UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

DIPARTIMENTO DI GIURISPRUDENZA

DOTTORATO DI RICERCA IN
"DIRITTO DELL'ECONOMIA"
XXXIV CICLO

Settori scientifici-disciplinari
IUS/01 e IUS/02 - Diritto privato e Diritto privato comparato

LA RESPONSABILITÀ DELL'INTERNET SERVICE PROVIDER

INTERNET SERVICE PROVIDER LIABILITY

Coordinatore:
Prof. Massimo Iovane

Candidata:
Dott. Flavia Stefanelli

Tutor:
Prof. A. Procida Mirabelli di Lauro

Anno Accademico 2020/2021

INDICE

CAPITOLO PRIMO

LE ATTIVITÀ DELL'INTERNET SERVICE PROVIDER: TIPOLOGIE E SERVIZI OFFERTI IN RETE

1. La responsabilità degli intermediari informatici nell'era digitale **7**

2. ISP e le diverse attività svolte in rete **15**

2.1 Mere conduit **17**

2.2 Caching **19**

2.3 Hosting (attivo e passivo) **21**

3. Gli ulteriori servizi d'informazione e di comunicazione dell'ISP. **28**

3.1. La comunicazione interpersonale **28**

3.1.1 E-mail e mailing list **29**

3.1.2 Newsgroup **31**

3.1.3 Instant Messaging e chat **32**

3.2 Content provider **33**

3.3 La fornitura di servizi applicativi via Internet: ASP **34**

3.4 Servizi accessori **35**

3.4.1 Bullettin Board Sistem **39**

4. Profili conclusivi **39**

CAPITOLO SECONDO

CRITERI DI IMPUTAZIONE DELLA RESPONSABILITÀ CIVILE DELL'INTERMEDIARIO DELLA RETE. UNA LETTURA (ANCHE) IN CHIAVE COMPARATISTICA

1. Responsabilità del provider e possibili criteri di imputazione **42**

1.1 *Strict liability* e teoria del rischio d'impresa **45**

1.2 *Vicarious liability* e responsabilità per il fatto altrui **48**

1.3 Ricorso alla responsabilità per i danni cagionati da cose in custodia **49**

1.4 Ricorso alla responsabilità per esercizio di attività pericolosa **54**

1.5 Approdo al criterio di imputazione a carattere colposo **57**

2. La responsabilità civile degli intermediari della rete nel sistema americano **59**

3. La responsabilità civile degli intermediari della rete nel modello europeo **78**

4. La responsabilità del provider nell' esperienza inglese **85**

5. La responsabilità del provider nell' esperienza francese **91**

6. La responsabilità del provider nell' esperienza tedesca **102**

CAPITOLO TERZO

LA RESPONSABILITÀ DEGLI INTERMEDIARI INFORMATICI NELL'ORDINAMENTO ITALIANO. VERSO LA "RESPONSABILIZZAZIONE" DEL PROVIDER…

1. Le posizioni della giurisprudenza italiana prima del recepimento della direttiva europea **108**

2. Il Decreto 70/2003 e il recepimento della Direttiva europea: un quadro d'insieme. **117**

   2.1 La normativa italiana in materia di intermediazione informatica: criterio della neutralità e carattere compromissorio della disciplina **129**

3. Profili di responsabilizzazione del provider: il requisito della conoscenza e il superamento del sistema qualificato **131**

4. *Segue*. Profili di responsabilizzazione del provider: host provider attivo, sistemi di algoritmi e filtraggio e onere della prova **137**

5. I poteri inibitori esperibili in ambiente digitale. Quali i doveri dei provider? **162**

6. Il "*Revenge Porn*": i primi passi concreti del legislatore **169**

7. Profili conclusivi **174**

CAPITOLO QUARTO

DIRITTO ALL'OBLIO E RIEVOCAZIONE STORICA NELL'ERA DIGITALE

1. Il diritto all'oblio e l'avvento dell'era digitale **177**

2. La protezione dei dati personali alla luce del nuovo Regolamento europeo **183**

3. Il diritto all'oblio nella giurisprudenza comunitaria **191**

4. Il diritto all'oblio, il diritto di cronaca e la rievocazione storica nella giurisprudenza italiana **203**

BIBLIOGRAFIA **217**

CAPITOLO PRIMO

Le attività dell'Internet Service Provider: tipologie e servizi offerti in rete

SOMMARIO: 1. La responsabilità degli intermediari informatici nell'era digitale. - 2. ISP e le diverse attività svolte in rete. - 2.1 Mere conduit. - 2.2 Caching. - 2.3. Hosting (attivo e passivo). - 3. Gli ulteriori servizi d'informazione e di comunicazione dell'ISP. - 3.1 La comunicazione interpersonale. 3.1.1 E-mail e mailing list. - 3.1.2 Newsgroup. - 3.1.3 Instant Messaging e chat. - 3.2 Content provider. - 3.3 La fornitura di servizi applicativi via Internet: ASP. - 3.4 Servizi accessori. - 3.4.1 Bullettin Board Sistem. - 4. Profili conclusivi.

1. La responsabilità degli intermediari informatici nell'era digitale

È il 6 agosto del 1991 quando un ricercatore del CERN, Tim Berners-Lee, pubblicò il primo sito web della storia. Bisognerà aspettare il 30 aprile 1993 perché il CERN decida di rendere pubblica la tecnologia alla base del World Wide Web in modo che sia liberamente implementabile da chiunque.

Da allora, la responsabilità dell'Internet Service Provider rappresenta una delle questioni maggiormente complesse e controverse poste dall'avvento di quella che oramai è comunemente nota come "era digitale"[1].

La modernità pone l'operatore del diritto di fronte a nuove sfide derivanti dalla sempre crescente diffusione di strumenti tecnologici di comunicazione e dalla correlata necessità di adeguare le norme giuridiche all'evoluzione, al fine di fornire tutela effettiva ai cittadini e regolare i diversi ambiti di funzionamento.

Dalla lettura dei plessi normativi in materia, quali la direttiva 2000/31/CE dell'8 giugno 2000 e la direttiva 2001/29/CE del 22 maggio 2001, emerge come la regolamentazione della

[1] G. PASCUZZI, *Il diritto nell'era digitale*, Bologna, 2016, p. 17 ss.; G.M. RICCIO, *La responsabilità civile degli Internet providers*, Torino, 2002, *passim*; M. DE CATA, *La responsabilità civile dell'Internet service provider*, 2010, p. 17 ss.

responsabilità dei prestatori intermediari dei servizi della rete telematica intercetti "inevitabilmente la disciplina di uno dei beni più importanti della società contemporanea: l'informazione"[2].

Il momento più avanzato dello sviluppo della tecnologia e della comunicazione è rappresentato proprio dal complesso fenomeno dello sviluppo di Internet, divenuto "propulsore di pluralismo" [3] che consente la diffusione dei dati in piena libertà ed autonomia. Benché spesso Internet venga comunemente individuata come l'infrastruttura della rete o, addirittura, come il soggetto che la gestisce, con tale termine non si indica una realtà fisica o tangibile, ma il fenomeno telematico conseguente alla connessione attraverso l'uso di reti locali di comunicazione esistenti.

La possibilità di colloquio tra gli elaboratori si fonda sull'esistenza di mezzi di telecomunicazione in grado di veicolare informazioni e questo dipende da due fattori fondamentali: l'esistenza di protocolli comuni di comunicazione, ossia sistemi di regole condivise utilizzabili dei computer indipendentemente dai loro programmi, e l'elaborazione di un sistema di indirizzi che consente di individuare univocamente ogni elaboratore presente in rete e perciò di instradare correttamente le informazioni immesse da e verso quello elaboratore.

Nelle attuali società dell'informazione[4] oramai si assiste ad un sempre più imponente fenomeno di "democratizzazione dei meccanismi di produzione dell'informazione"[5]. Così come è stato ben evidenziato dalla Corte EDU[6], ogni utente si trasforma in utente attivo che può con la sola connessione alla rete diffondere e condividere in tempo reale il frutto del proprio lavoro, il proprio pensiero, video, immagini *et similia.*

Internet, essendo costituita da una serie indefinita e potenzialmente infinita di collegamenti decentralizzati tra elaboratori e reti è una struttura "acefala", non governata da nessuno. Si tratta di un fenomeno che, nelle sue applicazioni civili, è sorto spontaneamente per volontà autonoma degli utenti che hanno deciso di collegarsi tra loro e che altrettanto

---

[2] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, 2019, p. XIV ss.

[3] V. ZENO ZENCOVICH, *La libertà di espressione, Media mercato, potere della società dell'informazione*, Bologna, 2004, p. 130.

[4] Terminologia adoperata per la prima volta nel Libro bianco *"Crescita, competitività, occupazione"*, COM (93) 700. Per V. Zeno Zencovich è preferibile l'espressione "società della conoscenza". Cfr. R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. XV.

[5] Così come è stato autorevolmente affermato da J.M. BALKIN, *Old School/New School Speech Regulation*, in *Faculty Scholarship Series*, *paper* n. 4877, 2014, p. 2304.

[6] Corte EDU, *Cengiz c. Turkey*, 1° dicembre 2015, n. 48226/10.

spontaneamente si sviluppa, ricevendo impulso dall'evoluzione continua dei mezzi tecnologici[7].

Si tratta di un'interconnessione globale tra reti di telecomunicazioni e informatiche di natura e di estensione diversa, resa possibile da una serie di protocolli di rete comune, chiamata "TCP/IP" dal nome dei due protocolli principali, il TCP e l'IP, che costituiscono la "lingua" comune con cui i computer connessi a Internet (gli host) sono interconnessi e comunicano indipendentemente dalla loro sottostante architettura hardware e software, garantendo così l'interoperabilità tra sistemi e sottoreti fisiche diverse.

La "acentralità" di Internet pone intuitivamente la questione della riconducibilità a discipline telecomunicative a qualsiasi livello, non essendo univocamente individuabile alcuna infrastruttura né identificabile alcun soggetto ai quali applicare le relative regolamentazioni. Infatti, World Wibe Web[8], è un sistema di immissione e recupero di informazioni che funziona attraverso una struttura ipertestuale multimediale. Nel World Wide Web le risorse disponibili sono organizzate secondo un sistema di librerie, o pagine, a cui si può accedere utilizzando appositi programmi detti *web browser* con cui è possibile navigare visualizzando file, testi, ipertesti, suoni, immagini, animazioni e filmati.

La vera novità di Internet è invece costituita dalla globalizzazione intesa come convergenza tra dematerializzazione o, meglio, digitalizzazione della realtà, cioè tra la trasformazione dei dati, informazioni, opere dell'ingegno etc., in forma di bit, e la comunicazione in tempo reale e a livello planetario del prodotto digitale così ottenuto.

Con la trasformazione in segnali digitali i dati assumono una fisicità diversa da quella reale cui si attagliano male e comunque con difficoltà, le tradizionali categorie giuridiche nate e sviluppatesi nella "realtà fisica".

Con l'avvento dell'era digitale sono cambiate addirittura le nozioni tradizionali di bene e di persona. Il processo di dematerializzazione ha riguardato i beni oggetto della proprietà, il credito, la moneta, i prodotti finanziari in generale.

La dematerializzazione ha avuto come ulteriore importante effetto la delocalizzazione. Il carattere delocalizzato e a-territoriale di Internet ha comportato dal punto di vista giuridico la crisi del principio di territorialità del diritto.

---

[7] G. FACCI, *La responsabilità del provider*, in C. ROSSELLO-G. FINOCCHIARO-G. TOSI (a cura di), *Commercio elettronico. Documento informatico, Firma digitale. La nuova disciplina*, 2003, p. 131 ss.

[8] WWW o semplicemente Web, "ragnatela". Il primo browser con caratteristiche simili a quelle attuali, il *Mosaic*, venne realizzato nel 1993.

L'inesistenza di barriere geografiche nella rete infatti consente di mettere informazioni ed agire nella realtà virtuale indifferentemente da un punto qualsiasi del mondo, rendendo irrilevante l'ubicazione spaziale del server in cui le informazioni sono caricate.
Con semplici clic del mouse si possono attraversare infinite volte le frontiere degli Stati, senza un percorso identificabile a priori.
Con i necessari accorgimenti tecnici è dunque possibile non solo occultare ma anche spostare l'ubicazione fisica del sito, rendendo particolarmente difficoltosa l'individuazione dell'elaboratore attraverso cui è stato commesso l'illecito.
I messaggi vengono suddivisi in pacchetti di informazioni che sono inviati dopo il protocollo che ha provveduto a numerarli e ad identificarli e si mischiano nel tragitto con altri pacchetti di informazioni seguendo un percorso casuale e non prevedibile.
Poiché tra i nodi di trasmissione vi sono più percorsi alternativi, non è detto che i diversi pacchetti dello stesso messaggio restino compatti e seguano lo stesso tragitto. Il messaggio nella trasmissione in rete perde così la sua unità e identità.
Infatti solo al momento del raggiungimento del nodo di destinazione i diversi pacchetti in cui è suddiviso il messaggio saranno riordinati e ricomposti. Il tragitto del messaggio o, meglio, dei suoi frammenti, può subire variazioni anche solo per ragioni contingenti, quali un guasto o il sovraccaricamento di un nodo.
Alla difficoltà di individuazione dell'elaboratore si aggiunge la difficoltà di identificazione dell'utente. Esistono infatti siti anonimi che non sono individuati tramite un normale nome a dominio ma hanno un nome protetto da chiave criptata e cancellano i dati dei loro titolari e ciò talvolta per consentire la manifestazione del pensiero da parte di utenti cittadini di paesi in cui tale libertà è limitata ma, più spesso, per consentire l'esercizio indisturbato di attività illecite[9].
Da tutto ciò consegue che chi intende compiere attività illecite in Internet può non solo scegliere ma anche occultare il luogo di svolgimento di tale attività, evitando l'applicazione di regole di ordinamenti territoriali severi o persino tentando di sottrarsi all'applicazione di qualsivoglia norma territoriale.
Nonostante siano chiare le reali potenzialità positive di tale mezzo comunicativo, inteso quale *marketplace of ideas*, gli spazi digitali sono sempre più pieni di disinformazione,

[9] L. BUGIOLACCHI, *Principi e questioni aperte in materia di responsabilità extracontrattuale dell'Internet provider. Una sintesi di diritto comparato*, in *Dir. inf.*, 2000, p. 836 ss.; F. DI CIOMMO, *La responsabilità civile nell'era di Internet*, in G. PONZANELLI, *La responsabilità civile*, Padova, 2002, p. 179 ss.; A. PIERUCCI, *La responsabilità del provider per i contenuti illeciti della Rete*, in *Riv. crit. dir. privato*, 2003, p. 144 ss.

notizie false, contenuti xenofobi, vendette a sfondo sessuale, diffamazioni, incitamento all'odio e alla violenza.

È ormai risaputo, infatti, che attraverso la rete è possibile moltiplicare a dismisura le possibilità di lesione di posizioni giuridiche altrui come anche gli effetti pregiudizievoli ad esse collegati. Il suo sviluppo ha fatto nascere nuove figure criminose che implicano, come elemento necessario, proprio l'utilizzo del computer e di una connessione alla rete per la loro commissione. Si è anche dovuta affrontare l'evoluzione di atti illeciti "tradizionali", cioè azioni proibite già configurabili e punibili prima dell'avvento del *web*, i quali, per essere efficacemente ostacolati in tale nuovo contesto, devono essere rivisitati ed adattati alle attività telematiche.

A fronte del vertiginoso aumento della possibilità e dell'occasione di commettere illeciti e degli effetti pregiudizievoli che ne discendono, in Internet si riscontra una notevole difficoltà di individuare gli autori degli stessi e di renderli responsabili, imputando loro la condotta dannosa ed i suoi effetti.

Gli illeciti che possono essere commessi sulla rete sono innumerevoli: si persi a titolo esemplificativo alla violazione delle norme sul diritto d'autore, che si realizza quando documenti, immagini ed altre opere protette sono riprodotte e pubblicate sulla rete senza la necessaria autorizzazione da parte dell'autore o del titolare dei diritti su di esse; alla diffamazione, avvenuta mediante l'invio di materiale offensivo su un sito della rete; alla violazione delle norme sul buon costume e contro lo sfruttamento sessuale dei minori, con la pubblicazione di materiale pornografico con minori; alla violazione delle norme sull'ordine pubblico, con la pubblicazione, ad esempio, di materiale di stampo terroristico; alla violazione del diritto alla riservatezza, che si ha quando dati riservati o segreti relativi ad un individuo o ad un'organizzazione vengono resi pubblici su un sito internet; alla concorrenza sleale, nel caso di informazioni false o diffamatorie messe in rete tra imprese concorrenti; alla violazione delle norme sulla protezione dei marchi, ai reati informatici (si pensi alla frode).

In tema di responsabilità civile in rete, seguendo una partizione ormai consolidata, mutuata dalla dottrina penalistica in materia di reati di stampa, è oramai accolta la distinzione tra: illeciti di internet; gli illeciti contro Internet; gli illeciti per mezzo di internet.

A tal proposito, ci si interroga su quale sia il ruolo degli intermediari informatici nella condotta illecita degli utenti[10].

[10] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., pp. XIX e XX.

Le responsabilità dei soggetti che concorrono alla veicolazione dei contenuti riferibili agli internauti sono regolati da plessi normativi che impongono un'indagine comparatistica: accanto ai più importanti e recenti arresti giurisprudenziali delle Corti nazionali e sovranazionali, spesso pietre miliari nella disciplina di tale ipotesi di responsabilità, di particolare rilievo sono gli interventi del legislatore americano con il *Digital Millennium Copyright Act* del 1998 e del legislatore europeo con la direttiva 31/2000, recepita poi nei vari ordinamenti nazionali con appositi testi normativi[11].

Sicuramente si tratta di disposizioni che, risultando oramai datate, mal si attagliano all'attuale contesto di riferimento ma sicuramente rappresentano un tassello importante nella ricostruzione della problematica.

I caratteri della rete, in particolare l'antigerarchicità, hanno addirittura indotto una corrente di pensiero a sostenere, spesso in forma larvata, la teoria secondo la quale Internet sfuggirebbe o dovrebbe sfuggire ad ogni disciplina positiva, orientamenti insostenibili a parere di chi scrive perché una tale interpretazione significherebbe dar vita ad un vero e proprio far west mediatico ed assistere impotenti, e dunque avallare e giustificare, i più terribili misfatti.

In posizione intermedia si collocava un ulteriore teoria secondo la quale la rete dovrebbe essere lasciata all'autoregolamentazione. Fonti di tale autoregolamentazione sono state individuate ora nel complesso delle regole deontologiche degli utenti della rete, ora in una costituita o costituenda lex mercatoria, ora, invece, nei codici di condotta delle categorie di utenti di Internet, strumenti insomma del tutto inadeguati a disciplinare un fenomeno altamente complesso e conflittuale come la rete e gli atti che vi si compiono

La teoria della refrattarietà della realtà virtuale ad ogni forma di disciplina positiva presenta il limite di lasciare prive di regolamentazione normativa fenomeni di notevole rilevanza sociale ed economica.

Tale teoria appare legata ai tempi pionieristici di Internet quando la rete era appannaggio di pochi soggetti ed utilizzata a scopi non imprenditoriali e, quindi, i conflitti di interesse erano rari e modesti.

