOMMO, *Programmi-filtro e criteri di imputazione/esonero della responsabilità* on-line*. A proposito della sentenza Google/Vivi Down*, in *Dir. inf.*, 2010, 829.

DI TANO, *Prospettive* de iure condendo *sulla responsabilizzazione dei* content provider, in *Inf. dir.*, 2017, 1-2, 113.

D'URSO, *I profili informatici nella valutazione della responsabilità dell'*Hosting Provider, in *RIID*, 2021, 1, 79.

ELEEY, *Internet Regulation - Second Circuit Follows Majority of Courts in Broad Application of Communications Decency Act Immunity - Force v. Facebook, Inc.934 F.3d 53 (2d Cir. 2019)*, in *Suffolk J. Trial & App. Advoc.*, 2021, 1, 169.

FABIANO, *Il liberal-protezionismo digitale statunitense fra difesa della* leadership *nel mercato tecnologico e sicurezza nazionale*, in *DPCE online*, 2023, 3, 2335.

FANCHER, DUNN, *The Trend toward Limited Internet Service Provider (ISP) Liability for Third Party Copyright Infringement on the Internet: A United States and Global Perspective*, in *Bus. L. Int.*, 2002, 143.

FEROLETO, *I diritti umani dal giusnaturalismo alla nuova era digitale: i processi di tutela dei soggetti socialmente vulnerabili nel cyberspazio e la responsabilità dell'*internet service provider, in *TIGOR*, 2024, 1, 94.

FERRARESE, *La responsabilità civile degli* internet provider*: un'analisi degli artt. 14 - 17 del d.lgs. n. 70/2003*, in *Jei-Jus e Internet*, 2008, 1.

FERRARI, *L'*executive order *sulla prevenzione della censura* online*: quali effetti sull'autonomia dei* social network*?,* in *DPCE online*, 2020, 2, 1145.

FERRARIO, *Gli algoritmi come decisori nel contrasto al terrorismo* online*. Alcune riflessioni a partire dal Regolamento (UE) 2021/784*, in *DPCE Online*, 2025, 2, 631.

FERRARIO, *La portata transnazionale del regolamento (UE) 2021/784 e i possibili profili di incompatibilità con le normative di Stati terzi: un'analisi comparata*, in IMPARATO, PIGNATIELLO (a cura di), *La libertà di espressione nel diritto comparato tra stato di diritto e stati di emergenza*, Torino, 2024, 339.

FINOCCHITO, Digital Services Act*, che cambia per le aziende italiane*, in *Agenda Digitale*, 2024, 1.

FIORINELLI, *L'attuale ruolo del* provider *nella società digitale: modelli di responsabilità penale*, in *Leg. pen.*, 2022, 4, 1.

FLOR, *Tutela penale e autotutela tecnologica, dei diritti d'autore nell'epoca di* internet*. Un'indagine comparata in prospettiva europea ed internazionale,* Padova, 2010, 604.

FLOR, Social network *e violazioni penali dei diritti d'autore. Quali prospettive per la responsabilità del fornitore del servizio?*, in *Riv. trim. dir. pen. econ.*, 2012, 3, 647.

FLOR, *Dalla* 'Data retention' *al diritto all'oblio. dalle paure Orwelliane alla recente giurisprudenza della corte di giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive* 'de jure condendo', in *Dir. inf.*., 2014, 4, 223.

FOTI, *Regolamentazione digitale: il* Digital Services Act *e le piattaforme* online, in *Altalex*, 2024, 1.

FRAGASSO, *La regolamentazione europea sulla* Mutual Legal Assistance *(MLA) nel* cyberspace, in FONDAZIONE OCCORSIO (a cura di), *Intelligenza artificiale e giurisdizione penale*, Roma, 2021, 22.

FRANCESCHETTI, *Dolo*, in *Altalex*, 2016, 1.

FROSINI, *L'orizzonte giuridico dell'*Internet, in *Dir. inf.*, 2000, 2, 271.

FROSINI, *Il costituzionalismo nella società tecnologica*, in *Dir. inf.*, 2020, 3, 465.

FUMAGALLI, *La responsabilità penale del* provider, in *Salvis Juribus*, 2020, 1.

FUMO, *La diffamazione mediatica*, Torino, 2011.

GARGANI, *Tra sanzioni amministrative e nuovi paradigmi punitivi: la legge delega di 'riforma della disciplina sanzionatoria' (art. 2 l. 28.4.2014 n. 67)*, in *Leg. pen.*, 2015, 1.