Il diritto della rete non può essere la legge di una categoria particolare, ma deve essere la legge di tutti gli utenti di Internet e, in primis, dei cittadini e dei consumatori, ossia di soggetti titolari di diritti, e, in quanto portatori di interessi meritevoli di tutela spesso contrapposti a quelli degli imprenditori, bisognosi di norme di protezione.

[11] Per la trattazione approfondita del regime di responsabilità, della normativa e della giurisprudenza di riferimento, si rimanda ai capitoli successivi.

La *vexata quaestio* di configurare una responsabilità in capo all'Internet provider è amplificata dal fatto che non sempre è possibile identificare l'autore materiare dell'illecito; infatti, anche se ogni utente accede alla rete mediante un codice di accesso, ciò non garantisce di poter individuare con sicurezza l'identità del soggetto che ha commesso l'illecito.

Tecnicamente è sempre possibile identificare il nome d'accesso dell'utente che ha commesso la violazione attraverso quello che viene chiamato il *log file* contenente il nome dei login e dei tempi di accesso di ogni utente.

Tuttavia nulla vieta che tale nome possa essere stato in precedenza sottratto, insieme alla sua password, ed utilizzato fraudolentemente da terzi al fine di evitare ogni possibile conseguenza.

La stessa difficoltà di individuazione si ha quando uno stesso nome di accesso alla rete è utilizzato da più persone contemporaneamente.

In più non va dimenticato che esistono siti che consentono ai navigatori di restare anonimi.

Proprio da questa oggettiva difficoltà di individuare l'effettivo autore dell'illecito, nasce la tendenza ad allargare la sfera di responsabilità oltre la persona dell'autore.

Può accadere, altresì, che anche se si individua il responsabile, questo sia inutile, nel caso in cui l'autore dell'illecito si trovi in uno Stato, la cui normativa applicabile non permette di perseguire il responsabile.

L'Internet provider, invece, è un soggetto sempre identificabile[12].

L'affermazione di responsabilità in capo al provider, inoltre, non solo comporta indubbi vantaggi sul versante della semplificazione probatoria ma può fornire anche al danneggiato maggiori garanzie dal punto di vista economico.

Dunque, anche nel caso in cui gli autori degli illeciti in rete vengano individuati, è spesso difficile per i danneggiati ritenerli responsabili poiché si tratta di frequente di soggetti, quali piccole imprese o persone fisiche non ancora in età lavorativa, che, pur avendo cagionato grazie alla potenzialità offensive della rete danni notevoli, non sono in grado di ristorarli.

In questo contesto è naturale che le pretese risarcitorie dei danneggiati si indirizzino prima di tutto verso gli Internet provider e, più specificatamente, verso gli host provider che hanno fornito ai propri users il mezzo e lo spazio virtuale con cui è stato commesso l'illecito.

Il provider, infatti, a differenza degli users è soggetto facilmente individuabile e spesso patrimonialmente capiente.

---

[12] G.M. RICCIO, *Anonimato e responsabilità in Internet*, in *Dir. inf.*, 2000, p. 20 ss.

Il tema della responsabilità del provider dunque non riguarda tanto i casi in cui la condotta antigiuridica sia imputabile direttamente all'intermediario, quanto piuttosto i casi in cui il servizio offerto in rete sia stato il mezzo per la commissione dell'illecito da parte degli utilizzatori.

Il punto centrale della questione perciò non è rappresentato dalla responsabilità del provider per il fatto proprio ma per il fatto altrui o per omessa vigilanza sulla condotta degli utenti.

La necessità di reprimere gli illeciti telematici comporta, perciò, l'esigenza di dirimere certe delicate questioni direttamente collegate allo sviluppo della rete stessa.

Tuttavia, se per un verso è necessario tutelare in modo adeguato ed effettivo i soggetti che subiscono lesioni di propri diritti, per un altro non bisogna penalizzare eccessivamente il web nella sua interezza.

Per tale ragione, le possibili soluzioni da adottare in materia rischiano di comportare importanti ricadute circa le possibilità di sviluppo del commercio elettronico, nonché limitare la libertà di espressione del pensiero in rete.

Internet difatti non è solo uno strumento di scambio di beni aventi rilevanza economica ma anche un cosiddetto "*marketplace of ideas*", cioè un luogo dove gli utenti possono esercitare i propri diritti fondamentali, come manifestare il proprio pensiero o presentare le proprie idee. Internet non deve, quindi, solo essere considerato come una minaccia o un nuovo strumento con scopo commerciale ma deve, altresì, necessariamente intendersi anche come un eccezionale mezzo di comunicazione e di diffusione della cultura, nonché un luogo nel quale si crea e si sviluppa la personalità umana.

Il tema principale per gli operatori in questo settore, quindi, non riguarda solo il raggiungimento di un punto di equilibrio ottimale nel bilanciamento di interessi contrastanti ovvero, da un lato lo sviluppo di Internet e dall'altro la protezione di soggetti che possono subire fatti illeciti, ma necessariamente anche l'armonizzazione delle normative attuabili in tale contesto, sempre tenendo conto del rispetto dei diritti individuali fondamentali.

Le attività poste in essere su Internet, così come precisato dalla Corte EDU, "costituiscono un mezzo straordinario e senza precedenti per l'esercizio della libertà di espressione" ma rappresentano anche "uno strumento per amplificare rischi" e generare contenuti illeciti "che possono diffondersi come mai prima d'ora in tutto il mondo, in pochi secondi e talvolta rimangono permanentemente accessibili on line"[13].

[13] Corte EDU, Grande Camera, 16 giugno 2015, *Delfi v. Estonia*, n. 64569/09, par. 157.

Ecco perché il tema della responsabilità del provider non riguarda tanto i casi in cui la condotta antigiuridica sia imputabile direttamente all'intermediario, quanto piuttosto i casi in cui il servizio offerto in Rete sia stato il mezzo per la commissione dell'illecito da parte degli utilizzatori. Il punto centrale della questione è rappresentato dalla responsabilità del provider per il fatto altrui o per omessa vigilanza sulla condotta degli utenti non per il fatto proprio.

Per poter ben comprendere i regimi di responsabilità degli intermediari, i criteri di imputazione e gli sviluppi in materia, è necessario capire cosa intende per Internet Service Provider e quali attività lo stesso può svolgere perché chiaramente i regimi cambiano a seconda delle condotte poste in essere concretamente dall'intermediario informatico.

2. ISP e le diverse attività svolte in rete

Con il termine *Internet provider* si suole far riferimento ad una vasta ed eterogenea categoria di intermediari telematici che la direttiva 2000/31/CE, fonte che disciplina a livello comunitario la responsabilità dell'*ISP*, definisce come "prestatori di servizi della società dell'informazione".

Si intendono tali tutti quei soggetti, connessi ad Internet e generalmente costituiti giuridicamente come impresa, che svolgono nelle reti telematiche un'attività di intermediazione[14], diretta a consentire l'accesso a Internet, la fornitura dei relativi servizi agli utenti, la diffusione di informazioni telematiche, l'immagazzinamento dei dati, servizi di connessione e trasmissione, spesso consistenti nell'ospitare un sito sulle proprie apparecchiature.

La rilevanza del *provider* è assolutamente centrale: è l'interfaccia tra gli internauti ed i gestori delle linee telefoniche e di comunicazione[15].

[14] G.M. RICCIO, *La responsabilità civile degli Internet providers*, cit., p. 23 ss.; R. BOCCHINI, *La responsabilità extracontrattuale del provider*, in D. VALENTINO (a cura di), *Manuale di diritto dell'informatica*, Napoli, 2016, p. 539; G.M. RICCIO, *La responsabilità degli internet providers nel d. legisl. n. 70 del 2003*, in *Danno e resp.*, 2003, p. 1157; L. BUGIOLACCHI, *La responsabilità dell'host provider alla luce del d. legisl. n. 70 del 2003: esegesi di una disciplina "dimezzata"*, in *Resp. civ. prev.*, 2005, p. 188; V. ZENO ZENCOVICH, *Note critiche sulla nuova disciplina del commercio elettronico dettata dal d. legisl. n. 70 del 2003*, in *Dir. inf.*, 2003, p. 505; G. CASSANO-I.P. CIMINO, *Il nuovo regime di responsabilità dei providers: verso la creazione di un novello "censore telematico"*, in *Contratti*, 2004, p. 88.

[15] M. DE CATA, *La responsabilità civile dell'Internet service provider*, cit., p. 66 ss.

Il *provider* si pone dunque come confluenza di due relazioni di natura privatistica di cui egli è al contempo parte, da un lato con l'operatore e dall'altro con l'utente, rapporto quest'ultimo qualificato come un appalto di servizi[16].

La prima definizione di intermediario informatico a livello istituzionale è stata adottata dall'OCSE (Organizzazione per la Cooperazione e lo sviluppo economico) e risale al 2010: si tratta di "soggetti che sfruttano la loro posizione di intermediari per favorire la comunicazione con gli altri attori presenti sul mercato al fine di concludere transazione e, quindi, creare valore economico e sociale"[17].

In altri termini questi prestatori provvedono a "offrire l'infrastruttura; raccogliere, organizzare e valutare informazioni che sono presenti on line in maniera non correlata; facilitare la comunicazione e lo scambio di informazioni; aggregare domanda ed offerta; facilitare i processi di mercato; fornire la legittimazione ovvero favorire la creazione di un clima di fiducia in rete; contemperare gli interessi dei compratori/utenti con quelli dei venditori/inserzionisti"[18].

Emerge in maniera immediatamente evidente la complessa articolazione delle funzioni di intermediazione assunte dai provider, al punto tale che lo stesso rapporto dell'OCSE enuclea una serie di operatori che costituirebbero delle sottocategorie del più ampio concetto di intermediario on line.

La Commissione Europea ha definito per la prima volta gli intermediari della rete come "guardiani di contenuti" [19] delle reti digitali, identificandoli come quei soggetti che gestiscono gli strumenti tecnologici, garanti non solo dell'accesso e della diffusione delle informazioni ma anche del controllo del flusso dei contenuti che circolano in rete, occupandosi della rimozione, selezione ed organizzazione dei caricamenti[20].

Questo chiaramente non significa che il provider possa prestare attenzione a tutto il materiale che viene caricato sui portali telematici, un "oceano di informazioni e di fonti di

[16] Il rapporto tra provider e utente è qualificato dalla dottrina maggioritaria come appalto di servizi. Il rapporto tra provider e network è configurato come contratto di locazione; R. BOCCHINI, *Il contratto di accesso ad Internet*, 2004, *passim.*

[17] OECD, *The Economic and Social Role of Internet Intermediaries*, 2010, 15.

[18] *Ibidem*. Cfr. M.L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, 2018, pp. 14 e 15.

[19] Comunicazione della Commissione al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo e al Comitato delle Regioni - *Lotta ai contenuti illeciti on line-Verso una maggiore responsabilizzazione delle piattaforme on line*, 28 settembre 2017, COM (2017) 555, spec. 21.

[20] J.M. BALKIN, *Free Speech in a Triangle*, 2018, p. 2011 ss. Cfr., R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. XVIII.

produzione"[21], ma senza dubbio gli algoritmi delle piattaforme possono e, a parere di chi scrive, devono svolgere un'attività di filtro per quanto lo stato della scienza consente.

Il provider è il soggetto che organizza l'offerta ai propri utenti dell'accesso alla rete Internet e dei servizi connessi all'utilizzo di essa.

Data la varietà dei servizi offerti agli utenti, diventa particolarmente rilevante la distinzione sotto il profilo oggettivo e funzionale delle attività del *provider*, distinzione che viene ad essere fondamentale ai fini del corretto inquadramento delle responsabilità degli intermediari di servizi in Internet.

La vastità ed eterogeneità delle attività si riflette anche sulla diversa misura di partecipazione del *provider* alla commissione eventuale di illeciti da parte di terzi, sul grado di diligenza esigibile e sul regime stesso di responsabilità che deve essere necessariamente differenziata[22].

Il riferimento normativo per la qualificazione giuridica delle posizioni dei vari *Internet Service Provider* è oggi rappresentato dalla Direttiva 2000/31/CE sul commercio elettronico, negli articoli 12-14 e dalla legge statale di recepimento d.lgs. n. 70 del 2003, artt. 14,15,16.

Nel disciplinare la responsabilità degli operatori in rete, la suddetta normativa muove, più che dalla distinzione dei vari tipi di intermediari di Internet, dall'individuazione delle attività dagli stessi effettivamente svolte: semplice trasporto (*mere conduit*), memorizzazione temporanea (*caching*), memorizzazione di informazioni (*hosting*)[23].

2.1 Mere conduit

L'art. 12 della direttiva europea disciplina l'ipotesi del semplice e mero trasporto di informazioni: l'attività di *mere conduit* consiste nel fornire l'accesso alla rete di comunicazione e nel trasmettere sulla stessa le informazioni fornite da un destinatario del servizio[24]. Si pensi, a titolo esemplificativo, ai servizi offerti dalle compagnie telefoniche per la connessione alla rete e la ricezione di dati.

Nelle attività di trasmissione e di fornitura di accesso vanno incluse anche 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.

---

[21] G. PITRUZZELLA, *La libertà di informazione nell'era di Internet*, in *Media Laws, Rivista di diritto dei media*, 2018, p. 12.

[22] A. PIERUCCI, *La responsabilità del provider per i contenuti illeciti della Rete*, 2003, p. 12 ss.

[23] M. GAMBINI, *Le responsabilità civile dell'Internet service provider*, 2006, pp. 13 e 14.

[24] M.L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, cit., pp. 88 e 89.

Per ragioni di natura tecnica, infatti, il caricamento e la memorizzazione dei contenuti sono propedeutiche all'elaborazione e al trasferimento delle informazioni del destinatario del servizio.

Per tale genere di operatori, la normativa prevede l'assenza di un obbligo di verifica del contenuto delle informazioni che vengono trasmesse e subordina la responsabilità alla sussistenza di diverse condizioni, quali l'aver originato la trasmissione, l'aver selezionato il destinatario della trasmissione oppure l'aver selezionato o modificato le informazioni trasmesse[25].

L'art. 14 del d.lgs. 70/2003 disciplina tale attività di intermediazione in termini di sostanziale e formale identità con la direttiva 31/2000.

È dunque previsto, così come sostenuto da autorevole dottrina[26], un regime di *favor legis*, di cui questa attività gode, sebbene tali condizioni di esonero da responsabilità cessino di esistere nel momento in cui il provider partecipi in modo attivo al procedimento di trasmissione, stabilendo un rapporto qualificato con le informazioni che diffonde, sia dal punto di vista contenutistico che di selezione dei destinatari[27].

Tale scelta, sia a livello europeo che nazionale, è frutto della considerazione che tale tipologia di intermediario, che svolge quindi un ruolo assimilabile a quello svolto dagli operatori dei servizi di telecomunicazione nella diffusione delle conversazioni telefoniche, non possa avere alcun controllo su una eventuale comunicazione digitale lesiva dei diritti di terzi e non possa, dunque, essere ritenuto responsabile dei contenuti di tale comunicazione.

Questa conclusione riprende il dictum di una pronuncia della Corte Suprema statunitense del 2000[28]. Nella risoluzione del caso di specie, relativo ad un' ipotesi di diffamazione a mezzo Internet, il collegio ha confermato la sentenza della Corte d'appello dello stato di New York, secondo la quale il provider (*Prodigy*) era stato il semplice veicolo attraverso cui è transitato il messaggio offensivo, sicché avendo un ruolo passivo, vale a dire non avendo avuto alcun ruolo di compartecipe nella commissione dell'illecito, al pari di una compagnia telefonica, non è stata riconosciuta la sua responsabilità in ordine ai contenuti della comunicazione digitale offensiva.

---

[25] E. BASSOLI, *Giurisprudenza italiana e comunitaria sulla responsabilità civile del service provider e la sentenza della Corte di Appello di Milano nel caso Yahoo vs. RTI*, in *Contratto e impresa*, 2015, pp. 231 e 232.
[26] G.M. RICCIO, *La responsabilità civile degli Internet providers*, cit., p. 202.
[27] M.L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, cit., p. 88.
[28] Sul punto v. l'url: *http://www.tin.it/ notiziapiu/new//170798_provider_soc.html*. Cfr., altresì, E. BASSOLI, *Giurisprudenza italiana e comunitaria sulla responsabilità civile del service provider e la sentenza della Corte di Appello di Milano nel caso Yahoo vs. RTI*, cit., p. 233.

Rientrano, dunque, nell'art. 14 della direttiva i *network layer* e i *physical layer* provider, come soggetti che operano a livello in infrastruttura della rete, i fornitori di connettività, i *network blackbone* provider, come gestori delle dorsali informatiche e gli operatori di telefonia mobile.

Qualche difficoltà interpretativa è sorta nell'ipotesi in cui l'operatore filtri i dati trasmessi, impedendo che essi vengano recapitati al destinatario originario, al fine di reindirizzarli ad un *blackhole*, che è uno spazio della rete in cui il traffico dei dati è dirottato mediante un sistema di blocco che si caratterizza per l'avvalersi di una lista di indirizzi e per il fatto che i pacchetti di informazioni da questi provenienti vengano automaticamente rifiutati.

Ci cerca solitamente di contrastare con tali modalità il fenomeno dello spam.

Il dubbio si pone perché se da un lato si potrebbe sostenere che per i dati filtrati non si registra alcuna alterazione di contenuto, dall'altro resta valida anche la contestazione che l'operatore così facendo verrebbe meno all'obbligo di non selezionare il destinatario della trasmissione e di non modificare le informazioni trasmesse[29].

Tuttavia, al netto di questa unica ipotesi dubbia, il provider *mere conduit* non pone particolari problemi all'attenzione dell'operatore di diritto, data l'esenzione di responsabilità che effettivamente trova una sua ratio nella effettiva incidenza effimera della sua attività di intermediazione informatica.

L'immunità del prestatore facilmente si giustifica alla luce del mancato contatto qualificato con i dati veicolati, fermo restando che non è esclusa la possibilità per gli stati membri di imporre precisi obblighi di cooperazione attiva e tempestiva con le autorità amministrative e giudiziarie che abbiano individuato un illecito, specie al fine di evitare che venga reiterato il crimine informatico, facendo ricorso a strumenti tecnologici a sua disposizione, come la disabilitazione all'accesso web.

2.2 Caching

L'attività di caching consiste nella memorizzazione temporanea dei dati, non al fine di trasmetterli ma per massimizzare l'efficacia del successivo inoltro ad altri utenti su loro richiesta.

A differenza dell'ipotesi di *mere conduit*, il caching non è un'attività transitoria ma è effettuata allo scopo di creare i cosiddetti "*cache*", ossia delle copie temporanee di risorse

[29] M.L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, cit., p. 90 ss.

on line e di pagine ipertestuali o all'interno di siti web (il c.d. *mirroring*) cui l'utente intende accedere.

In tal modo si rendono più efficienti e meno dispendiosi in termini di tempo e connessione gli accessi successivi e si elimina la necessità di connettersi ogni volta ai server contenenti le pagine originali[30].

L'art. 13 della direttiva eurocomunitaria, relativo all'attività di caching, ha escluso la responsabilità del caching provider in ordine alla memorizzazione automatica e temporanea di informazioni.

L'esclusione della responsabilità di tale genere di operatore è stata comunque condizionata al rispetto di cautele ed obblighi da parte del provider che non dovrà modificare le informazioni veicolate, dovrà rimuovere prontamente le informazioni una volta che sia stato messo al corrente della loro illiceità, dovrà disabilitare l'accesso o rimuovere le informazioni su ordine

dell'autorità amministrativa o giudiziaria[31].