GARGANI, *La posizione di garanzia*, in *Giur. it.*, 2016, 214.

GARGIULO, *La* Declaration on a common understanding of international law in cyberspace *del Consiglio dell'Unione europea*, in *Osservatorio sulle attività delle organizzazioni internazionali e sovranazionali, universali e regionali, sui temi di interesse della politica estera italiana*, Roma, 2025.

GIRARDI, *Libertà e limiti della comunicazione nello spazio pubblico digitale*, in *Federalismi.it*, 2024, 17, 150.

GOLDMAN, *Online User Account Termination and 47 U.S.C. § 230 (c)(2)*, in *U.C. Irvine L. Rev.*, 2012, 659.

GRANDINETTI, *La responsabilità dell'*internet provider *tra* privacy *e diritto d'autore*, in BOMBI, ORIOLES (a cura di), *Nuovi valori dell'italianità nel mondo. Tra identità e imprenditorialità*, Udine, 2011, 141.

GRAZIANI, *Intelligenza artificiale e fonti del diritto: verso un nuovo concetto di* soft law*? La rimozione dei contenuti terroristici* online *come* case-study, in *DPCE Online*, 2022, 1473.

GULLO, *I delitti contro l'onore*, in PIERGALLINI, VIGANÒ (a cura di), *Reati contro la persona e contro il patrimonio*, Torino, 2015.

HAMDANI*, Who's Liable for Cyberwrongs?*, in *Cornell L. Rev.*, 2002, 902.

HILTON, *An ethics analysis of the Digital Millennium Copyright Act*, in *Information System*, 2004, 2, 495.

HIRNING, *Contributory and Vicarious Copyright Infringement in Computer Software*, in *Chi-Kent J. Intell. Prop.*, 2006, 1, 10.

HUA, *Establishing Certainty of Internet Service Provider Liability and Safe Harbor Regulation*, in *NTU L. Rev.*, 2014, 1, 1.

IASELLI, Internet Service Provider. *Guida all'ISP: cos'è, regime e tipologie di responsabilità*, in *Altalex*, 2019, 1.

IMPERADORI, *La responsabilità dell'*Internet Service Provider *per la violazione del diritto d'autore: un'analisi comparata*, in *LawTech*, 2014, 1.

INGRASSIA, *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine*, in LUPARIA, Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione procesuale*, Milano, 2012.

JEANNERET, *The Digital Millennium Copyright Act: Preserving the Traditional Copyright Balance*, in *Fordham Intell. Prop. Media & Ent. L.J.*, 2002, 1, 157.

JOHNSON, *Defamation in Cyberspace: A Court Takes a Wrong Turn on the Information Superhighway in Stratton Oakmont, Inc. v. Prodigy Services Co.*, in *Ark. L. Rev.*, 1996, 3, 589.

KAMDAR, *CDA 230: The Most Important Law Protecting Internet Speech*, in *Electronic Frontier Found.*, 2012, 1.

KOSSEFF, *The Gradual Erosion of the Law that Shaped the Internet: Section 230's Evolution over Two Decades*, in *Colum. Sci. & Tech. L. Rev.*, 2016, 1, 2.

KOSSEFF, *Twenty Years of Intermediary Immunity: The US Experience*, in *Scripted*, 2017, 1, 5.

LADEIA, *The Internet Service Provider Secondary Liability: A Comparative Analysis of Brazilian and United States Legislation and Case Law*, in *Int'l Media & Ent. L.*, 2016, 2, 187.

LARINNI, *Garantismo europeista: un ossimoro? A proposito dell'accesso abusivo ad un sistema informatico o telematico (615-ter c.p.)*, in *Criminalia*, 2019, 301.

LAVAGNINI, *La responsabilità degli* Internet Service Provider *e la nuova figura dei prestatori di servizi di condivisione* online *(art. 17)*, in LAVAGNINI (a cura di), *Il diritto d'autore nel mercato unico digitale: direttiva (UE) 2019/790 e d. lgs. n. 177/2021 di recepimento*, Torino, 2022, 209.

LEINER, CERF, CLARK, KAHN, KLEINROCK, LYNCH, POSTEL, ROBERTS, WOLFF, *The Past and Future History of the Internet*, in *Communications of the ACM*, 1997, 2, 102.

LESSIG, *Code. Version 2.0*, New York, 2006.