Non è difatti escluso che l'intermediario, sebbene esente da responsabilità, sia comunque destinatario di un decreto ingiuntivo che gli imponga un intervento diretto ad impedire o comunque a porre fine alla perpetrazione delle attività illecite on line.

A contrario, la memorizzazione può avvenire legittimamente solo se come parte di un processo meramente tecnico si attiva automaticamente, se l'origine e la destinazione dell'informazione provengano da soggetti diversi dal prestatore, senza che questi eserciti alcuna attività di controllo o forma di direzione ma si configura solo come "anello in una catena di trasmissioni successive"[32], ferma restando la possibilità per l'intermediario di compiere quelle operazioni necessarie per ragioni eminentemente tecniche.

Si pensi al servizio di ricerca predisposto dai motori di ricerca, consistente nel cercare e organizzare in un elenco i siti pertinenti ai criteri di ricerca indicati dall'utente interrogante, fornendo i link che consentono la connessione con ciascuno di essi.

Per svolgere tale attività il motore di ricerca procede ad eseguire una copia di ogni sito che viene memorizzata temporaneamente in una *cache*, così da fornire, per le chiavi di ricerca più frequentemente utilizzate, i risultati della ricerca stessa in tempi estremamente rapidi.

---

[30] Esistono dei meccanismi standard utilizzati per evitare che certe informazioni siano oggetto di copia. Si pensi al meccanismo di protocollo di esclusione "robot", utilizzato dai gestori di pagine web per comunicare ai software automatici per le attività dei motori di ricerca *(*i *crawlers*) restrizioni alle creazioni di estratti della pagina. Cfr. M.L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, cit., p. 93.

[31] E. BASSOLI, *Giurisprudenza italiana e comunitaria sulla responsabilità civile del service provider e la sentenza della Corte di Appello di Milano nel caso Yahoo vs. RTI*, cit., pp. 233 e 234.

[32] M.L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, cit., p. 9.

Si realizza, pertanto, una "memorizzazione automatica, intermedia e temporanea" delle informazioni senza che il prestatore del servizio le modifichi.

Quest'ultimo mantiene una situazione di neutralità non solo relativamente all'attività di *linking* (semplice offerta di collegamenti ipertestuali), ma anche a quelle di *embedding* (strumento che consente all'utente di visionare direttamente sul motore di ricerca immagini presenti su siti di terzi) e di *suggest search* (strumento che offre suggerimenti per completare automaticamente le chiavi della ricerca sulla base delle combinazioni più utilizzate dagli utenti)[33].

Si può pertanto ritenere, alla luce di quanto analizzato circa le attività di *mere conduit* e di *caching*, che il punto di discrimine fra fornitore neutrale e non neutrale debba essere individuato nella manipolazione o trasformazione delle informazioni o dei contenuti trasmessi o memorizzati, come peraltro suggerito dal considerando n. 43 della Dir. n. 2000/31/CE.

Tale criterio, sebbene espresso in riferimento alle attività di *mere conduit* e *caching*, si può ritenere estensibile, per analogia, anche al caso dell'*hosting* provider.

2.3 Hosting (attivo e passivo)

L'attività di *hosting* implica, a differenza delle altre, una memorizzazione permanente per conto dell'utente e per sua espressa richiesta.

Trattandosi di un esercizio di immagazzinamento di dati né transitorio né temporaneo (come rispettivamente nel caso del *mere conduit* e del *caching*), l'attenzione del giurista si è maggiormente concentrata su tale tipologia di provider e sulla sua relativa responsabilità.

L' attività di memorizzazione duratura delle informazioni è tipica dei prestatori di servizi delle società dell'informazione ed è essenziale per il funzionamento e l'esistenza del web. Quest'ultimo è caratterizzato da un insieme amplissimo di contenuti multimediali e di servizi accessibili a tutti o ad una parte selezionata di utenti Internet e costituisce la più grande possibilità offerta a privati, aziende ed enti pubblici di ottenere visibilità in ogni parte del mondo.

Detti contenuti sono organizzati in pagine web realizzate con appositi linguaggi di programmazione (html, dhtml, java, php ecc.). L'insieme di più pagine web, correlate tra loro tramite link, compone un sito web.

[33] V. Trib. Milano, 25 marzo 2013, in *Danno e resp*., 2013, p. 908, con nota di P. CARBONE e F. ZANOVELLO, *La responsabilità dell'Internet Service Provider. Brevi note a Cass. 19 marzo 2019, nn. 7708 e 7709*, in *Studium Iuris*, 2020, pp. 563 e 564.

Tutti coloro che dispongono di uno spazio di memoria su di un computer *host* collegato alla rete possono, quindi, pubblicare i propri contenuti raccolti in pagine web con l'evidente possibilità di diventare "editore" e raggiungere un pubblico vastissimo con esiguo impegno economico.

L'*hosting* provider è il fornitore di servizi che si limita a mettere a disposizione di un utilizzatore, in maniera duratura, una parte di hard disk del proprio server, di cui però resta proprietario, al fine di consentire la pubblicazione e l'*upload* di pagine web e contenuti multimediali[34].

La memorizzazione duratura determina un rischio decisamente più elevato, proprio in ragione della permanenza dei dati in Internet e della conseguente possibilità di perpetrazione degli illeciti.

Il provider mette a disposizione dell'utente uno "spazio" telematico, incidendo nella catena causale che dalle informazioni dell'utente conduce alla commissione dell'illecito[35].

Pertanto, risulta evidente che un'eventuale esenzione di responsabilità del prestatore informatico deve necessariamente richiedere dei requisiti e delle condizioni più stringenti, nonché un grado di diligenza decisamente più elevato.

Il prestatore instaura una relazione stabile con le informazioni ed è dunque chiamato ad assumere una posizione di garanzia volta ad impedire o a porre fine alla commissione degli illeciti da parte degli utenti[36].

Il legislatore eurocomunitario è stato piuttosto generico nella formulazione delle regole in materia di responsabilità dell'*hosting* provider, specie nell'indicare le condizioni che delimitano l'attività tipica del prestatore, dando rilievo a profili soggettivi come la conoscenza e la conoscibilità.

Più nel dettaglio, è l'art. 14 della direttiva comunitaria 31/2000, quello che qui maggiormente rileva, recepito dal legislatore italiano con l'art. 16 d.lgs. 70/2003, a dettare per gli Stati membri la disciplina in materia di responsabilità del fornitore del servizio di hosting.

---

[34] N. DE LUCA- E. TUCCI, *Il caso Google/Vivi Down e la responsabilità dell'Internet Service Provider. Una materia che esige chiarezza*, in *Giur. comm*., 2011, p. 1215. Vedi anche Trib. di Torino, 7 aprile 2017, n. 1928, il commento di V. VOZZA, *La responsabilità civile degli Internet Service Provider tra interpretazione giurisprudenziale e dettato normativo*, in *Danno e resp*., 2018, p. 95 ss.

[35] Sul punto, M.L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, cit., p. 94 e L. BUGIOLACCHI, *Evoluzione dei servizi di hosting provider, conseguenze sul regime di responsabilità e limiti all'attuale approccio case by case*, in *Resp. civile e previdenza*, 2013, p. 1997 ss.

[36] M.L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, cit., pp. 94 e 95.

Il dato normativo stabilisce che tale operatore, come si dirà ancor più diffusamente in seguito, non sarà responsabile per le informazioni memorizzate a richiesta di un destinatario del servizio a condizione che: a) svolga un'attività di ordine meramente tecnico, automatico e passivo e sia quindi neutrale rispetto ai contenuti memorizzati; b) 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 dell'informazione, o, non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

È tuttavia fatta salva la possibilità, per un organo giurisdizionale o un'autorità amministrativa, in conformità con gli ordinamenti giuridici degli Stati membri, di esigere che il prestatore ponga fine ad una violazione o la impedisca nonché l'opportunità, per gli Stati membri, di definire procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime.

È il considerando 42 della direttiva CE 2000/31 a chiarire che le deroghe previste dalla norma comunitaria "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".

Tale disposizione sembrerebbe quindi confermare che le limitazioni di responsabilità previste dalla normativa di settore non possono essere applicate a quei provider che offrono dei servizi che comportano la modifica ed il trattamento dei dati memorizzati.

La Corte di Giustizia ha infatti operato un'interpretazione evolutiva introducendo un filtro preventivo di valutazione legato allo svolgimento dell'attività concretamente posta in essere dal prestatore informatico[37].

Risulta chiaro, ma sul punto si approfondirà in seguito, che il legislatore europeo e quello nazionale hanno voluto dettare un regime di *favor* per incentivare l'attività degli Internet

[37] CdG, 23 marzo 2010, *Google c. Louis Vuitton*, C-236/08 e CdG, *Google France SARL c. CNRRH*, C-238/08, in *De Jure.*

provider, prevendendo l'assenza di un obbligo generale di sorveglianza[38] e delle condizioni di esonero di responsabilità.

In tutte le ipotesi non previste dai dettati normativi summentovati, si applicano le regole generali in materia di responsabilità civile (artt. 2043 e 2055 c.c.)[39].

Sebbene emerga questa sola figura nel dettato legislativo della direttiva, la giurisprudenza prima della Corte di Giustizia dell'UE e poi delle Corti italiane ha attuato quel fenomeno di "responsabilizzazione" del provider, che ha trovato il suo apice nella creazione giurisprudenziale della figura dell'*hosting* provider attivo.

Come meglio si analizzerà, la sentenza L'*Oréal c. eBay* e l'arresto giurisprudenziale della Suprema Corte italiana, n. 7708/2019, rappresentano delle vere pietre miliari nel sistema della responsabilità dell'Internet Service Provider in evoluzione applicativa alla normativa più datata.

L'*hosting* provider attivo è 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, (questi ultimi intermediari non conoscono né controllano le informazioni trasmesse o memorizzate dalle persone alle quali forniscono i loro servizi) e pone, invece, in essere una condotta attiva, concorrendo con altri nella commissione dell'illecito.

In tale ipotesi l'intermediario attivo resta sottratto al regime generale di esenzione di cui all'art. 16, d.lgs. n. 70 del 2003, dovendo la sua responsabilità civile atteggiarsi secondo le regole comuni.

Così come precisato dal considerando 42 della direttiva, infatti, le limitazioni di responsabilità ed il regime privilegiato descritto non sono applicabili nel caso in cui il prestatore di servizi svolga un ruolo attivo.

Gli elementi idonei a delineare la figura e gli "indici di interferenza" da accertare in concreto ad opera del giudice del merito, mediante l'ausilio di un CTU, sono - a titolo esemplificativo e non necessariamente tutti compresenti - le attività di filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione o

[38] L'art. 15 della direttiva comunitaria, facendo riferimento a tutte e tre le tipologie di Internet Service Provider stabilisce l'assenza dell'obbligo generale di sorveglianza: "1. 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. 2. 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".

[39] A. DI MAJO, *La responsabilità del provider tra prevenzione e rimozione*, in *Corriere giur.*, 2012, p. 553.

promozione dei contenuti, operate mediante una gestione imprenditoriale del servizio, come pure l'adozione di una tecnica di valutazione comportamentale degli utenti per aumentarne la fidelizzazione.

Si tratta di condotte che hanno, in sostanza, l'effetto di completare ed arricchire in modo non passivo la fruizione dei contenuti da parte di utenti indeterminati[40].

È condivisibile in tale ipotesi configurare una responsabilità in capo al provider, sottraendolo ad una "irresponsabilità" e a dei benefici ingiustificati, lesivi oltremodo per l'utente danneggiato.

Anche l'inserzione pubblicitaria, spesso utilizzata dai prestatori informatici per fini di guadagno, può essere considerata un indice della condotta attiva del provider. E' quanto ha confermato anche il Tribunale di Roma nel caso Reti Televisive Italiane s.p.a. c. VIMEO LLC[41].

Nel caso di specie il ctu ha accertato che ad alcuni video non erano stati associati annunci pubblicitari veri e propri ("*display advertisement*") sotto forma di banner pubblicitari direttamente visibili sulle pagine. Vimeo ha comunque associato agli stessi contenuti collegamenti pubblicitari ("*sponsored links*") a pagine web di terzi, generati automaticamente da algoritmi di Google mediante il servizio chiamato AdSense.

Di norma, tali link risultano "contestualizzati", in quanto il contenuto della pubblicità è correlato attraverso alcuni elementi (p.es. attraverso certe parole chiave) al contenuto della pagina visualizzata.

Con specifico riferimento al modello di business adottato da Vimeo, il CTU ha evidenziato che i canali attraverso i quali Vimeo incamera gli utili sono: (i) gli introiti derivanti dalle iscrizioni e dalle transazioni associate alla commercializzazione dei video, (ii) le inserzioni pubblicitarie.[42]

Sicché, in considerazione dell'"effetto rete", i video in oggetto, considerata la loro popolarità, potrebbero aver aumentato gli utenti della piattaforma Vimeo, attirandone di nuovi, quantomeno nella sezione italiana del sito, e quindi potrebbero aver creato valore per la società e per gli utenti paganti.

Tenuto conto delle pluriarticolate attività svolte dal provider nella gestione dei contenuti audiovisivi immessi sulla propria piattaforma digitale, si è affermato che Vimeo non si è

[40] Cass. civ., 19 marzo 2019, n. 7708, in *Giur. it.*, p. 2604. Cfr. R. BOCCHINI, *La responsabilità civile plurisoggettiva, successiva ed eventuale dell'ISP*, in *Giur. it.*, 2019, p. 2609 ss.

[41] Trib. di Roma, Sez. XVII, Sez. Specializzata in materia di impresa, 10 gennaio 2019, n. 693, in *De Jure*.

[42] S. SICA, *Responsabilità del provider: per una soluzione "equilibrata" del problema*, in *Corriere giur.*, 2013, p. 506 ss.

limitata ad attivare il processo tecnico che consente l'accesso alla piattaforma di comunicazione sulla quale sono trasmesse o temporaneamente memorizzate le informazioni messe a disposizione da terzi, al solo fine di rendere più efficiente la trasmissione, ma ha svolto una complessa e sofisticata organizzazione di sfruttamento dei contenuti immessi in rete che vengono selezionati, indirizzati, correlati, associati ad altri, arrivando a fornire all'utente un prodotto audiovisivo di alta qualità e complessità dotato di una sua precisa e specifica autonomia.

Un sistema tecnologico così avanzato e sofisticato è del tutto incompatibile con la figura dell'hosting provider "passivo".

Per le ragioni innanzi indicate, l'attività svolta dalla convenuta Vimeo non può essere ricondotta nell'ambito del mero *hosting* provider "passivo", ma piuttosto nell'ambito di attività che la giurisprudenza definisce di *hosting* provider "attivo".

Questo ci dà un quadro più pratico di cosa si intenda con tale tipologia di prestatore informatico.

Nella Comunicazione della Commissione COM (2017) 555 del 28 settembre 2017 viene in rilievo come le piattaforme online, ad oggi, "dispongono solitamente dei mezzi tecnici per identificare e rimuovere" i contenuti illeciti e che, alla luce del "progresso tecnologico nell'elaborazione di informazioni e nell'intelligenza artificiale, l'uso di tecnologie di individuazione e filtraggio automatico sta diventando uno strumento ancora più importante nella lotta contro i contenuti illegali online".

Attualmente molte grandi piattaforme utilizzano forme di algoritmo di abbinamento basate su una serie di tecnologie, dal semplice filtraggio dei metadati fino all'indirizzamento calcolato e alla marcatura (*fingerprinting*) dei contenuti[43].

Volendo riportare una testimonianza di quanto sostenuto, nel settore del diritto d'autore - a titolo esemplificativo - il riconoscimento automatico dei contenuti si dimostra uno strumento efficace da diversi anni, addirittura in funzione "proattiva", giustamente escludendo però che questo possa di per sé implicare, *ex adverso*, la perdita della deroga alla responsabilità.

Inoltre gli strumenti tecnologici possono essere usati con un maggiore livello di affidabilità per marcare e filtrare i contenuti che sono già stati identificati e valutati come illegali, mediante riconoscimento automatico degli stessi e procedure automatiche di rimozione permanente, volte a prevenire la ricomparsa di contenuti illegali online.

[43] R. BOCCHINI, *La responsabilità civile plurisoggettiva, successiva ed eventuale dell'ISP*, cit., p. 2617 ss.

Il punto di discrimen tra fornitore neutrale e non neutrale deve essere individuato nella manipolazione o trasformazione delle informazioni o dei contenuti trasmessi o memorizzati, come peraltro suggerito dal considerando n. 43 della Dir. n. 2000/31/CE[44].

Affinché l'attività del prestatore di servizi perda il suo carattere di neutralità, e, con esso, l'esenzione di responsabilità, non è necessaria una conoscenza personale e diretta del contenuto illecito ma è sufficiente che i mezzi tecnologici dallo stesso utilizzati siano comunque idonei a conferirgli la conoscenza o il controllo dei dati memorizzati.

Pertanto anche se il prestatore di servizi si avvale di un software per indicizzare, organizzare, catalogare, associare ad altri o alla pubblicità i video caricati dagli utenti, viene comunque a svolgere un ruolo attivo di ingerenza nei contenuti memorizzati, tale da permettergli di conoscere o controllare e di fornire un importante contributo all'*editing* del materiale memorizzato.

L'*hosting* provider attivo è apparso come una "figura atipica di creazione giurisprudenziale"[45], una sorta di *tertium genus* tra l'intermediario passivo e il fornitore di contenuti che svolge funzioni editoriali[46].

Chiaramente non è possibile ricondurre a priori un intermediario ad una categoria piuttosto che ad un'altra ma è necessario svolgere un'attenta e prudente valutazione del caso concreto: in linea con quanto ricordato anche dalla Corte di Giustizia, sarà il giudice di merito a svolgere l'arduo compito di valutare il grado di interferenza dell'attività del provider, tenendo conto dell'organizzazione e della selezione dei contenuti forniti dagli utenti, dell'esistenza di eventuali strumenti di ricerca che permettano agli *users* di reperire i contenuti desiderati mediante parole chiave, del meccanismo di suggerimento, dell' esistenza di spiegazioni sul funzionamento della piattaforma e del linking, dell'eventuale presenza di clausole contrattuali da cui si deduce un controllo sui contenuti degli utenti e degli eventuali profitti economici in ragione dello sfruttamento pubblicitario, profitti decisamente superiori rispetto a quelli del mero servizio di hosting[47].

Alla luce di quanto analizzato, nel giudizio di (ir)responsabilità del provider occorre prima valutare la natura della sua condotta e poi occorre considerare l'elemento soggettivo che

---

[44] P. SAMMARCO, *Atti di concorrenza sleale attraverso Internet e responsabilità del "provider"*, in *Dir. inform.*, 2002, p. 100; F. DI CIOMMO, voce *Internet (responsabilità civile)*, in *Enc. Giur. Treccani*, 2002, p. 340 ss.; G. PASCUZZI, *Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche*, 2003, p. 127.

[45] L. BUGIOLACCHI, *Ascesa e declino della figura del provider attivo? Riflessioni in tema di fondamento e limiti del regime privilegiato di responsabilità dell'hosting provider*, in *Resp. civ. prev*., 2015, p. 1261.

[46] M.L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, cit., pp. 103 e 104.

[47] CdG, 23 marzo 2010, *Google c. Louis Vuitton*, C-236/08, in *EUR- Lex*; Trib. Milano, 7 giugno 2011, n. 7680, in *De Jure*. Cfr. M.L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, cit., p.106.

guarda al grado di conoscenza dell'attività illecita, aspetto quest'ultimo, così come si vedrà più diffusamente in seguito, che soggiace a criteri diversi, dati i differenti approcci affermatisi nella normativa di recepimento nazionale e nella prassi delle Corti[48].

3. Gli ulteriori servizi d'informazione e di comunicazione dell'ISP

Per avere un quadro chiaro dell'ampia portata delle attività dei provider, che dimostri ancora più intensamente quanto sia determinante il tema della responsabilità degli intermediari informatici, è opportuno comprendere quali siano i servizi offerti dagli stessi - oltre quelli essenziali di *mere conduit*, *hosting* e *caching* appena analizzati.

La classificazione funzionale dei servizi Internet che si propone è ripresa da una storica sentenza del giudice nordamericano che ha definito Internet come una "conversazione mondiale senza fine, la forma di comunicazione di massa più partecipativa che sia mai stata realizzata, la cui vera forza è il caos che essa stessa ha creato"[49].

Consapevoli dell'estrema difficoltà insita in ogni operazione definitoria, tanto più in un contesto quale quello tecnologico-telematico in continua evoluzione, si sono raggruppati i diversi servizi connessi all'utilizzo della rete offerti dagli *Internet service providers*, considerati in una prospettiva dinamico-funzionale, in base alla funzione cui gli stessi assolvono:

- i servizi di comunicazione interpersonale: il servizio di posta elettronica, le *mailing list* e i *newsgroup*, il servizio di telefonia via Internet (*VOICE-IP*), l'*Instant Messaging*, le *chat;*
- il *blog*;
- la fornitura di contenuti via web (*content provider*);
- la fornitura di servizi applicativi via Internet (l'*Application Service Provider*);
- I servizi accessori: *ex multis* i sistemi antivirus, filtri *antispamming*, posta certificata, i motori di ricerca, assistenza tecnica e consulenza, il B*ullettin Board Sistem* (BBS).

3.1 La comunicazione interpersonale

Internet, come rete globale, è lo strumento di comunicazione interpersonale più utilizzato al giorno d'oggi.

[48] R. BOCCHINI, *La responsabilità civile degli intermediari del commercio elettronico*, 2003, p. 159 e ss.; L. BUGIOLACCHI, *I presupposti dell'obbligo di rimozione dei contenuti da parte dell'hosting provider tra interpretazione giurisprudenziale e dettato normativo*, in *Resp. civ. prev*., 2017, p. 536 ss.

[49] Pronuncia della Corte Federale degli Stati Uniti dell'11 giugno 1996 (Distretto della Pennsylvania).

La sua caratteristica principale è infatti proprio quella di connettere terminali privati, consentendo loro di interagire mediante un protocollo comune (c.d. TPC/IP)[50].
Il protocollo TCP/IP indica l'uso combinato di due protocolli per la trasmissione di dati su internet, TCP (*Transmission Control Protocol*) e IP (*Internet Protocol*).
Il protocollo TCP crea la connessione tra due *host* e gestisce la consegna dei pacchetti da un sistema all'altro, mentre il protocollo IP fornisce le istruzioni per il trasferimento dei dati.

3.1.1 E-mail e mailing list

La forma di comunicazione telematica individuale più diffusa, seconda per grado di diffusione tra gli utenti solo alla connettività, è il servizio di posta elettronica, *l'e-mail*, consistente nella concessione da parte del provider di uno spazio sul proprio server: la casella di posta elettronica (la cosiddetta *mail-box*), utile all'utente per inviare e ricevere messaggi di posta elettronica.
L'art. 22 del DPR 445/2000 dà una definizione di indirizzo elettronico e lo presenta come "l'identificatore di una risorsa fisica o logica in grado di ricevere e registrare documenti informatici".
Si tratta della seconda forma di comunicazione più diffusa tra gli utenti[51].
Tale servizio comprende la fornitura di un indirizzo di posta elettronica, avente funzione di ricezione di messaggi nella mail box - intesa quale spazio di memoria di un server.
L'email consente quindi di ricevere ed inviare messaggi mediante il collegamento ad una casella personale. Si tratta di uno strumento rapido, sicuro e gratuito.
Le regole circa l'utilizzazione di tale servizio impongono l'utilizzo di un nome utente e di un dominio che identifica il server di ricezione della posta perché è ad esso collegato.
Il fornitore del servizio e-mail fornisce a colui che ne fa richiesta uno o più indirizzi mail, la possibilità di accedere alla casella di posta mediante username e password, uno spazio di memoria del server per consentire la conservazione dei messaggi che pervengono a quel determinato indirizzo.
Accanto a queste prestazioni principali, se ne possono accompagnare altre, alle volte a pagamento.

[50] M. GAMBINI, *Le responsabilità civile dell'Internet service provider*, cit., p. 25.
[51] Bisogna sottolineare e specificare che, data l'imprecisione terminologica della definizione di indirizzo elettronico, la sua esplicitazione e, soprattutto, il contesto normativo nel quale viene utilizzata, fanno ritenere che essa individui più propriamente la macchina connessa alla rete che funziona da server di posta elettronica e, soltanto per estensione, l'indirizzo di posta elettronica.

Si pensi ai sistemi antivirus, necessari a garantire la sicurezza e l'operatività del server, i filtri *antispamming*[52], i servizi di assistenza e consulenza tecnica online, la posta certificata[53].
Per posta elettronica certificata si intende ogni sistema di posta elettronica nel quale è fornita al mittente la documentazione elettronica attestante l'invio e la consegna dei documenti informatici[54].
Un utilizzo peculiare del servizio di posta elettronica è dato dalle *mailing list*. Queste ultime permettono la ricezione dei messaggi di posta elettronica indirizzati a tutti cloro che sono inseriti in una medesima lista.
Si tratta di un servizio che solitamente viene impiegato per agevolare e velocizzare gli aggiornamenti su determinati argomenti o quale forma di abbonamento a riviste telematiche. Si crea quindi un messaggio che viene poi trasmesso via posta elettronica a tutti gli abbonati alla newsletter, anche mediante smistamento automatico e periodico dei messaggi di trasmissione.
Lo scambio dei messaggi avviene in maniera differita nel tempo, mancando la compresenza degli interlocutori.
I destinatari generalmente possono inserire o togliere il proprio indirizzo dalla mailing list, mentre in casi specifici l'iscrizione alla lista deve essere autorizzata.
Spesso ai servizi di mailing list se ne accompagnano altri altrettanti noti come i forum, le chat, gli spazi per pagine web[55].
Attualmente le mailing list vengono utilizzate da gruppi di piccole dimensioni, magari focalizzati su uno stesso interesse, si pensi agli hobbies, alle attività professionali, allo sport, ai progetti.

---

[52] La ricezione di posta elettronica indesiderata sulla propria casella e-mail (o spazzatura, da cui *spamming*), quasi sempre a scopi pubblicitari, ha assunto oramai dimensioni da "piaga telematica": nel 2003 circa il 40% delle e-mail circolate sulla rete era costituito da posta indesiderata.
Il fenomeno, cui gli stessi provider stanno cercando di porre rimedio, onde evitare la disaffezione dell'utente verso questo comodo ed efficiente mezzo di comunicazione, nasce dalla pericolosa, ma diffusa, abitudine di rendere pubblici o propri indirizzi e-mail sulle pagine web, rendendoli così di facile preda degli "*spider*", programmi automatici che navigano su Internet alla ricerca di tutto ciò che somigli ad un indirizzo e-mail.
[53] M. GAMBINI, *Le responsabilità civile dell'Internet service provider*, cit., pp. 26-27.
[54] Tale definizione la ritroviamo nel d. P.R. 11 febbraio 2005, n. 68, "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n.3" (G.U. n. 28 marzo 2005, n. 97).
Successivamente, sono state approvate le "Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata" (D.M.- Ministro per l'innovazione e le tecnologie del 2 novembre 2005, in G.U. del 15 novembre 2005) con conseguente piena operatività del sistema P.E.C.
[55] M. GAMBINI, *Le responsabilità civile dell'Internet service provider*, cit., p. 28.

3.1.2 Newsgroup

Per newsgroup si intendono quelle bacheche elettroniche pubbliche o rubriche dedicate in cui un soggetto può inserirsi per essere aggiornato o informato circa un determinato aggiornamento.

L'utente inscrivendosi al servizio newsgroup con un programma dedicato o multifunzione può leggere i messaggi degli altri compartecipi ed aggiungere i propri contributi, rendendoli disponibili per tutti i partecipanti.

Si crea in questo modo una sorta di dibattito telematico, seppur asincrono, in cui i soggetti possono organizzare conferenze in rete leggendo e pubblicando articoli e scritti.

Dal punto di vista tecnico, l'accesso è reso possibile mediante il *news-server*, un elaboratore che ospita aree di discussione a cui i singoli utenti accedono, usufruendo di alcuni programmi di collegamento installati sui propri terminali.

Non si tratta necessariamente di un sito web ma di uno spazio concesso da un provider su un suo *server*, che ospita i messaggi degli utenti che intendono contribuire al dibattito su specifiche tematiche.

In genere si tratta di luoghi virtuali ad accesso libero, non moderati e dunque sottratti ai poteri di controllo del provider ma esistono anche newsgroup che si caratterizzano per una forma di controllo e di coordinamento generalizzato, affidato ad un coordinatore che analizza i messaggi in arrivo, gestisce le comunicazioni tra gli utenti, cancella gli eventuali interventi non coerenti con i requisiti formali e sostanziali del gruppo[56].

Può trattarsi dello stesso provider ospitante, ovvero questi può servirsi di un soggetto che assume il compito, spontaneamente o contrattualmente, di vigilare sulla pertinenza e liceità dei contenuti immessi nel sito.

A differenza delle mailing list, gli utenti non devono iscriversi previamente in una lista e quindi non ricevono dei messaggi sulla propria casella di posta elettronica.

Nati nel 1979, sono i servizi più antichi di Internet. Prima del web, i newsgroup erano proprio il luogo virtuale di ritrovo per discutere di vari argomenti. Ad oggi si contrano decine di migliaia di conferenze, organizzate e classificate secondo criteri ben precisi.

Continuano a svolgere il loro compito di bacheche virtuali, consentendo agli utenti di leggere i messaggi scritti da altre persone e di partecipare con i propri contributi, in maniera del tutto asincrona, dunque non in tempo reale, alla discussione sugli argomenti trattati.

[56] M. GAMBINI, *Le responsabilità civile dell'Internet service provider*, cit., p.28.

In sostanza, è possibile sostenere che queste bacheche pubbliche telematiche o rubriche dedicate siano impostate secondo il modello delle bacheche universitarie, in cui un soggetto si inserisce per essere aggiornato su un determinato argomento.
Il forum, noto ai più, altro non è se non una forma peculiare di newsgroup: si tratta di pagine web che consentono di leggere e scrivere messaggi sia di risposta che del tutto nuovi.
Si differenziano dal modello tradizionale di newsgroup perché non sono indicizzati e catalogati[57].

3.1.3 Instant Messaging e chat

L'Instant Messaging e le chat si caratterizzano per la compresenza degli utenti e per l'immediatezza comunicativa, realizzando la forma più evoluta di connessione in tempo reale.
Tale sincronia, a differenza delle bacheche telematiche e dei servizi di posta elettronica, riproduce in via informatica la velocità e la vivacità del dialogo diretto, senza che sia necessario svelare all'utente l'identità reale dell'interlocutore.
Gli utenti, tramite appositi software, possono essere permanentemente in comunicazione multimediale purché siano tutti on line nello stesso momento. Nel caso in cui un contatto sia offline al momento dell'invio della comunicazione, il messaggio sarà ricevuto al successivo collegamento ed attivazione del programma dedicato.
Spesso integra sistemi di comunicazione di diversa natura[58], consentendo di ricevere messaggi di testo sul telefono e su altro dispositivo.
Le potenzialità comunicative delle chat hanno riscosso un notevole successo, tanto da divenire un fenomeno "sociologicamente rilevante"[59]. Viene data la possibilità a soggetti, che si trovano distanti migliaia di chilometri, di essere virtualmente compresenti.
Si tratta, infatti, del sistema interattivo virtuale più diffuso attualmente, in grado di riprodurre ed emulare la più tradizionale comunicazione telefonica attraverso l'intermediazione informatica e la rete Internet[60].
L'efficienza ed il livello di qualità del sistema è strettamente proporzionale alla velocità ed alla stabilità della rete di connessione.

[57] M. GAMBINI, *Le responsabilità civile dell'Internet service provider*, cit., pp. 29-30.
[58] Si pensi ai cellulari o ai palmari.
[59] M. GAMBINI, *Le responsabilità civile dell'Internet service provider*, cit., p. 32.
[60] Tramite un microfono, eventualmente una webcam, ed un apposito programma (o anche via *browser web*) all'utente viene offerta la possibilità, a tariffe vantaggiose, di effettuare telefonate o video telefonate in tutto il mondo, sia ad utenti connessi a loro volta via Internet, sia ad utenti connessi al normale apparecchio telefonico.

In tal caso sarà possibile utilizzare il servizio di telefonia *over Ip* offerto dal proprio provider di accesso (*mere conduit*) oppure uno qualunque dei diversi fornitori del servizio specifico di *"voice over Ip",* la cui operatività è strettamente connessa a quella della rete a cui sono collegati grazie al provider.

Dal punto di vista più strettamente tecnico, viene messo a disposizione degli utenti uno spazio di memoria degli elaboratori del provider che fornisce il servizio, permettendo così l'instaurazione di legami telecomunicativi.

L'*Instant Messaging* consente agli utenti, tramite appositi *software*, di essere permanentemente in comunicazione multimediale[61] con una lista di persone predefinita oppure con soggetti di cui si conosce almeno l'indirizzo *e-mail*, purché siano *on line* nello stesso momento[62].

3.2 Content provider

Il Tribunale di Bologna, nella sentenza 331/2001, ha definito il *Content Provider* come "l'operatore che mette a disposizione del pubblico informazioni ed opere (riviste, fotografie, libri, banche dati, versioni telematiche di quotidiani e periodici), caricandole sulle memorie dei computer server e collegando tali computer alla rete. Content provider è anche chi si obbliga a gestire e ad organizzare una pagina web immessa in rete dal proprio cliente".

L'attività di *content providing* si esplica, pertanto, attraverso la fornitura di contenuti destinati ad essere distribuiti e fruiti attraverso tutte le tecnologie di riproduzione compatibili con il protocollo TCP/IP (testi, immagini, grafici, animazioni, video e audio, etc..), in genere realizzati o comunque organizzati e selezionati dalla redazione del provider o anche da soggetti terzi, a seconda della necessità del cliente.

Il *content* provider, più che un fornitore di tecnologie dell'informazione e della comunicazione, è un fornitore di contenuti, di servizi informativi e mette a disposizione dell'utente (si tratta quasi sempre di aziende) un servizio di realizzazione di pagine web, più o meno complesse e articolate, al cui interno sono reperibili varie tipologie di informazioni, strutturate o meno in vere e proprie banche dati che dallo stesso provider vengono proposte, organizzate e gestite[63].

[61] Siano esse comunicazioni testuali, audio o audio-video…

[62] In caso contrario il messaggio verrà ricevuto dall'altro utente al successivo collegamento ed attivazione del programma dedicato.

[63] M. GAMBINI, *Le responsabilità civile dell'Internet service provider*, cit., pp. 32 e 33.

Può altresì offrire l'accesso a contenuti multimediali, a programmi di vario tipo e documenti, messi a disposizione sul proprio sito. Più spesso ci troviamo di fronte ad un vero e proprio portale, ossia ad un sito che offre una molteplicità di servizi[64].

A richiesta, poi, possono essere forniti servizi aggiuntivi rispetto a quelli tipicamente editoriali, banche dati testuali, si pensi alle banche dati normative e giurisprudenziali, banche dati multimediali, come gli archivi musicali dai quali si può scaricare musica a pagamento sul proprio pc, aggiornamenti sulle ultime notizie (attualità, mondanità, cinema, sport, musica, etc.) servizio di oroscopo giornaliero ed altro.

Sempre più spesso, l'attività posta in essere dal content provider non si limita alla costruzione delle pagine HTML statiche, e dunque di sola lettura, ma include anche la funzionalità avanzate che permettono ai visitatori del sito di interagire in vari modi direttamente con i sistemi informativi dell'azienda, di cui il provider ha realizzato il sito web, ad esempio mediante la consultazione in tempo reale del relativo catalogo dei prodotti ed anche la realizzazione di piattaforme di commercio elettronico che consentano l'acquisto dei prodotti e servizi aziendali direttamente dal web[65].

Il grado di coinvolgimento del *content* provider è, come si può facilmente intendere, all'evidenza massimo con l'informazione immessa in rete, essendone egli l'autore e conservando sulla stessa il pieno controllo sin dal momento della creazione[66].

Il suo ruolo dunque non rientra nella prestazione di un servizio ed è più ampio rispetto a quello di chi esercita una mera attività di intermediazione tecnica[67].

3.3 La fornitura di servizi applicativi via Internet: ASP

Se gli applicativi di commercio elettronico possono essere vantaggiosamente alloggiati in tutto o in parte presso il provider, forse lo stesso si può dire anche per le altre componenti software ed al limite per l'intero Centro Elaborazione Dati (CED) aziendale.

---

[64] Si tratta di servizi dai contorni non troppo definiti, cui fanno talvolta riferimento i contratti, con clausole del tipo "il provider si impegna a fornire pire software per Windows e/o Apple", a significare che il provider ha installato un archivio o una banca dati di software sulle proprie pagine.

[65] M. GAMBINI, *Le responsabilità civile dell'Internet service provider*, cit., p. 33.

[66] O. TROIANO, *L'impresa di content, host e access providing*, in *AIDA*, 2011, p. 201.

[67] La divisione delle attività di un Internet service provider è accettata da S. SICA, *Il sistema delle responsabilità*, in S. SICA-G. COMANDÈ, *Il commercio elettronico*, Torino, 2001, p. 221 ss.; P. STANZIONE, *Commercio elettronico e altre categorie civilistiche*, in S. SICA- P. STANZIONE, *Commercio elettronico e categorie civilistiche*, 2002, p. 37 ss.; G.M. RICCIO, *Profili di responsabilità civile dell'Internet Provider*, in *Quaderni del Dipartimento di Diritto dei rapporti civili ed economici nei sistemi giuridici contemporane*i, diretti da P. Stanzione, Salerno, 2000, p. 19 ss.; T. HOEREN-R. PICHLER, *Zivilrechtliche Haftungim Online-Bereich*, in U. LOEWENHEI-F.A. KOCH, *Praxis des Online-Rechts*, Weinheim, 1997, p. 107 ss.

Dall'evoluzione dei servizi di housing è nata, pertanto, una nuova figura di azienda che si occupa della gestione centralizzata degli applicativi (*Application Service Provider* o ASP), fornendo e gestendo, attraverso una rete di trasmissione, l'utilizzo di un'applicazione, di un programma a diversi soggetti da un unico centro di elaborazione dati.

Si tratta, comunque, di un tipo di azienda del tutto nuova, che, nel panorama più vasto dell'informatica, trova i suoi precedenti nei servizi di *outsourcing*, erogati dalle aziende che gestiscono progetti ed applicazioni per conto del cliente.