LICHTMAN, POSNER, *Holding Internet Service Providers Accountable*, in *Sup. Ct. Econ. Rev.*, 2006, 221.

LONGO, *Diffamazione via* mass media *e* social network*, tutele e risarcimenti. Requisiti, circostanze aggravanti e principali cause di esclusione del reato alla luce della prevalente giurisprudenza degli ultimi anni*, in *Altalex*, 2020, 1.

LUKMIRE, *Can the Courts Tame the Communications Decency Act?: The Reverberations of Zeran v. American Online*, in *N.Y.U. Ann. Surv. Am. L.*, 2010, 2, 371.

MACILOTTI, *Il contrasto alla pedopornografia* online*: esperienze italiane e francesi a confronto*, in *RCVS*, 2011, 1, 81.

MAESTRI, Lex informatica*. Diritto, persona e potere nell'età del cyberspazio,* Napoli, 2015.

MAESTRI, *Stupri digitali: una questione di governance del cyberspazio*, in *ADFD*, 2024, 27, 26.

MANNA, *Considerazioni sulla responsabilità penale dell'*Internet provider *in tema di pedofilia*, in *Dir. inf.*, 2001, 145.

MANSOURI, *Money, magic, and machines: International Telecommunication Union and liberalisation of telecommunications networks and services (1970s–1990s)*, in *London R. of Inter. L.*, 2023, 2, 231.

MARSICO, *La responsabilità civile dell'*Internet Service Provider*: sulla dibattuta* species *del contratto di accesso*, in *Dir. amm.*, 2022, 1.

MARTANI, *La* net neutrality *alla luce del Regolamento UE n. 2120/2015 e delle Linee Guida BEREC*, in *Cibersp. dir.*, 2017, 3.

MARTIN, *Sulla diffamazione e sull'istigazione a delinquere: distinzioni e profili applicativi*, in *Camm. dir.*, 2020, 1.

MARTINELLI, *L'autorità privata del* provider, in SIRENA, ZOPPINI (a cura di), *I poteri privati e il diritto della regolazione. A quarant'anni da «Le autorità private» di C.M. Bianca*, Roma, 2018, 555.

MARTORANA, Digital Markets Act *(DMA), la Commissione individua i 6 gatekeeper*, in *Altalex*, 2023, 1.

MASSA, *L'evoluzione della responsabilità degli* internet service providers*: dalla direttiva e-commerce al* Digital Services Act, in *Giustizia*, 2022, 2, 42.

MATTARELLA, *La futura Convenzione ONU sul* cybercrime *e il contrasto alle nuove forme di criminalità informatica*, in *Sist. pen.*, 2022, 3, 41.

MAZZANTI, *Il delitto di diffamazione al tempo dei* social network*: punti fermi e spunti problematici*, in PASSAGLIA, POLETTI (a cura di), *Nodi virtuali, legami informali:* Internet *alla ricerca di regole*, Pisa, 2016, 207.

MERCIER, *The Communications Decency Act, Congress' First Attempt to Censor Speech over the Internet*, in *Loy. Consumer L. Rev.*, 1997, 3, 274.

MERCURIO, *Il* cyberspace*: la sovranità nel quinto dominio*, in *Camm. dir.*, 2024, 2.

MICELI, *Profili evolutivi delle responsabilità in Rete: il ruolo* degli Internet Service Provider *tra prevenzione e repressione*, in *MediaLaws*, 2017, 1, 106.

MIRTI, *La disciplina giuridica del* cyberspace*. Una panoramica sulle problematiche attuali e le principali linee evolutive*, in *Opinio Juris*, 2016, 3, 1.

MOLINARI, *Nascita, evoluzione e funzionamento della rete*, in *Filodiritto*, 2008, 1.

MONACO, *Prolegomena alla riforma del diritto penale dell'informatica nell'ordinamento giuridico della repubblica di San Marino*, in *Studi Urb., A - Sci. Giur. Pol. Econ.*, 2017, 3-4, 337.

MONTI, *La* network neutrality *e la responsabilità dei* provider, in *Ict Lex*, 2009. 1.

MORGESE, *Moderazione e rimozione dei contenuti illegali* online *nel diritto dell'UE*, in *Federalismi.it*, 2022, 1, 80.

MORGESE, *Proposta di* Digital Services Act *e rimozione dei contenuti illegali* online, in CAGGIANO, CONTALDI, MANZINI (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2021, 31.