Vi sono però alcune differenze importanti tra un *outsourcer* ed un *ASP*, in quanto il primo gestisce i clienti uno per uno e non si occupa solo di informatica, mentre nel caso dell'*ASP* un certo servizio viene sempre proposto a molti clienti e si occupa principalmente di aspetti tecnico-informatici.

Il successo delle applicazioni distribuite via *ASP* è inevitabilmente legato all'efficienza ed alla velocità delle reti trasmissive, dalle quali risulta dipendere il loro regolare ed utile funzionamento.

Per quanto riguarda le tipologie di applicazioni o di servizi forniti dagli *ASP*, si va dal software di produttività individuale[68] al software cosiddetto collaborativo[69], passando attraverso la gestione di servizi essenziali trasversali, quali contabilità, gestione del personale, gestione del magazzino, per arrivare fino agli applicativi cosiddetti verticali, specifici per una certa azienda.

3.4 Servizi accessori

Accanto ai principali servizi Internet ed ai servizi strettamente connessi già richiamati nell'analisi delle attività principali (assegnazione numeri Ip; installazione di dispositivi di sicurezza e di protezione degli utenti quali antivirus, firewall, filtri antispamming, etc.; assistenza tecnica e consulenza inerenti l'uso delle reti; posta certificata) possono aggiungersi ulteriori servizi Internet di tipo accessorio, in quanto connessi, in funzione strumentale, ad altra prestazione principale, in particolare di *hosting*, *housing* o *content providing*[70].

Meritano di essere ricordati, innanzitutto, i motori di ricerca, ossia quei siti che consentono agli utenti di cercare e di reperire informazioni in rete utilizzando parole-chiave.

---

[68] Si pensi all'elaborazione dati e di testi, fogli di lavoro, calendari, etc.

[69] *Groupware*, messaggistica, teleconferenza.

[70] F.D. BUSNELLI, *Nuove frontiere della responsabilità civile*, in *Jus Civile*, 1976, p. 41 ss.; M. LIBERTINI, *Le nuove frontiere del danno risarcibile*, in *Contr. e impr*., 1987, p. 85 ss.

Tecnicamente sono databases che indicizzano i siti e i testi cercati ed offrono un accesso per la loro consultazione.

I motori di ricerca svolgono una funzione di fondamentale importanza nella navigazione in rete. Visto che i siti sono numerosissimi, circa tre miliardi, senza i motori di ricerca l'accesso ad un sito sarebbe possibile solo conoscendone l'esatto indirizzo telematico.

Senza i *search engines* non sarebbe possibile la ricerca casuale delle informazioni.

Digitando parole-chiave il *search engines* conduce al sito o all'informazione desiderata o propone una serie di risultati della ricerca pertinenti con il criterio di ricerca impostato dall'utente.

I motori di ricerca utilizzano diversi sistemi: i più diffusi sono quelli tramite *spiders* e *metatags*[71].

Nel primo sistema i siti ed i testi sono reperiti ed organizzati attraverso appositi software, o meglio attraverso appositi programmi, i cosiddetti *spiders*. I motori provvedono tramite gli *spiders* ad una lettura dei siti presenti nella Rete e ad una loro classificazione sintetica per poi proporre un indice di risultati pertinenti con il criterio di ricerca impostato dal navigatore.

Nel secondo sistema il motore cerca i *metatags* corrispondenti alla parola chiave usata dal navigatore per la ricerca.

I *metatags* sono, infatti, "etichette elettroniche" presenti nelle testate delle *home page* che descrivono sinteticamente il contenuto del sito attraverso parole che possono corrispondere a quelle impostate dal navigatore per la ricerca.

Il sistema basato su *metatags* è molto diffuso oggigiorno soprattutto perché è immediatamente efficace e semplice, più di quanto lo sia il sistema *spider*.

In tale sistema infatti il motore, attraverso le etichette elettroniche, provvede a raccogliere le informazioni proposte ed infine offre all'utente una serie di risultati pertinenti con il criterio di ricerca impostato.

Allo scopo di portare ad un sito il numero maggiore possibile di visitatori, è necessario procedere alla registrazione dello stesso presso i principali motori di ricerca oggi disponibili sul web (*Google, Yahoo,* etc.) in modo da far sì che il sito stesso possa essere rintracciato anche da utenti che non ne conoscano direttamente l'indirizzo web.

Anche questa attività può essere svolta in prima persona dal titolare o responsabile del sito, magari avvalendosi degli operatori che prestano questo tipo di attività a titolo gratuito, oppure ricorrendo alle prestazioni di un provider specializzato, ad esempio, nel caso in cui

[71] M. DE CATA, *La responsabilità civile dell'Internet service provider*, cit., pp. 68-69.

al numero di visitatori delle proprie pagine web possa essere direttamente collegato un aumento del volume di affari. È ciò che accade sui siti di *e-commerce*.

In quest'ultimo caso, l'oggetto della prestazione offerta dal provider è portare al sito in questione traffico di qualità, cioè visitatori autenticamente interessati ai prodotti o ai servizi presenti sulle pagine web del contraente.

Per ottenere questo risultato, sono necessarie le seguenti operazioni che giustificano il ricorso ad un professionista specializzato:

- studio delle parole chiave, da sottoporre al motore di ricerca per la descrizione del sito e sulle quali avverrà in via prioritaria la ricerca;
- analisi della concorrenza, allo scopo di indirizzare il più possibile la ricerca dei beni e servizi sul sito prescelto e di evitare che l'utente finisca sul sito del concorrente;
- ottimizzazione delle pagine, anche attraverso le modifiche delle stesse e l'inserimento nel testo in chiaro o nel codice HTML delle parole chiave precedentemente identificate;
- richieste di inserimento del sito nelle directories, una sorta di elenchi o indici dei motori di ricerca;
- richiesta di registrazione presso i motori di ricerca italiani ed internazionali;
- attivazione di sponsorizzazioni a pagamento basate sul numero di click ricevuti, *pay-per-click*;
- iniziative a favore dello scambio di link ad un certo sito per attribuirgli una posizione migliore nella lista dei risultati, come Google;
- eventuale promozione su portali telematici, tramite, annunci, banner[72], sponsorizzazione di newsletter;
- monitoraggio del posizionamento e studio delle opportune misure migliorative[73].

Oltre ai motori di ricerca, va ricordata l'attività di assistenza tecnica, amministrativa e giuridica, per la registrazione di un nome di dominio presso l'autorità, *Naming Autorithy*, deputata in Italia all'assegnazione, che detiene il registro del *country code Top Level Domani* ".it" ed è responsabile dell'assegnazione dei nomi a dominio.

---

[72] Si tratta di uno strumento molto diffuso in rete per aumentare il traffico utenti di un certo sito. È una forma di pubblicità *on-line*, attuata tramite l'utilizzo di striscioni statici o animati contenenti il logo o lo slogan dell'azienda pubblicizzata, posizionati in testa alla *home page* ed alle altre pagine di un sito Internet. Quando l'utente clicca sul *banner*, viene trasportato sulla pagina dell'azienda a cui il *banner* stesso è collegato, tramite *link.*

Attraverso tale strumento, l'operatore influisce, organizzandola, sulla fruizione dei siti ospitati o richiamati, incrementandone il relativo traffico e, ad un tempo, incide, orientandola, sulla libera navigazione in rete degli utenti.

[73] M. GAMBINI, *Le responsabilità civile dell'Internet service provider*, cit., pp. 37 e 38.

Si tratta di una funzione molto importante perché attribuisce al sito un nome che vale ad identificarlo in maniera univoca sulla Rete[74].

Il criterio utilizzato segue l'ordine cronologico delle richieste così come esplicitato nella regola *first come first serve.*

Il provider che presta tale servizio, detto anche *maintainer*, registra e gestisce il mantenimento di nomi a dominio per conto dei suoi clienti, stipulando, a sua volta, un apposito contratto con l'Istituto di Informatica e Telematica del CNR.

Il servizio di registrazione del dominio si affianca, di norma, quale prestazione accessoria, al contratto principale di messa a disposizione di uno spazio web (*hosting o housing*), oppure può essere fornito come servizio autonomi oggetto di un separato contratto con il *maintainer*.

In entrambi i casi le prestazioni principali del fornitore di questo particolare servizio consistono:

- nell'eseguire tutte le operazioni di registrazione del nome a dominio per conto del cliente;
- nel richiedere, sempre per conto del cliente, l'assegnazione del nome a dominio ai competenti organismi nazionali ed internazionali preposti a tali operazioni, secondo le modalità indicate dagli stessi;
- nel gestire il servizio di rinnovo della registrazione del dominio.

La titolarità del dominio registrato spetta al richiedente la registrazione o, più precisamente, al soggetto a cui favore viene richiesta la registrazione stessa, che assume su di sé ogni più ampia responsabilità in ordine all'utilizzo del nome di dominio assegnato, con espresso esonero del *maintainer* da ogni forma di responsabilità al riguardo.

Merita menzione anche il cosiddetto *accounting*, cioè l'invio di un rapporto periodico col riepilogo delle connessioni, del traffico, degli accessi al sito, delle informazioni maggiormente prelevate dal navigatore e così via.

La conoscenza di tali dati consente di orientare l'offerta informativa da indirizzare a quel dato utente e, più in generale, di migliorare l'informazione in rete.

Ciò rende tale servizio, per sua natura accessorio rispetto alla prestazione principale di accesso o di messa a disposizione dello spazio *web*, un importante strumento di *marketing* a disposizione dei titolari o gestori del sito *web*, specie per i casi in cui attraverso lo stesso venga esercitata un'attività di commercio elettronico[75].

[74] M. GAMBINI, *Le responsabilità civile dell'Internet service provider*, cit., p. 36 ss.
[75] M. GAMBINI, *op. cit.*, pp. 38 e 39.

3.4.1. Bullettin Board Sistem

La tipologia di provider può essere ulteriormente specificata e tende a crescere con l'evoluzione dei mezzi tecnologici: vi sono operatori che garantiscono all'utente, tramite motori di ricerca, il reperimento di siti ricercati[76] ed altri ancora che garantiscono i servizi di messaggeria, il cosiddetto *Bullettin Board operator.*

Inizialmente questi *BBS* erano sistemi di comunicazione usati in "reti chiuse" del tipo Intranet. Con l'avvento di Internet, i *BBS* si sono trasformati in bacheche dati "aperte". [77]

Più precisamente, i *BBS* sono bacheche elettroniche che consistono in database organizzati automaticamente per argomento.

L'accesso è solitamente libero, senza necessità di abbonamento e persino senza bisogno di iscrizioni ad apposite liste, presupposto invece richiesto per la partecipazione ai *newsgroup.*

Ciascun utilizzatore può inviare informazioni scegliendo la casella pertinente per argomento e raccogliere le informazioni immesse da altri utenti riversandole nel proprio computer (*client computer*).

Dunque chiunque, collegandosi ad un *BBS*, può liberamente caricare (*upload*) informazioni e scaricare (*download*) materiali immessi da altri, determinando una propagazione di dati a livello mondiale.

Infatti non solo le informazioni scaricate possono essere trasmesse individualmente ad altri utenti ma, quando un'informazione è immessa in un server *"usenet",* un programma automatico la invia a tutti gli altri *server* deputati alla funzione *BBS* presenti nel mondo.

4. Profili conclusivi

Alla luce dell'analisi fatta è venuto fuori in modo evidente e pacifico come l'informatica debba essere intesa comunemente come quel ramo della scienza e della tecnica che tratta i sistemi per l'elaborazione delle informazioni, sia sotto l'aspetto logico-progettuale, di ricerca e sviluppo di nuovi componenti o circuiti, l'*hardware,* sia per quanto si riferisce all'architettura ed alla preparazione dei *software* (programmi), sia infine per ciò che concerne l'impiego dei mezzi di elaborazione nei numerosi campi in cui essi sono applicati[78].

---

[76] Il noto *information location tool provider.*

[77] M. DE CATA, *La responsabilità civile dell'Internet service provider*, cit., p. 69.

[78] Che al centro di questa branca scientifica ci sia l'informazione, nel senso del contenuto informativo del dato, risulta evidente anche dalla derivazione etimologica del termine, data che la corrispondente espressione francese, l'*informatique*, deriverebbe dalla contrazione di "informazione" *(information*) e "automatica" (*automatique*), a sottolineare proprio l'applicazione di automatismi al trattamento delle informazioni.
La corrispondente espressione anglosassone, in uso ancora oggi, del resto, manifesta e conferma questa concezione dell'informatica come tecnologia dell'informazione (*Information technology*, anglicismo usualmente abbreviato nel noto acronimo IT).

L'informatica è, dunque, tecnologia dell'informazione, trattamento automatizzato (ieri meccanico ed oggi digitale, cioè basato sull'utilizzo della tecnologia binaria) del contenuto informativo insito in ogni dato o insieme di dati.

L'applicazione diffusa delle tecnologie elettroniche di elaborazione dei dati, specialmente con l'avvento dei *personal computer*, non si pone rispetto al trattamento delle informazioni in un rapporto meramente strumentale, avendo, invece, stravolto il concetto e la natura stessa di informazione.

Essa, in quanto informazione automatizzata, ha assunto, infatti, caratteri del tutto peculiari[79]. In primo luogo, il fatto di risiedere in un sistema automatizzato e di essere accessibile attraverso un collegamento tra elaboratori elettronici, determina l'accentuarsi della sua natura intangibile, dematerializzata e volatile, oltre a giustificare la stretta commistione che in essa si realizza tra contenente e contenuto, tra il dato informativo ed il dato tecnologico.

L'avvento delle tecnologie dell'informazione non rappresenta, quindi, soltanto una ulteriore tappa nel processo storico di sviluppo delle tecniche di trasmissione della conoscenza ed esperienza umana: dalle primitive tecniche fondate sull'utilizzo del senso della vista (gesti, segnalazione ottica, scrittura), alle tecniche fondate sull'udito (parola, segnalazioni sonore) fino ad arrivare alla moderna società industriale ed al conseguente utilizzo diffuso delle tecnologie elettriche (telegrafo e telefono) ed elettroniche (radio e televisione) e, oggi, alla veicolazione delle informazioni attraverso i canali informatici e telematici, caratterizzati dall'immaterialità dei modi in cui esse vengono comunicate e apprese entro la dimensione virtuale della rete.

Se da ciò, in positivo, consegue una maggiore facilità ed un aumento delle possibilità di raccolta, consultazione e scambio dati da una parte all'altra del mondo, a prezzi e tempi contenuti; in negativo, non può non discenderne la difficoltà, quando non addirittura l'impossibilità, di controllare ed impedire, sul piano materiale prima ancora che giuridico, le forme telematiche di trasmissione, comunicazione e diffusione dei dati informativi e, dunque, di poter disporre di una coerente ed efficace disciplina della circolazione giuridica dell'informazione computerizzata.

Si segna dunque il passaggio ad una nuova epoca, l'epoca dell'era digitale o delle tecnologie informatiche e telematiche, così come un po' enfaticamente si è soliti affermare, perché è il concetto stesso di informazione che ne risulta cambiato: non è più informazione come

[79] Secondo V. Zeno Zencovich, la diffusione delle nuove tecnologie informatiche e telematiche cambia qualitativamente l'informazione, pone nuovi problemi all'interprete e soprattutto dà vita a nuove entità, la cui qualificazione come beni è appunto in discussione: si pensi agli ipertesti, ai motori di ricerca, ai *domain names.*

messaggio statico, ma come messaggio dinamico, in quanto destinato alla trasmissione ed in quanto facilmente trattabile ed elaborabile[80].

Quanto al connotato della trasmissibilità, l'informazione elettronica è, per sua natura, estremamente adatta alla comunicazione ed alla diffusione, non avendo bisogno di intermediari ed essendo fruibile dagli altri a costi contenuti ed in tempi rapidissimi, tanto da renderla informazione di tipo recettizio, nel senso che per essere tale deve essere comunicata, dal produttore al destinatario individuato o alla collettività.

[80]A. PALMIERI, *I contratti di accesso*, Milano, 2012.

CAPITOLO SECONDO

Criteri di imputazione della responsabilità civile dell'intermediario della rete. Una lettura (anche) in chiave comparatistica

SOMMARIO: 1. Responsabilità del provider e possibili criteri di imputazione. - 1.1 *Strict liability* e teoria del rischio d'impresa. - 1.2 *Vicarious liability* e responsabilità per il fatto altrui. - 1.3 Ricorso alla responsabilità per i danni cagionati da cose in custodia. - 1.4 Ricorso alla responsabilità per esercizio di attività pericolosa. - 1.5 Approdo al criterio di imputazione a carattere colposo. - 2. La responsabilità civile degli intermediari della rete nel sistema americano. - 3. La responsabilità civile degli intermediari della rete nel modello europeo. - 4. La responsabilità del provider nell' esperienza inglese. - 5. La responsabilità del provider nell' esperienza francese. - 6. La responsabilità del provider nell' esperienza tedesca.

1. Responsabilità del provider e possibili criteri di imputazione

Il *punctum dolens* da esaminare ai fini dell'individuazione della responsabilità del provider non riguarda tanto i casi in cui la condotta antigiuridica sia imputabile direttamente all'intermediario, quanto piuttosto i casi in cui il servizio offerto in Rete sia stato il mezzo per la commissione dell'illecito da parte degli utilizzatori.

La questione che merita maggiore attenzione e che solleva più problematiche non è rappresentata dalla responsabilità del provider per il fatto proprio ma per il fatto altrui o per omessa vigilanza sulla condotta degli utenti.

Nella rete il rapporto intersoggettivo non è bilaterale ma trilaterale perché coinvolge il danneggiante, l'intermediario ed il danneggiato e non solo danneggiante e danneggiato.

Il fine è quello di individuare o comunque predisporre degli strumenti che possano impedire o ridurre le possibilità di danno e l'aggravarsi delle relative conseguenze con maggiore efficienza.

La responsabilità del provider per fatto illecito degli utenti ha visto, con varietà di sfumature ed argomentazioni, diverse posizioni da quella favorevole all'irresponsabilità dell'intermediario di servizi telematici a quella opposta, incline ad accollare all'Internet Service Provider l'obbligo risarcitorio in base a criteri di imputazione oggettivi, fino a giungere all'utilizzazione del criterio della colpa[81].

Il bilanciamento di interessi imposto dall'esigenza di tutelare i diversi diritti degli utenti è arduo nella misura in cui coinvolge gli aspetti più intimamente legati alle libertà fondamentali della persona.

La scelta di un criterio di imputazione piuttosto che di un altro, motivata anche da ragioni di tipo economico, potrebbe produrre degli effetti di *underdeterrence* o *overdeterrence*[82].

Da un lato vi è chi privilegia l'interesse a dare il massimo impulso possibile alla Rete non gravando i providers, soggetti fondamentali per il funzionamento di Internet e per lo sviluppo del commercio elettronico, dei costi derivanti dagli obblighi risarcitori, dal lato opposto vi è chi, a causa della potenzialità offensiva del nuovo mezzo di comunicazione, si manifesta incline a non lasciare il danneggiato privo di ristoro, anche in assenza di colpa dell'intermediario o a prescindere da questa[83].

In sostanza si pone anche in ambito telematico la tradizionale alternativa tra lasciare il danno senza ristoro o individuare un soggetto che, indipendentemente da una propria colpa, appare idoneo a prevenirlo e risarcirlo.