MOROTTI, *Luci e ombre delle piattaforme di* crowdfunding donation, in *Pers. mer.*, 2024, 4, 1301.

NARDI, *I discorsi d'odio nell'era digitale: quale ruolo per l'*internet service provider*?*, in *DPC*, 2019, 1.

NEWHALL, *Criminal Copyright Enforcement Against Filesharing Services*, in *North Carolina Journal of Law and Technology*, 2013, 101.

NOTARI, *La controversa responsabilità dell'*Internet Service Provider *in materia di* privacy *nella giurisprudenza europea e interna: il caso Google*, in *Amm. camm.*, 2016, 1.

NOVELLI, *Il social giudizioso. La giurisprudenza italiana sulla responsabilità civile degli* Internet Service Providers, in *RIID*, 2019, 1, 97.

OROFINO, *La politica europea delle telecomunicazioni (comunicazioni elettroniche): la nuova sfida della* net-neutrality, in *Eurojus*, 2017, 1.

PAMPANIN, *I nuovi protagonisti del mondo digitale tra neutralità della Rete e accesso all'informazione*, in *Inf. dir.*, 2017, 1-2, 237.

PANATTONI, *Gli effetti dell'automazione sui modelli di responsabilità: il caso delle piattaforme* online, in *DPC.*, 2019, 2, 33.

PANTAZIS, *Zeran v. America Online, Inc.: Insulating Internet Service Providers from Defamation Liability*, in *Wake Forest L. Rev.*, 1999, 531.

PASQUALE, *Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power*, in *Theoretical Inquiries L.*, 2016, 24, 487.

PASSAGLIA, *Cenni* sull'Online Copyright Infringement Liability Limitation Act *statunitense*, in PASSAGLIA (a cura di), *Tutela del diritto d'autore e oscuramento dei siti* web, Corte cost., Servizio Studi – Area di diritto comparato, 2015, 95.

PELLICONI, *La pornografia minorile nella sfera privata e il reato di pedopornografia virtuale. Considerazioni critiche alla luce di Cass. Pen., Sez. III, Sent. N. 22265/2017*, in *Giustizia*, 2018, 2.

PELLIZZONI, Gatekeeper*: vecchie idee o nuove soluzioni?,* in *CERIDAP*, 2024, 1, 214.

PERDONÒ, *Le responsabilità penali collegate all'uso di* Internet *fra comparazione e prospettive di riforma*, in *Dir. inf.*, 2007, 323.

PETRINI, *La responsabilità penale per i reati via* internet, Napoli, 2004.

PETRUSO, *La responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto,* Torino, 2019.

PEZZANO, BUONGIORNO, P*rofili di criticità del nuovo art. 174-sexies Legge n. 633/1941 in relazione al D. Lgs. n. 231/2001*, in *Giur. Pen. Web*, 2024, 11.

PEZZUTO, *Contenuti terroristici* online*: l'Unione europea lavora a nuove norme per prevenirne la diffusione*, in *DPC*, 2019, 4, 35.

PICA, *La tutela della libertà di informazione nel* Digital Services Act *tra contrasto alle "manipolazioni algoritmiche" e limiti alla* content moderation, in *MediaLaws*, 2024, 1, 11.

PICOTTI, *Profili penali delle comunicazioni illecite via* Internet, in *Dir. inf.*, 1999, 2, 283.

PICOTTI, *Fondamento e limiti della responsabilità penale dei* Service-Providers *in* Internet, in *Dir. pen. proc.*, 1999, 379.

PICOTTI, *La responsabilità penale dei* service providers *in Italia*, in *Dir. Pen. proc.*, 1999, 501.

PICOTTI, *La legge contro lo sfruttamento sessuale dei minori e la pedopornografia in Internet (L. 6 febbraio 2006, n. 38) (Parte seconda)*, in *Studium Iuris*, 2007, 1196.

PICOTTI, *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. eco.*, 2011, 4, 827.

PICOTTI, *Reati informatici, riservatezza, identità digitale*, contributo disponibile sul sito dell'AIPDP, s.d., 1.

PIETRELLA, *Reati informatici e concorso di norme: come l'evoluzione tecnologica informa il diritto penale. Il caso delle* Botnets, in *DisCrimen.*, 2021, 1.

PIETRELLA, *L'incidenza dello sviluppo tecnologico sulla tenuta di condotte offensive. Rilevanza giuridica della comunicazione degradante online nel reato di diffamazione*, in *Sist. pen.*, 2023, 10, 5.

PIRAINO, *Spunti per una rilettura della disciplina giuridica degli* Internet Service Provider, in *d/SEAS Working Paper*, 2018, 152.

PIROZZOLI, *La responsabilità dell'*Internet Service Provider*. Il nuovo orientamento giurisprudenziale nell'ultimo caso Google*, in *AIC*, 2012, 3, 1.

POLLICINO, *La prospettiva costituzionale sulla libertà di espressione nell'era di* Internet, in *MediaLaws*, 2018, 1, 49.

POLLICINO, *Regolazione e innovazione tecnologica nell' "ordinamento della rete"*, in *AIC*, 2025, 2, 119.

POMA, *L'interpretazione del regolamento 2015/2120 tra principio di neutralità della rete, principio di non discriminazione e* Internet *aperta*, in *MediaLaws*, 2021, 3, 227.

PURPURA, *Osservazioni sul* Digital Services Act*: responsabilità e gestione del rischio nella prestazione di servizi intermediari*, in *Comp. dir. civ.*, 2022, 3, 1035.

RASI, *Progresso tecnologico e sviluppo civile: la tutela dei dati personali*, in RASI (a cura di), *Innovazioni tecnologiche e* privacy*. Sviluppo economico e progresso civile*, Roma, 2005, 7.

REIDENBERG, *Lex Informatica: The formulation of Information Policy Rules Through Technology*, in *Texas L. R.*, 1998, 568.

RODOTÀ, *Una Costituzione per* Internet*?*, in *Pol. dir.*, 2010, 3, 337.

ROJSZCZAK, *Gone in 60 Minutes: Distribution of Terrorist Content and Free Speech in the European Union*, in *Democracy & Sec.*, 2024, 179.

ROMITO, Digital Services Act *(DSA): cosa prevede e quali sono le implicazioni?*, in *Il QG*, 2023, 1.

ROSSELLO, *Gli obblighi informativi del prestatore di servizi,* in ROSSELLO, FINOCCHIARO, TOSI (a cura da), *Commercio elettronico*, Torino, 2007, 135.

RUGGIERO, *Individuazione nel ciberspazio del soggetto penalmente responsabile e ruolo dell'*internet provider, in *Giur. mer.*, 2001, 593.

RUGOLO, *Cos'è il* cyberspace, in *Difesa Online*, 2024, 1.

RUM, *Le nuove frontiere della normativa sui servizi digitali nel mercato unico europeo: si rafforza la protezione dei diritti fondamentali degli utenti* online

con la garanzia pubblicistica delle Authorities*. Il* Digital Services Act, in *Dir. amm.*, 2022, 1.

RUOTOLO, *Le fonti dell'ordinamento internazionale e la disciplina della Rete*, in *DPCE online*, 2021, 701.

RUOTOLO, *Le proposte europee di riforma della responsabilità dei fornitori di servizi su* Internet, in *RIID*, 2022, 1, 17.

RUSSO, *La responsabilità dei* providers, in *SalvisJuribus*, 2022, 1.

SABIA, *L'*enforcement *pubblico del* Digital Services Act *tra Stati membri e Commissione europea: implementazione, monitoraggio e sanzioni*, in *MediaLaws*, 2023, 2, 88.

SANTARELLI, *Lotta* al cyber *crimine, ecco il secondo protocollo addizionale alla convenzione di Budapest: le finalità*, in *Cybersecurity360*, 2023, 1.

SARTOR, VIOLA DE AZEVEDO CUNHA, *Il caso Google e i rapporti regolatori USA/EU*, in *Dir. inf.*, 2014, 657.

SCENNA, *Il bilanciamento tra i diritti d'autore e i diritti fondamentali alla luce della direttiva UE 2019/790. Note alla sentenza della Corte di giustizia europea*, in *DPCE Online*, 2022, 3, 1759.

SCHWARTZ, *The Hidden and Fundamental Issue of Employer Vicarious Liability,* in *S. Cal. L. Rev.*, 1996, 1739.

SCIACOVELLI, *Attività ostili nel ciberspazio: il quadro normativo internazionale e dell'UE e l'importanza di istituire un'Unità congiunta per il ciberspazio*, in GARGIULO, INGRAVALLO (a cura di), *Osservatorio sulle attività delle organizzazioni internazionali e sovranazionali, universali e regionali*, Napoli, 2022, 10.

SCORZA, *In principio era* Internet *e lo immaginavamo diverso*, in *RIID*, 2022, 1, 13.