Da un punto di vista più generale, secondo una prima tesi, la scelta di un criterio di responsabilità poco severo non sarebbe efficiente perché i providers, certi della loro impunità, non adopererebbero alcuno sforzo di diligenza nel controllo delle attività degli users, né sarebbero indotti ad investire risorse nell'adozione o nella ricerca di sistemi idonei a prevenire gli illeciti in Internet.

Secondo la tesi opposta, l'adozione di un regime di responsabilità eccessivamente severo provocherebbe un corto circuito del sistema perché i providers meno solidi dal punto di vista

---

[81] M. DE CATA, *La responsabilità civile dell'internet service provider*, cit., p. 75 ss.

[82] A. YEN, *A preliminary economic analysis of Napster: Internet Technology, Copyright liability and the possibility of Coasen Bargaining*, in *Dayton*, 2000, p. 248 ss.

[83] L. NIVARRA, *Responsabilità del provider*, in *Dig. Disc. priv*., 2003, p. 1996 ss.; F. DI CIOMMO, *Internet, diritti della personalità e responsabilità aquiliana del provider*, in *Danno e resp*., 1999, p. 756 ss.; G. CASSANO-I. CIMINO, *Il nuovo regime di responsabilità dei providers: verso la creazione di un novello "censore telematico"*, in *Contratti*, 2004, p. 90 ss.; S. SICA-G. COMANDÈ, *Il commercio elettronico*, cit., p. 230; E. TOSI, *I problemi giuridici di Internet*, Milano, 2001, p. 523 ss.; G. FACCI, *La responsabilità extracontrattuale dell'internet provider*, in *Resp. civ. prev*., 2002, p. 265 ss.; C. GATTEI, *Considerazioni sulla responsabilità dell'internet provider*, in *www.interlex.it*; S. TORRIANI-O. PARISE, *Internet e diritto*, Milano, 1998, p. 130 ss.; G.M. RICCIO-S. PERON, *Responsabilità extracontrattuale: problematiche connesse all'utilizzo della Rete Internet*, in *Resp. civ. prev*., 2000, p. 820 ss.

economico, e pertanto non idonei a sopportare i costi derivanti dalla scelta di un criterio di responsabilità gravoso, abbandonerebbero il mercato, con l'effetto di determinare una concentrazione oligopolistica degli operatori, con effetti deleteri sul pluralismo di Internet[84].
In più, ne risulterebbe pregiudicato il diritto di manifestazione del pensiero degli utenti della Rete: tale diritto fondamentale resterebbe così assoggettato al "sindacato censorio"[85] di soggetti privati sforniti di ogni legittimazione istituzionale e mossi più che dal perseguimento del pubblico interesse, dalla valutazione della convenienza economica delle loro scelte[86].
D'altra parte, è pur vero che non si può lasciare che il web diventi un "far-west" mediatico, privo di tutela ed indifferenti agli illeciti più gravi che minano i diritti fondamentali degli internauti e, più in generale, dei soggetti dell'ordinamento.
Si pensi, a titolo esemplificativo, agli atti illeciti lesivi della reputazione, della dignità umata *et similia*…
Proprio per cercare di trovare una via mediana che possa far fronte agli effetti indesiderati c'è chi anziché optare per una soluzione unica e specifica si è mostrato favorevole a valutare i singoli casi concreti e dunque scegliere di volta in volta i diversi criteri di imputazione dell'ordinamento a seconda delle fattispecie concrete, con distinzioni tra i vari servizi offerti in rete e tra le diverse tipologie di operatori.
L'approccio *case by case* certamente porta con sé il vantaggio della flessibilità ma senza dubbio si presta a diventare una modalità eccessivamente rischiosa, volta ad una discrezionale e dunque pericolosa parcellizzazione della materia[87].
Pertanto, pur facendo salve le debite eccezioni e distinguo, necessario ed assolutamente imprescindibile risulta essere l'individuazione di un criterio di imputazione per responsabilizzare il provider.
Tuttavia, per poter meglio comprendere i possibili scenari attuali e futuri risulta fondamentale ripercorrere le posizioni che specie in passato hanno caratterizzato gli orizzonti della materia.

---

[84] G. PONZANELLI, *Verso un diritto uniforme per la responsabilità degli internet service provider*, in P. STANZIONE-S. SICA, *Commercio elettronico e categorie civilistiche*, Milano, 2002, p. 371; L. BUGIOLACCHI, *La responsabilità dell'host provider alla luce del d. legisl. n. 70 del 2003: esegesi di una disciplina "dimezzata"*, cit., p. 201 ss.; U. RUFFOLO, *La tutela del navigatore in Internet*, Milano, 2002, p. 183 ss.
[85] S. RODOTÀ, *Libertà, opportunità, democrazia, informazione*, in *https://www.privacy.it*.
[86] M. DE CATA, *La responsabilità civile dell'internet service provider*, cit., pp. 76 e 77.
[87] T. PASQUINI, *Servizi telematici e criteri di responsabilità*, Milano, 2003, p. 237 ss.; F. RUGGIERO, *Individuazione nel cyberspazio del soggetto responsabile e ruolo dell'Internet provider*, in *Giur. it.*, 2001, p. 601 ss.

1.1 Strict liability e teoria del rischio d'impresa

L'analisi comparatistica denota come la giurisprudenza, primo formante ad essersi confrontato con la questione, abbia, nei diversi sistemi, seguito una linea evolutiva simile, facendo prima ricorso ad ipotesi di *no-fault liability* ed optando, solo in un momento successivo, per un criterio di imputazione a carattere colposo[88].

L'esperienza americana al riguardo è stata molto significativa, facendo luce con le prime applicazioni in materia.

Ictu oculi, si è pensato, nei primi casi giurisprudenziali, di poter far ricorso all'analogia e ricondurre la posizione del provider alla figura del *publisher*. L'attrazione della responsabilità dell'intermediario informatico nell'alveo della responsabilità editoriale è stato considerato strumento utile per individuare una forma di responsabilità oggettiva.

Non è da trascurare, in questo senso, la circostanza che, nella maggior parte delle vicende giudiziarie, l'autore materiale dell'illecito agiva anonimamente.

In questa situazione, l'attenzione si è focalizzata sul provider in quanto unico soggetto reperibile nell'universo immateriale e magmatico della rete e dunque in grado di risarcire il danno.

È fin troppo evidente, come meglio sarà evidenziato, che in questa scelta abbia pesato, in maniera determinante, l'esigenza di non allocare gli effetti dell'illecito sul danneggiato[89].

Vi è anche un'altra ragione che ha indotto la giurisprudenza più risalente ad adottare tale soluzione.

Oltre alla migliore "reperibilità" rispetto agli utenti della rete, i providers sono soggetti economicamente più capienti. In altri termini, questi intermediari svolgono, in misura professionale ed imprenditoriale, la propria attività e detta attività, ovviamente, è remunerativa e comporta un arricchimento patrimoniale della posizione dell'intermediario a titolo diretto[90] o a titolo indiretto[91].

A fronte di questi dati, è apparso ragionevole ricondurre tale attività nell'alveo della teoria del rischio d'impresa, facendo applicazione del noto brocardo *cuius commoda eius et incommoda*[92].

---

[88] G.M. RICCIO, *La responsabilità civile degli Internet providers*, cit., p. 35.
[89] G.M. RICCIO, *op. cit.*, p. 36.
[90] Gli utenti pagano un canone fisso di abbonamento ai servizi offerti o una somma versata una *tantum* e commisurata all'entità delle controprestazioni.
[91] Il servizio è offerto gratuitamente agli utenti, ma il provider ottiene un guadagno, consentendo ad altre imprese di utilizzare detto servizio per scopi pubblicitari.
[92] G.M. RICCIO, *La responsabilità civile degli Internet providers*, cit., p. 37.

Il provider ottiene un vantaggio economico dall'esercizio della propria attività e di quella degli utenti e per tale ragione deve sopportare danni che da queste possono scaturire.

Non si possono tuttavia tacere i limiti che l'applicazione della teoria del rischio d'impresa, seppur ritenuta affascinante, reca in sé.

Due sono gli aspetti rispetto ai quali sono state avanzate delle perplessità.

Anzitutto, l'allocazione del rischio sugli esercenti le attività di fornitura di servizi telematici potrebbe comportare un aggravio dei costi in termini di predisposizione di sistemi protezione più efficienti, e quindi più onerosi, e di spese necessarie per sopportare un eventuale giudizio di responsabilità.

Di conseguenza, l'imposizione di una *strict liability* potrebbe determinare l'inevitabile aumento di prezzi dei servizi offerti e l'allocazione di questi sugli utenti dei servizi: "le imprese, per restare sul mercato, aumenterebbero i prezzi dei loro servizi, spostando i *costs of accidents* sugli utenti della rete"[93].

Una tale soluzione rischia di vanificare lo sviluppo delle fonti di informazione e di menomare la società di uno dei suoi beni più preziosi: l'informazione e la libertà di comunicazione.

Il rischio paventato che reca con sé tale teoria del rischio di impresa consiste nel fatto che essa determinerebbe "una concentrazione oligopolistica del mercato"[94].

Come afferma un'autorevole dottrina, è indubbio che "informazione e democrazia siano strettamente legate. Le pluralità delle fonti d'informazione, l'accessibilità ad esse, la controllabilità del loro contenuto costituiscono i connotatati di una società democraticamente organizzata"[95]. È altresì vero che "il diritto all'informazione, garantito dall'art. 21 Cost., implica indefettibilmente il pluralismo delle fonti e comporta per il legislatore il vincolo di emettere norme preordinate ad impedire la formazione di posizioni dominanti, che causano la riduzione dell'ambito della libertà di manifestazione del pensiero di coloro che sono privi delle condizioni tecniche ed economiche"[96].

Vi è però da rilevare che comunque queste libertà non possono non incontrare i limiti della tutela della libertà, dell'onore e della dignità dei soggetti che potrebbero essere lesi dalla

---

[93] G.M. RICCIO, *La responsabilità civile degli Internet providers*, cit., p. 38 ss.

[94] G.M. RICCIO, *op. cit.*, p. 40.

[95] P. STANZIONE, *Informazione, potere, contropotere: e le libertà del cittadino?*, in S. SICA-P. STANZIONE, *Informazione, verità e tutela della persona*, in *Quaderni del Dipartimento dei rapporti civili ed economici nei sistemi giuridici contemporanei dell'Università degli studi di Salern*o, 1997 p. 55 ss.

[96] V. ZENO ZENCOVICH, *Appunti sulla disciplina costituzionale delle telecomunicazioni*, in *Dir. inf.*, 1996, p. 400 ss. Corte cost., 7 dicembre 1994, n. 420, in *Foro amm*., 1994, p. 1667.

commissione di fatti illeciti telematici, visto che gli stessi hanno spesso delle conseguenze molto gravi sull'integrità psico-fisica dei danneggiati.

Oltre ai limiti evidenziati, connessi ad un'eventuale applicazione della teoria del rischio di impresa, si è ritenuto preferibile propendere per un regime colposo anche per altre ragioni.

In primo luogo, la responsabilità oggettiva sembra mal attagliarsi alle possibilità concrete dei prestatori di controllare le informazioni ed i dati che circolano nei siti e nei servizi da loro forniti.

La questione ha assunto particolare rilevanza sia nel modello francese sia in quello americano.

La prima posizione, in entrambi i casi, è stata quella di considerare i providers responsabili per non aver monitorato i siti e, quindi, per non aver né prevenuto né impedito la commissione dell'illecito.

Si è ritenuta tale ricostruzione viziata da una cattiva conoscenza del funzionamento dei servizi telematici. Prendiamo ad esempio il servizio di *hosting*. Il soggetto, che fruisce di una porzione dell'*hard disk* del computer del prestatore stesso, è in possesso di una password: attraverso di essa può accedere al sito, modificandone, in qualsiasi momento e senza l'ausilio del prestatore, i contenuti diffusi in rete.

Questo meccanismo opera anche nei forum di discussione, nelle *chatrooms*, nei *Bullettin Board Systems* e in tutti gli altri strumenti che consentono una comunicazione in tempo reale, via Internet, tra gli utenti[97].

Occorre altresì rilevare che gli illeciti compiuti con maggiore frequenza nel web (diffamazione, violazione della proprietà intellettuale, lesione del diritto di riservatezza…) realizzano la fattispecie dannosa nel momento stesso in cui il dato è diffuso. Una eventuale, successiva rimozione di questo materiale servirebbe solo a circoscrivere l'entità del danno, non ad evitarlo.

Atteso, quindi, che un controllo preventivo è difficilmente esigibile, potrebbe apparire corretto non imputare la verificazione del danno al provider a titolo di responsabilità oggettiva ma di responsabilità colposa, ipotizzando, dato il particolare tecnicismo che interessa l'attività svolta dal provider, soggetto dotato di competenze professionali specifiche, un'inversione dell'onere della prova a vantaggio dell'utente danneggiato.

[97] G.M. RICCIO, *La responsabilità civile degli Internet providers*, cit., p. 42 ss.

1.2 Vicarious liability e responsabilità per il fatto altrui

Piuttosto circoscritto è stato, nell'applicazione del formante giurisprudenziale, il ricorso alle ipotesi cosiddette speciali di responsabilità.

Al riguardo l'unico sistema nel quale si è assistito ad una elaborata ricostruzione è, ancora una volta, quello statunitense. In particolare, la giurisprudenza americana ha ammesso, in diverse occasioni, l'applicabilità della *vicarious liability* ai soggetti di Internet.

Lo scopo principale dovrebbe essere ricercato nell'intento di consentire al danneggiato di essere riparato dei danni subiti, anche nel caso in cui chi ne è autore non ha i mezzi finanziari per soddisfare la pretesa risarcitoria. In particolare, il ricorso alla *vicarious liability* consentirebbe di perseguire due scopi principali:

a) soddisfare un principio di giustizia: il *master* beneficia dell'attività del suo preposto; per contro, sopporta anche gli eventuali danni commessi da quest'ultimo;

b) perseguire finalità di prevenzione: il *master* è nella posizione ideale per sostituire i suoi collaboratori e/o per cambiare il metodo di lavoro (o di produzione), minimizzando *gli acts of negligence.*

Il primo presupposto affinché si abbia *vicarious liability* è che sussista un rapporto di preposizione tra *master* ed *employee* e che il danno sia stato commesso da quest'ultimo *in the corse of his employement*, ossia nello svolgimento delle funzioni a lui assegnate[98].

Sotto altra prospettiva, va detto che una cruciale importanza, nella dimostrazione del danno, deve essere ascritta al criterio finalistico: la *vicarious liability* dovrebbe, infatti, ricorrere nel solo caso in cui il *servant* agisca per la realizzazione di un interesse del preponente.

Alcuni di questi principi, per grandi linee, reggono anche le norme codicistiche dell'esperienza francese e di quella italiana.

L'art. 1242 *Code Civil* prevede l'obbligo di risarcire il danno non solo nel caso in cui questo costituisca effetto diretto della propria condotta ma anche qualora sia causato dalle persone delle quali si è responsabili.

È necessario che tra il *commettant* (ossia il preponente) ed il *préposé* (ossia il soggetto incaricato) sussista un rapporto di subordinazione, detto *lien de préposition*, che giustifica la nascita di un obbligo giuridico di *garde* in capo al committente. Anche in questo caso i presupposti necessari all'applicazione della norma sono, essenzialmente, riconducibili a

[98] Questo elemento, semplice da definire in astratto, si rivela, nell'applicazione pratica, dagli incerti contorni: ne è riprova, del resto, sia la copiosa produzione giurisprudenziale, sia l'ampio spazio dedicato a questo profilo dall'*American Law Institute*, in sede di redazione dei *Restatements*. G.M. RICCIO, *La responsabilità civile degli Internet providers*, cit., p. 45 ss.

detto rapporto: il danneggiante deve essere un dipendente e deve aver arrecato il danno nell'esercizio delle sue funzioni.

L'art. 1384 *Code Civil* costituisce l'antecedente normativo dell'art. 2049 c.c.

Anche in questo caso, infatti, la giurisprudenza, nell'interpretare e nell'applicare l'art. 2049 c.c., richiede che sussista un rapporto di preposizione tra l'autore materiale del danno ed il soggetto chiamato a rispondere e un nesso di occasionalità necessaria tra l'esercizio delle incombenze ed il danno al terzo.

Tale ultimo nesso è ritenuto sussistente non solo se il fatto dannoso derivi dall'esercizio delle incombenze ma anche nell'ipotesi in cui l'esercizio si limiti ad esporre il terzo all'ingerenza dannosa del preposto, anche se questi abbia abusato della sua posizione o agito per finalità diverse da quelle per le quali le incombenze gli erano state affidate.

Il nesso di occasionalità necessaria e la responsabilità del preponente sussistono nella misura in cui le funzioni esercitate abbiano determinato, agevolato o reso possibile oggettivamente la realizzazione del fatto lesivo, nel qual caso è irrilevante che il dipendente abbia superato i limiti delle mansioni affidategli o abbia agito con dolo per finalità strettamente personali; alla condizione che però la condotta del preposto costituisca pur sempre il non imprevedibile sviluppo dello scorretto esercizio delle mansioni, non potendo il proponente essere chiamato a rispondere di un'attività del preposto che non corrisponda, neppure quale degenerazione o eccesso, al normale sviluppo di sequenze di eventi connesso all'espletamento delle sue incombenze.

Non è prevista alcuna prova liberatoria e pertanto, si può pacificamente ritenere che si tratti di responsabilità oggettiva.

Il riferimento che la giurisprudenza e la dottrina talvolta hanno fatto alla *culpa in vigilando* o *in eligendo* è un retaggio oramai appartenente del passato.

La responsabilità per fatto altrui non sembra applicabile alle tipologie di providers esaminati. Non sussiste, infatti, tra i prestatori intermediari di Internet e gli utenti un nesso di occasionalità necessaria.

1.3 Ricorso alla responsabilità per i danni cagionati da cose in custodia

Qualche perplessità ha sollevato anche il tentativo di ricondurre la responsabilità del provider nell'alveo della responsabilità da cosa in custodia ex art. 2051 c.c.

Affinché possa configurarsi la responsabilità per danno cagionato da cosa in custodia è necessario che il danno sia causato dalla cosa in forza di un dinamismo connaturato o innescato da fattori esterni.

È pertanto fondamentale che, sebbene attivato da fattori esterni, il danno sia il frutto di un processo dinamico scaturente dalla cosa e che la cosa non sia mero strumento della condotta umana.

Per le cose statiche o inerti la giurisprudenza, ai fini dell'applicazione dell'art. 2051 c.c., richiede che lo stato dei luoghi presenti una situazione di oggettiva pericolosità tale da rendere molto probabile, se non inevitabile, il danno.

È indispensabile altresì che vi sia un rapporto di custodia, rapporto che implica il potere di controllare la cosa e di governarne i rischi insorti. Pertanto, si può pacificamente ritenere che il custode possa essere anche non proprietario.

La prova liberatoria coincide con la prova del caso fortuito, ossia di un fattore straordinario e oggettivamente imprevedibile, che ha spezzato il rapporto di causalità.

Se l'art. 2050 c.c. può essere considerato un testo critico, almeno nella sua scrittura, altrettanto non può dirsi degli artt. 2051 e 2052 c.c., che rappresentano invece "un modello di rilievo planetario, che il nostro legislatore ha verbalizzato sulla base di una felicissima comparazione trans-sistematica con la scienza giuridica francese"[99].