SEGAL, *A short history of Internet protocols*, in *CERN IT-PDP-TE*, 1995, 1.

SEMINARA, *La responsabilità penale degli operatori su* internet, in *Dir. inf.*, 1998, 1.

SENOR, *Convenzione di Budapest: le modifiche al c.p.p. ed al codice della* privacy, in *Altalex*, 2008, 1.

SERINI, *La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europee e italiana*, in *RIID*, 2023, 2, 41.

SGANGA, *Dall'armonizzazione alla frammentazione: obiettivi e fallimenti della Direttiva* Copyright *(2019/790/UE) in materia di ricerca, educazione e accesso al patrimonio culturale*, in *RIID*, 2023, 1, 47.

SHAHIN, *The role of the International Telecommunication Union*, in *Wereldbeeld*, 2010, 11.

SICA, D'ANTONIO, *La procedura di de-indicizzazione*, in *Dir. inf.*, 2014, 703.

SIEBER, *Responsabilità penali per la circolazione di dati nelle reti internazionali di* computer. *Le nuove sfide di* Internet (trad. it. a cura di SFORZI), in *Riv. trim. dir. pen. econ.*, 1997, 3, 775.

SPAGNOLETTI, *La responsabilità del* provider *per i contenuti illeciti di* Internet, in *Giur. mer.*, 2004, 1922.

SPINOGLIO, *Contenuti illeciti e responsabilità degli ISP: tutto quello che da sapere*, in *Agenda Digitale*, 2019, 1.

STELLA, *Il contrasto alla diffusione dei contenuti terroristici* online *a seguito dell'adozione del* Digital Services Act*: riflessi sulla tutela della libertà di espressione*, in *DPCE Online*, 2025, 2, 797.

SYKES, *The Economics of Vicarious Liability*, in *Yale L.J.*, 1984, 1231.

TABARELLI DE FATIS, *Prospettive di riforma del delitto di diffamazione, con particolare riferimento alla diffamazione* online, in PICOTTI (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013, 193.

TAVERNITI, *Profili di responsabilità dell'*internet service provider *tra disciplina vigente e nuove esigenze di tutela*, in *Camm. dir.*, 2022, 2.

TEDESCHI TOSCHI, BERNI FERRETTI, Social media*, profili artificiali e tutela della reputazione. Come l'avvento dei* social bot *per la gestione dei profili* social *possa rappresentare una grave minaccia per la reputazione delle persone e quali potrebbero essere le risposte a tale pericolo*, in *RIID*, 2021, 2, 107.

TORMEN, *La linea dura della Cassazione in materia di responsabilità dell'*hosting provider *(attivo e passivo)*, in *NGCC*, 2019, 5, 1039.

USMAN, *Guideline on Internet Service Providers' (ISPS) Liability Regime in the United States*, in AHMADU (a cura di), *Perspectives on Nigerian Law*, Sokoto, 2017, 1.

VASINO, *Censura "privata" e contrasto all'*hate speech *nell'era delle* Internet Platforms, in *Federalismi.it*, 2023, 4, 130.

VERRI, *Contenuto ed effetti (attuali e futuri) della Direttiva 2011/93/UE. Approvate dal legislatore europeo nuove norme contro l'abuso, lo sfruttamento sessuale dei minori e la pornografia minorile*, in *DPC*, 2012, 1.

VICINANZA, *La responsabilità delle piattaforme digitali nei confronti dei contenuti illegali: dal caso* Telegram *al* Digital Services Act, in *Quaderni AISDUE*, 2025, 1, 1.

VISCONTI, *L'attuazione della direttiva europea sul commercio elettronico e sui servizi della società dell'informazione*, in *Diritto.it*, 2004, 1.

WAN, *Monopolistic Gatekeepers' Vicarious Liability for Copyright Infringement*, in *Regent U. L. Rev.*, 2010, 65.

YEN, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, in *Geo. L.J.*, 2000, 1833.

ZANCAN, *La nuova direttiva sul diritto d'autore e sui diritti connessi nel mercato unico digitale*, in *MediaLaws*, 2019, 2, 338.

ZEPEDA, *A&M Records, Inc. v. Napster, Inc.*, in *Berkeley Tech. L.J.*, 2002, 71.

ZICCARDI, *La libertà di espressione in* Internet *al vaglio della Corte Suprema degli Stati Uniti*, in *Quad. cost.*, 1998, 1, 123.