Un'autorevole dottrina tedesca[100] ha criticato la scelta del nostro legislatore di aver recepito, nell'art. 2050, il modello della *Gefährdungshaftung* proveniente dall'esperienza germanica pre ed extra codicistica[101] e, nell'art. 2051, il modello di responsabilità *du fait des choses* che si era affermato in Francia grazie alla consolidazione giurisprudenziale[102] delle teorie elaborate, alla fine dell'800, da Jesserand[103] e da Saleilles[104].

Bisogna riconoscere alla nostra scienza giuridica, però, il merito di aver contraddistinto la sfera di applicazione della regola enunciata dal 2051 c.c. sulla base dell'aspetto più o meno dinamico del prodursi del danno rispetto alla cosa[105], distinguendo attività e custodia come

---

[99] A. PROCIDA MIRABELLI DI LAURO, *Intelligenze artificiali e responsabilità civile*, in A. PROCIDA MIRABELLI DI LAURO-M. FEOLA, *Diritto delle obbligazioni*, Napoli, 2020, p. 539 ss. e *passim.*

[100] C. VON BAR, *Gemeineuropäisches Deliktsrecht*, I, München, 1999, p. 137 ss.

[101] Tale modello di responsabilità nasce ben prima del BGB e poi prolifererà al di fuori del codice. Si pensi alla legge prussiana del 3 novembre 1838 sui danni da esercizio dell'attività ferroviaria e alla *Haftpflichtgesetz* del 7 giugno 1871.

[102] Un ruolo essenziale avrà il secondo *arrêt Jand'heur* (Cass., Ch. Réun., 13 février 1930, in *Dalloz Pér.*, 1930, I, p. 57, con nota di G. RIPERT), in merito all'applicazione di tale regola alla responsabilità da circolazione di veicoli. Ma le prime decisioni che individuano un autonomo regime di responsabilità sono il celeberrimo *arrêt Teffaine* (Cass. civ., 18 juin 1896, in *Rec. Sirey*, 1897, 1, p. 17, con nota di A. ESMEIN, e in *Dalloz Pér.*, 1897, I, p. 433, con il commento di R. SALEILLES) e, ancor prima, due decisioni rese in tema di responsabilità dell'animale (Req., 23 décembre 1879, in *Rec. Sirey*, 1880, 1, p. 463 ; Cass., 27 octobre 1885, in *Dalloz Pér.*, 1886, I, p. 207).

[103] L. JOSSERAND, *De la responsabilité des choses inanimées*, Paris, 1897, *passim*.

[104] R. SALEILLES, *Les accidents de travail et la responsabilité civile*, Paris, 1897, *passim*.

[105] P.G. MONATERI, *La responsabilità civile*, in *Tratt. dir. civ.* diretto da R. Sacco, Torino, 1998, p. 1012.

fonti distinte di responsabilità[106], anche se talvolta le Corti hanno creato un vero e proprio «ircocervo», avendo forgiato «la categoria delle *cose pericolose*» e avendola riportata «nella sfera di applicazione dell'art. 2051»[107]. Ma, evidentemente, l'art. 2051 può riguardare qualsiasi tipo di cosa[108], mentre il dato della "pericolosità", cioè di una «potenzialità lesiva *di grado superiore al normale*»[109], rappresenta un dato "tipico" di qualificazione dell'attività di cui all'art. 2050, rilevando l'eventuale pericolosità della cosa soltanto ai fini dell'aggravamento della prova del caso fortuito, là dove implica, per sua natura, una maggiore prevedibilità, da parte del custode, delle possibili conseguenze dannose[110].

La responsabilità "*du fait des choses*" si pone come una vera e propria "creazione" della scienza giuridica francese, tant'è che gli stessi trattati di diritto comparato citano tale regola come «l'esempio più famoso» di un «prodigioso sviluppo giurisprudenziale, che ha esteso e completato, ma anche profondamente modificato e innovato, il sistema legale»[111].

Come magistralmente sostenuto[112], il nostro legislatore trasforma l'ultimo inciso dell'art. 1384, comma 1 *(«On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causi par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde»*), ancora una volta testualmente tradotto nell'art. 1153, comma 1, del c.c. del 1865[113], in una regola compiuta e ben scritta, completata dall'elemento essenziale della prova del fortuito, posta a carico del custode.

Rispetto all'art. 2043 c.c., come si è lucidamente affermato[114], negli artt. 2051 e 2052 c.c. si assiste non soltanto ad un'inversione dell'onere della prova, che dal danneggiante trasla verso il custode, ma anche al mutamento del suo oggetto: una prova inerente non più alla condotta più o meno diligente (o non colposa) del custode, ma al verificarsi di un fatto esterno, imprevedibile, inevitabile e irresistibile.

La causa incerta o ignota, evidentemente, grava sul custode.

---

[106] C. CASTRONOVO, *Responsabilità civile*, Milano, 2018, p. 469 ss.
[107] P.G. MONATERI, *La responsabilità civile*, cit., p. 1021 ss.
[108] Per la dottrina in tal senso, si rinvia a P. ZIVIZ, *Art. 2050. Responsabilità per l'esercizio di attività pericolose*, in *Comm. cod. civ*. diretto da P. Cendon, IV, 2, Torino, 1991, p. 2107.
[109] P.G. MONATERI, *La responsabilità civile*, cit., p. 1019 (il corsivo è dell'A.).
[110] M. FRANZONI, *Colpa presunta e responsabilità del debitore*, Padova, 1988, p. 172 ss.
[111] Per tutti, L.-J. CONSTANTINESCO, *Il metodo comparativo*, ed.it. di A. Procida Mirabelli di Lauro, Torino, 2000, p. 147 ss.
[112] A. PROCIDA MIRABELLI DI LAURO, *Intelligenze artificiali e responsabilità civile*, cit., p. 541.
[113] Infatti, l'art. 1153, comma 1, del cod. civ. del 1865 così recita: «Ciascuno parimente è obbligato non solo pel danno che cagiona per fatto proprio, ma anche per quello che viene arrecato col fatto delle persone delle quali deve rispondere, o colle cose che ha in custodia».
[114] M. FEOLA, *Le obbligazioni di sécurité*, Torino, 2012, p. 370 ss. e *passim*.

Anche il fatto del terzo e del danneggiato, per assumere rilievo ai fini dell'esonero totale o parziale dalla responsabilità, devono rivestire quei caratteri di autonomia, imprevedibilità e inevitabilità che sono propri del caso fortuito[115].

Come a buon diritto si afferma in una recente sentenza della Cassazione[116] che, nel confermare un orientamento ormai consolidato, cassa la decisione della Corte d'appello di Milano che aveva individuato il fortuito nella sola condotta "negligente" della vittima, il "fatto della vittima", per integrare gli estremi del fortuito e, quindi, per escludere la responsabilità del custode, deve essere non soltanto colposo, ma anche imprevedibile. Se il primo giudizio va compiuto «guardando al danneggiato, e comparando la condotta da questi concretamente tenuta con quella che avrebbe tenuto una persona di normale avvedutezza, secondo lo schema di cui all'art. 1176 c.c.», il secondo va espresso «invece guardando al custode, e valutando con giudizio *ex ante* se questi potesse ragionevolmente attendersi una condotta negligente da parte dell'utente» che fosse imprevedibile, cioè «eccezionale, inconsueta, mai avvenuta prima, inattesa da una persona sensata»[117].

Al caso fortuito, che «per la nostra legge è quell'evento che non poteva essere previsto (ad esempio, un terremoto)», va «equiparata la forza maggiore, ovvero l'evento che, pur prevedibile, non può essere evitato (ad esempio, un evento atmosferico)»[118].

Da qui la massima standard secondo la quale la responsabilità per i danni cagionati da cose in custodia «ha carattere oggettivo e perché possa configurarsi in concreto è sufficiente che sussista il nesso causale tra la cosa in custodia ed il danno arrecato, senza che rilevi al riguardo la condotta del custode o l'osservanza o meno di un obbligo di vigilanza», essendo «funzione della norma [...] quella di imputare la responsabilità a chi si trova nelle condizioni di controllare i rischi inerenti alla cosa»[119]. Irrilevante, ai fini della prova del nesso causale, è la pericolosità attuale o potenziale degli oggetti e della condotta[120] del custode.

Il fortuito «è qualificazione incidente sul nesso causale e non sull'elemento psicologico dell'illecito», quale «fattore riconducibile a un elemento esterno, avente i caratteri

---

[115] Per le citazioni di un orientamento giurisprudenziale ormai consolidato si rinvia a P. ZIVIZ, *Art. 2050.*, cit., p. 2116 ss.; P.G. MONATERI, *La responsabilità civile*, cit., p. 1058 ss.

[116] Cass., Sez. III, 31 ottobre 2017, n. 25837, in *Danno e resp.*, 2018, p. 195 ss., con nota di V. CARBONE, *Danno da cosa in custodia: il caso fortuito richiede una condotta imprudente e imprevedibile della vittima*.

[117] Cass., 31 ottobre 2017, n. 25837, cit., p. 196.

[118] Cass., 31 ottobre 2017, n. 25837, in A. PROCIDA MIRABELLI DI LAURO, *Intelligenze artificiali e responsabilità civile*, op. cit., p. 542.

[119] Per tutte, Cass., Sez. III, 8 febbraio 2012, n. 1769, in *Danno e resp*., 2012, p. 756.

[120] Cass., 8 febbraio 2012, n. 1769, cit., p. 757.

dell'imprevedibilità e dell'inevitabilità»[121]. Tant'è che «il custode negligente non risponde in modo diverso dal custode perito e prudente, se la cosa ha provocato danni a terzi»[122].

Proprio quel carattere di «*dinamismo* interno connaturato alla cosa»[123], di «dinamismo intrinseco» di una cosa dotata di «energia interna», ben sottolineato dalla nostra giurisprudenza – sulla scia di quella francese[124] – pur sulla base di un linguaggio definito come animistico[125], fa sì che l'art. 2051 c.c. si riveli una regola chiara, utilizzabile per regolare anche le più recenti ipotesi di responsabilità delle intelligenze artificiali[126].

Sebbene l'art. 2051 sia una disposizione legislativa chiara, mal si attaglia alla responsabilità dell'intermediario informatico.

È stato dimostrato, infatti, come un controllo da parte degli operatori telematici sui dati che circolano nei loro server non sia ipotizzabile: ad ogni modo, oggetto del controllo dovrebbe comunque essere il comportamento di altra persona e non il mezzo.

La rete Internet - come ogni altro strumento di comunicazione - autonomamente non può arrecare danni a terzi: è sempre l'utilizzazione fattane da una persona fisica a determinare la lesione.

Allo stesso modo, il provider fornisce un servizio: il bene - ossia la pagina web o il forum di discussione - sfugge alla sua disponibilità.

Nei confronti di esso il prestatore non è titolare né di una situazione di possesso, né di detenzione, né di altra posizione di natura dominicale.

In definitiva, è stato sostenuto che il ricorso a questa forma di responsabilità appare difficile per due ragioni determinanti:

a) non è il bene ad arrecare la lesione, ma esso è solo il mezzo attraverso il quale la stessa si produce;

b) non sussiste un rapporto di locazione tra content ed host provider, ma di fornitura di un servizio. La discussione relativa a questa forma di responsabilità è, tuttavia, solo ipotetica,

---

[121] Cass., 19 maggio 2011, n. 11016, in *Danno e resp.*, 2012, p. 28.

[122] Cass., 19 maggio 2011, n. 11016, cit., p. 28.

[123] Già Cass., 22 gennaio 1980, n. 520, in *Giust. civ.*, 1980, I, p. 838. Per la costante giurisprudenza in tal senso, cfr. P. ZIVIZ, *Art. 2050.*, cit., p. 2108; P.G. MONATERI, *La responsabilità civile*, cit., p. 1039.

[124] La svolta, in Francia, si avrà con il celebre *arrêt Jand'heur* (Cass., Ch. Réun., 13 février 1930, cit., p. 57), sul quale L. JOSSERAND, *La responsabilité du fait des automobiles devant les Chambres réunies de la Cour de Cassation*, in *Dalloz Hebd.*, 1930, *Chron.*, p. 25; H. CAPITANT, *La responsabilité du fait des choses inanimées après l'arrêt des Chambres réunies du 13 févr. 1930*, *ivi*, 1930, p. 29.

[125] Così P.G. MONATERI, *La responsabilità civile*, cit., pp. 1013 e 1041.

[126] Più idonea a disciplinare quel rapporto tra *principal* e agente *software* autonomo che Gunther Teubner molto efficacemente descrive, ma che poi propone di regolare attraverso il riconoscimento di una soggettività giuridica parziale, anche perché il diritto tedesco non conosce una norma analoga a quella iscritta nell'art. 2051 c.c. Sul punto, cfr. A. PROCIDA MIRABELLI DI LAURO, *Intelligenze artificiali e responsabilità civile*, cit., pp. 542 e 543.

atteso che in nessun caso la giurisprudenza ha fatto ricorso a questa figura per determinare la responsabilità dei prestatori[127].

È dubbio che l'intermediario possa essere qualificato come custode, essendo molto discutibile l'esistenza di un potere di governo sulla casa e comunque non sembra che la porzione di disco, utilizzata dall'utente per commettere l'illecito, sia idonea a nocumento, così come è richiesto ai fini dell'affermazione della responsabilità.

È un'occasione per produrre il danno più che la causa dello stesso[128].

1.4 Ricorso alla responsabilità per esercizio di attività pericolosa

Come autorevole dottrina ha brillantemente sostenuto, la regola iscritta nell'art. 2050 c.c. può essere considerata come una delle più ambigue del nostro codice, soprattutto per quella esplicita volontà, che emerge con chiarezza nella Relazione al codice, n. 795, di adottare una soluzione intermedia tra colpa e responsabilità oggettiva [129].

Tale intento risulta chiaramente dall'equivoco enunciato che, da un lato, invertendo l'onere della prova (rispetto all'art. 2043 c.c.), fa gravare sull'esercente la prova di «aver adottato tutte le misure idonee a evitare il danno»; dall'altro, dispone una prova liberatoria imperniata comunque sul comportamento dell'esercente[130].

Tuttavia, poiché "tra colpa e responsabilità oggettiva *tertium non datur"*[131], la scienza giuridica italiana ha superato i più vetusti orientamenti volti ad individuare nell'art. 2050 c.c. una responsabilità «vincolata alla colpa, seppure presunta e rilevante anche se di tenuissima entità», riconducendo tale modello alla responsabilità oggettiva per rischio oggettivamente evitabile e considerandolo quale criterio di collegamento tipico e autonomo rispetto alla colpa.

L'esercente risponde, anche in assenza di una condotta illecita, per il fatto di aver posto in essere una serie di condizioni obiettive atte, nella loro globalità, a generare situazioni con elevata potenzialità di danno.

Malgrado il legislatore si sia sforzato di trovare una soluzione intermedia tra la colpa e il principio della pura causalità, considerato anzi «ingiusto, antisociale e antieconomico, e tale da scoraggiare attività e iniziative feconde» (Rel. n. 795), la costante interpretazione giurisprudenziale, attraverso l'utilizzo di un meccanismo «di aggravamento sostanziale

[127] G.M. RICCIO, *La responsabilità civile degli Internet providers*, cit., pp. 51 e 52.
[128] M. DE CATA, *La responsabilità civile dell'Internet service provider*, cit., p. 55.
[129] A. PROCIDA MIRABELLI DI LAURO, *Intelligenze artificiali e responsabilità civile*, cit., p. 536 ss.
[130] M. FRANZONI, *Il danno da attività pericolose nella giurisprudenza*, in *Contr. e impr.*, 1985, p. 155 ss.
[131] P. TRIMARCHI, *Rischio e responsabilità oggettiva*, Milano, 1961, p. 276.

(tutte le misure idonee) e processuale (l'inversione) dell'onere della prova», determinerà un importante risultato «sul piano sostanziale, trasformando una regola di responsabilità emersa nell'arcipelago della colpa in una regola di responsabilità oggettiva»[132].

Anche là dove la giurisprudenza si fa premura di riesumare la figura della "colpa presunta", o considera l'art. 2050 c.c. (a differenza dell'art. 2051 c.c.) come «un'ipotesi di responsabilità soggettiva», nella sostanza «applica un vero standard di responsabilità oggettiva, finendo per richiedere come liberatoria la sola interruzione del nesso causale, anche perché in svariate ipotesi il realizzarsi del danno viene assunto dai giudici come prova dell'insufficienza delle misure adottate».

Oltre ai fatti del terzo o del danneggiato, l'esonero dalla responsabilità interviene normalmente con la prova del caso fortuito, cioè di una «causa estranea non imputabile alla sfera giuridica dell'esercente».

Risulta incompatibile con la qualificazione di "attività pericolosa" l'eccezione del c.d. rischio da sviluppo, prevista invece dalla disciplina sulla responsabilità da prodotto difettoso, con la conseguenza che non può andare esente «da responsabilità chi immetta in circolazione una *res periculosa* per il fatto che, al momento dell'immissione, non era possibile, in base allo stato più avanzato delle conoscenze scientifiche, individuare il difetto che ha causato il danno»[133].

La nozione di cosa pericolosa prescinde dalla sua eventuale difettosità, essendo la responsabilità di cui all'art. 2050 c.c. interamente fondata sull'idea di esposizione al pericolo, non su quella di difetto di un prodotto che si presume, ex ante, come sicuro.

Rispetto all'esperienza tedesca[134], che pur individua nella *Gefährdungshaftung* una responsabilità oggettiva da pericolo, senza illiceità (*Rechtswidrigkeit*) né colpevolezza (*Verschulden*), quindi una responsabilità da atto lecito dannoso, il nostro codice ha il vantaggio di prevedere una clausola generale che, per essere applicata, non richiede ulteriori e specifici interventi legislativi.

Oltre ai consueti settori nei quali la giurisprudenza ha individuato la sussistenza di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati (nelle attività sanitarie e farmaceutiche, nelle attività sportive e venatorie, nelle attività di trasporto, nell'edilizia e nei lavori stradali, nella produzione e somministrazione di energia elettrica, nell'erogazione di

---

[132] A. PROCIDA MIRABELLI DI LAURO, *Intelligenze artificiali e responsabilità civile*, cit., p. 537 ss.
[133] A. PROCIDA MIRABELLI DI LAURO, *op. cit.*, p. 538.
[134] G. TEUBNER, *Soggetti giuridici digitali? Sullo* status *privatistico degli agenti* software *autonomi*, a cura di P. Femia, Napoli, 2019, p. 19 ss.

gas e carburanti, nella produzione e distribuzione di tabacchi lavorati, persino nella gestione di determinate attività ricreative ecc.), estremo rilievo assume, con riferimento al tema indagato, il rinvio all'art. 2050 c.c. contenuto nell'art. 15 del d.lgs. 30 giugno 2002, n. 196 in tema di trattamento dei dati personali (poi modificato dal d.lgs. n. 101 del 2018)[135].

Malgrado il legislatore della codificazione abbia riferito tale regola alla «pericolosità della tecnologia che opera nel mondo materiale non a quella che dà vita alla realtà virtuale, ancora fuori dalla portata dell'immaginazione del legislatore», da tale disciplina «finisce con l'emergere una interpretazione autentica dell'art. 2050, nella quale viene detto che la regola in esso contenuta, sinora applicata soltanto alle attività di pericolosità materiale, va estesa anche alle attività pericolose della realtà virtuale»[136].

Tanto il formante dottrinale quanto quello giudiziale non hanno mai pensato di poter applicare la regola di cui all'art. 2050 c.c. La prassi operazionale denota, infatti, una serie impensabile di attività ritenute pericolose.

Secondo una parte della dottrina, la pericolosità potenziale deve essere dimostrata secondo un metodo prognostico: un'attività, in definitiva, è pericolosa «quando statisticamente cagiona molti incidenti e quando minaccia di cagionarne di molto gravi».

Le attività svolte dai providers, statisticamente, non sono idonee a determinare frequentemente danni: lo dimostra il numero ingente dei siti Internet e, per contro, l'esiguità delle pronunce giurisprudenziali. Potrebbe obiettarsi che il numero limitato delle decisioni non coincide, effettivamente, con il numero delle lesioni realizzate attraverso la rete.

La non eccessiva pericolosità - sotto il profilo quantitativo sia degli illeciti commessi, sia dell'ammontare dei danni arrecati - porta, in definitiva, una parte della dottrina ad escludere

---

[135] In argomento, v. S. SICA, *Commento* sub *art. 18*, in E. GIANNANTONIO-M.G. LOSANO-V. ZENO-ZENCOVICH, *La tutela dei dati personali. Commentario alla l. 675/96*, Padova,1997, p. 176 ss.; M. FRANZONI, *Dati personali e responsabilità civile*, in *Resp. civ. prev.*,1998, p. 902 ss.; G. COMANDÈ, *Danni cagionati per effetto del trattamento dei dati personali*, in F.D. BUSNELLI-C.M. BIANCA, *Tutela della privacy*, in *Nuove leggi civ. comm.*, 1999, p. 482 ss.; F. D. BUSNELLI, *Il «trattamento dei dati personali» nella vicenda dei diritti della persona: la tutela risarcitoria*, in V. CUFFARO-V. RICCIUTO-V. ZENO-ZENCOVICH, *Trattamento dei dati e tutela della persona*, Milano, 1998, p. 177 ss.; G. ALPA, *La normativa sui dati personali. Modelli di lettura e problemi esegetici, in Dir. inf.*, 1997, p. 703 ss.; D. CARUSI, *La responsabilità*, in V. CUFFARO-V. RICCIUTO, *Il trattamento dei dati personali*, 2ª ed., Torino, 1999, p. 356 ss.; R. CLARIZIA, *Legge 675/96 e responsabilità civile*, in *Dir. inf.*, 1998, p. 235 ss.; G. BUTTARELLI, *Banche dati e tutela della riservatezza*, Milano, 1997, p. 350 ss.; M. BIN, *Privacy e trattamento dei dati personali*, in *Contr. e impr.*, 1997, p. 459 ss.; E. GIANNANTONIO, *Responsabilità civile e trattamento dei dati personali*, in *Dir. inf.*, 1999, p. 1035 ss.; C. PULIGHEDDU, *Trattamento dei dati personali e responsabilità da esercizio di attività pericolose*, in *Resp. com. impr.*, 1998, p. 445 ss.; V. ROPPO, *La responsabilità civile per trattamento di dati personali*, in *Danno e resp.*, 1997, p. 660 ss.

[136] C. CASTRONOVO, *Responsabilità civile*, cit., p. 464 ss. Per una trattazione diffusa sul punto, v. A. PROCIDA MIRABELLI DI LAURO, *Intelligenze artificiali e responsabilità civile*, cit., p. 539 ss.

l'applicazione della responsabilità per esercizio di attività pericolose ai soggetti di Internet[137].

Dunque, sebbene i danni prodotti dagli illeciti on line siano di gran lunga rilevanti, l'attività del provider non può essere considerata pericolosa[138].

1.5 Approdo al criterio di imputazione a carattere colposo

Scartate le ipotesi cc.dd. speciali di responsabilità, appare preferibile propendere per un criterio di imputazione a carattere colposo. Questa è stata la scelta delle diverse legislazioni nazionali: *Digital Millennium Copyright Act* negli Stati Uniti, *Teledienstegesetz* in Germania, legge n. 217 del 2000 in Francia.

Nello stesso senso si è mosso il legislatore comunitario con la direttiva n. 31 del 2000.

Questa soluzione, prima ancora che vi approdasse il formante legislativo, era già emersa in alcune sentenze statunitensi in materia di violazione del copyright.

In particolare, in questi casi, si era fatto ricorso alla figura del *contributory infrigement*[139].

Secondo le regole di Common law, si ha questa forma di responsabilità nel caso in cui un soggetto (*secondarily liable*) induca, causi o contribuisca materialmente alla commissione di un illecito da parte di un altro soggetto (*directly liable*).

Pertanto, questa figura ricorre allorquando sussiste una violazione "diretta" cui si aggiunge, poi, una condotta che solo indirettamente, aiuta a realizzare l'illecito (a titolo, appunto, di mera contribuzione).

Essenzialmente, possono aversi due forme di condotta: nella prima, il soggetto agevola l'autore materiale dell'illecito, assistendo o coadiuvando la sua azione; nell'altra, invece, si limita a fornire il mezzo o lo strumento tecnico con cui realizzare la violazione[140].

In quest'ultimo caso, inoltre, è necessario che il soggetto che distribuisce il prodotto sia a conoscenza dell'illiceità del comportamento del *directly liable*.

Le Corti, generalmente, fanno ricorso al concetto di *actual knowledge*, che ricorrerebbe quando il soggetto conosce o dovrebbe conoscere che la sua attività è strumentale rispetto alla commissione di una determinata violazione.

---

[137] G.M. RICCIO, *La responsabilità civile degli Internet providers*, cit., p. 52 ss.
[138] M. DE CATA, *La responsabilità civile dell'Internet service provider*, cit., p. 60 ss.
[139] G.M. RICCIO, *La responsabilità civile degli Internet providers*, cit., p. 57 ss.
[140] G.M. RICCIO, *op. cit.*, p. 60 ss.

In alcuni casi, invece, la giurisprudenza ha preferito far riferimento alla c.d. *constructive knowledge*, che si verifica allorquando un soggetto venda, produca o fornisca l'accesso a mezzi che possono facilitare la commissione di atti illeciti.

La determinazione del *level of knowledge* ha rappresentato, probabilmente, la problematica maggiore nell'applicazione di questa *doctrine* nei confronti dei prestatori intermediari della rete.

Infatti, non può dubitarsi che i providers, consentendo l'accesso alla rete e fornendo il servizio di hosting, offrano lo strumento per realizzare il danno: è discutibile, invece, che essi siano effettivamente a conoscenza delle azioni compiute dagli utenti della rete.

I dubbi sollevati dall'applicazione della teoria della *contributory negligence* sono stati, in parte, risolti dall'emanazione del *Digital Millennium Copyright Act*, che ha "codificato" le ipotesi nelle quali il provider non può essere considerato responsabile.

La stessa soluzione, pedissequamente, è stata recepita anche dal legislatore comunitario, che, sulla scia dell'esempio statunitense, ha fissato uno standard di diligenza, rispettando il quale il prestatore intermediario è esente da qualsiasi responsabilità.

Non deve, però concludersi che, sulla scorta delle argomentazioni finora prospettate, il ricorso al criterio di imputazione colposo avvenga, per dir così, de residuo, dopo aver scartato le altre ipotesi di responsabilità.

L'applicazione del principio colposo, infatti, è stata ritenuta idonea a contemperare le esigenze di *compensation* dei danneggiati con le pretese dei prestatori intermediari: questi ultimi, infatti, non saranno chiamati a risarcire, aprioristicamente, tutti i danni, ma solo quelli la cui commissione è stata agevolata dalla loro condotta.

Appare di immediata evidenza che il danneggiato non è e non deve essere una vittima che può essere sacrificato sull'altare dei bisogni sociali[141].

Occorre ricercare una via mediana tra posizioni estreme: quella che vuole il provider non responsabile in ogni caso e quella che viceversa ritiene che il danno debba essere riparato sempre da questo soggetto.

La ricerca di questo equilibrio passa per un criterio di imputazione a carattere colposo, garantendo alla vittima il risarcimento e consentendo ai provider di rispondere dei danni nei soli casi in cui la loro condotta di discosti da quello standard di diligenza[142].

L'imposizione di uno standard di diligenza è in grado di contemperare le aspettative degli utenti della rete e quelle dei prestatori intermediari.

---

[141] G.P. FLETCHER, *Fairness and Utility in Tort Theory*, in *84 Harv. L. Rev*., 1972, p. 537 ss.
[142] G.M. RICCIO, *La responsabilità civile degli Internet providers*, cit., p. 64 ss.

L'applicazione di un livello di diligenza ragionevole, che dovrebbe comportare l'adozione preventiva di misure atte ad evitare la verificazione di eventi dannosi o quanto meno a limitarne la possibilità di realizzazione.
In più, comporterebbe un intervento successivo alla commissione dell'illecito da parte degli utilizzatori dei servizi telematici, volto ad impedire la prosecuzione e/o la reiterazione della condotta lesiva attraverso la chiusura del servizio o la rimozione delle informazioni illecite.
Se negli anni passata la conoscenza più acerba delle reti telematiche e delle attività degli internauti rendeva certamente giustificabili tali orientamenti e potevano essere ammessi dubbi sulle effettive possibilità di responsabilizzazione degli intermediari informatici, oggi l'evoluzione tecnologica cambia lo scenario e attualmente non sembra potersi immaginare niente di diverso rispetto alla responsabilizzazione dei provider.
Potrebbe apparire corretto non imputare la verificazione del danno al provider a titolo di responsabilità oggettiva ma di responsabilità colposa, ipotizzando, dato il particolare tecnicismo che interessa l'attività svolta dal provider, soggetto dotato di competenze professionali specifiche, un'inversione dell'onere della prova a vantaggio dell'utente danneggiato.
Queste problematiche si manifestano anche in altri ordinamenti, dalla cui esperienza in tema di responsabilità del provider non si può prescindere.

2. La responsabilità civile degli intermediari della rete nel sistema americano

Nell'ottica di un approccio comparatistico, il primo modello che viene in considerazione non può che essere quello americano.
Gli USA, infatti, non detengono solo il primato della diffusione di Internet e dello sviluppo del commercio elettronico ma anche quello di avere individuato precocemente ed in termini chiari la questione della responsabilità del provider che, prima a livello giurisprudenziale e poi a livello legislativo, è stata risolta nell'arco concentrato di alcuni anni[143].
Il regime di responsabilità europeo previsto per le piattaforme online che offrono servizi di *hosting* - come quello per chi fornisce servizi di accesso alla rete e di memorizzazione temporanea – è stato profondamente influenzato dal sistema statunitense[144].
I due plessi normativi posti a regolamentazione delle responsabilità degli intermediari della rete rinvenibili nel diritto federale statunitense, il *Communications Decency Act* (CDA) ed

[143] M. DE CATA, *La responsabilità civile dell'Internet service provider*, cit., p. 100 ss.
[144] L. NIVARRA, *Internet e responsabilità extracontrattuale*, in A. PALAZZO-U. RUFFOLO, *La tutela del navigatore in Internet*, Milano, 2002, p. 204 ss.

il *Digital Millennium Copyright Act* (DMCA), approvati nello stretto giro temporale del biennio 1996-1998, sono stati scelti come parametro di riferimento per la legislazione posta a contemperamento del conflitto di interessi tra titolari dei diritti d'autore e prestatori dei servizi della rete.

Lo sviluppo dell'iter giurisprudenziale e normativo, per quanto relativamente breve, non è stato tuttavia lineare, anche a causa delle scelte dei singoli Stati, non sempre in armonia con quelle del legislatore federale, ma ha avuto certamente il pregio di avere evidenziato rapidamente e chiaramente le questioni sottese alla problematica della responsabilità del provider e di avere raggiunto soluzioni che, a prescindere dalla loro esportabilità in altri Paesi, costituiscono in generale, nel quadro dei principi e valori fondamentali dell'ordinamento statunitense, e sia pure con taluni eccessi, un ragionevole bilanciamento degli interessi coinvolti[145].

Il legislatore statunitense con il *Communications Decency Act* del 1996, primo formante normativo in materia, ha inaugurato un regime di particolare favore per gli intermediari della rete telematica, individuando una tutela che ruota attorno a due pilastri fondamentali.

Il comma primo della sezione 230, rubricata "*Treatment of publisher or speaker"*, stabilisce che tanto il provider quanto l'utente di servizio informatico interattivo non verranno considerati *publisher* o *speaker* di qualsivoglia informazione fornita da un *information content provider*.

Il comma secondo della medesima sezione estende il regime di favore anche a vantaggio di quei prestatori che operano una cernita dei contenuti multimediali diffusi sugli spazi digitali[146].

Si tratta di una legge che senza dubbio ha come obiettivo primario la protezione massima della libertà di espressione in Internet, al punto tale che alcuni l'hanno definita come una "vera e propria Magna Carta dell'impunità d'impresa"[147].

L'approdo alla sezione 230 CDA è stato fortemente influenzato dalle prime pronunce oscillanti della giurisprudenza che si sono trovate a dover applicare la *law of defamation* alle fattispecie sottoposte al suo vaglio.

---

[145] A. C. YEN, *Internet Service Provider Liability for Subscriber Copyright Infringement Enterprise Liability and the First Amendment*, in *Georgetown Law Journal*, 2002, p. 1 ss.

[146] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. 2 ss.

[147] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. 3, richiama F. PASQUALE, *Platform Neutrality: Enchancing Freedom of Expression in Spheres of Private Power*, in *17 Theoretical Inquiries L.*, 2016, p. 494.

Il riferimento è ai casi *Cubby vs Compuserve*[148] e *Stratton-Oakmont vs Prodigy*.

Le Corti statunitensi sono state poste dinanzi al quesito circa la possibilità di applicare agli illeciti diffamatori consumatisi in rete i principi di diritto comune riguardanti i classici mezzi di comunicazione ovvero circa la necessità di mettere a punto un vero e proprio circuito separato di regole, che ben si attagliasse alle peculiarità delle comunicazioni dell'era digitale.

Qualora si fosse voluta percorrere la prima strada si sarebbe dovuto decidere come qualificare il comportamento attivo o omissivo del convenuto che non fosse l'autore diretto delle dichiarazioni diffamatorie.

La *law of defamation* offriva all'interprete una classificazione tripartita: l'intermediario avrebbe potuto essere inteso come *publisher*, *distributor* o semplice *common carrier.*

L'inquadramento in una delle summentovate categorie è un'operazione molto delicata perché a ciascuna di esse è ricollegato un diverso regime giuridico, sulla base del grado di compartecipazione al fatto illecito altrui.

Il *common carrier*, non essendo in grado di esercitare alcuna forma di controllo, non risponde civilmente delle informazioni trasmesse; il *distributor* è tenuto a risarcire i danni cagionati a terzi sulla base della "*knowledge standard*" e dunque deve essere consapevole, o comunque avrebbe dovuto esserlo ragionevolmente, della natura diffamatoria delle opere divulgate.

Infine, il *publisher*, esercitando il controllo editoriale, è il destinatario del regime più rigoroso di responsabilità oggettiva (*strict liability*).

Il "banco di prova" della responsabilità civile dei providers è stato rappresentato dai casi di diffamazione telematica.

Nei modelli di Common law la *defamation* rappresenta una figura tipica di *tort*, il cui fine è quello di proteggere l'onore e la reputazione dei singoli.

La prima macroscopica differenza tra i modelli di Civil law e di Common law è data dal fatto che nel primo caso la diffamazione costituisce un illecito penale, risarcibile in sede civile, nel secondo caso, invece, essa rientra a pieno titolo nel capitolo dei *torts* e rileva esclusivamente quale illecito civile.

Il *tort of defamation* può essere scisso in due sottocategorie: il *libel* e lo *slander*.

La differenza tra le due figure si fonda sul mezzo utilizzato per propagare la diffamazione.

[148] M. GODWIN, *Internet libel: is the provider responsible?* in *www.eff.or.*

Il *libel* ricorre quando l'informazione è diffusa in forma "duratura" (ad es., scritti, disegni, riproduzioni filmografie, ecc.), lo *slander* quando il mezzo utilizzato ha natura "transitoria" (parole, gesti, ecc.). Nelle reti telematiche possono realizzarsi entrambe le fattispecie.

La prima controversia in cui è stata sollevata la questione della responsabilità del provider riguardava infatti un caso di lesione dell'onore e della reputazione, in particolare si trattava di messaggi diffamatori immessi in Rete dagli users.

La prima pronuncia (*Cubby vs Compuserve*) è stata una decisione giudiziaria del 1991 della Corte Distrettuale degli Stati Uniti (per il Distretto Meridionale di New York).

Questa ha stabilito che i fornitori di servizi Internet possono essere soggetti alla legge tradizionale sulla diffamazione per i contenuti ospitati ma sulla base del regime di responsabilità del *distributor*.

Il caso ha risolto una denuncia per diffamazione contro *CompuServe* , un provider di servizi Internet che ospitava contenuti presumibilmente diffamatori in uno dei suoi forum, applicando al mezzo Internet la legge sulla diffamazione, originariamente destinato alle copie cartacee di opere scritte.

Nel caso di specie, all'interno di *Bulletin Board System*, erano diffusi alcuni messaggi tendenti a gettare discredito nei confronti della società Cubby.

La Corte ha ritenuto che, sebbene Compuserve ospitasse contenuti diffamatori sui suoi forum, questi era semplicemente un distributore, piuttosto che un editore, del contenuto. In qualità di distributore, Compuserve potrebbe essere ritenuto responsabile per diffamazione solo se fosse a conoscenza, o avesse motivo di sapere, della natura diffamatoria del contenuto.

Poiché Compuserve non ha fatto alcuno sforzo per esaminare l'ampio volume di contenuti sui suoi forum, non può essere ritenuto responsabile per il contenuto diffamatorio[149].

Dunque, solo il *knowledge standard* alla base del regime di responsabilità del *distributor* è stato ritenuto compatibile con il Primo Emendamento alla Costituzione degli Stati Uniti d'America, che tutela al massimo grado la libertà di parola o di stampa[150].

Questo primo approdo, incentivando la fruizione delle informazioni del nuovo mezzo comunicativo, nasce dall'esigenza di evitare che una responsabilità oggettiva troppo rigorosa potesse avere l'effetto di inibire questo meccanismo.

---

[149] *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991).

[150] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. 6.

Come sul *distributor* non ricade un dovere generale di controllo sulla non illiceità delle informazioni contenute nei periodici distribuiti, al pari l'intermediario può astenersi dall'attività di accertamento della legittimità dei contenuti trasmessi.

L'analogia con il *publisher* è stata esclusa proprio sulla base del rilievo dell'impossibilità per il provider di effettuare il controllo preventivo sul materiale immesso dagli users[151].

Qualche anno dopo la *Supreme Court* di New York cambia registro argomentativo e, nell'applicare la *law of defamation,* approda ad una soluzione opposta rispetto a quella individuata in *Cubby vs Compuserve.*

Si tratta di una decisione della Corte Suprema di New York del 1995, la quale ha stabilito che i fornitori di servizi online possono essere ritenuti responsabili per il fatto dei loro utenti. Infatti, l'intermediario è apparso qualificabile come *publisher*, con la conseguente applicazione del severo regime di responsabilità oggettiva, perché ha trovato corso l'idea che il prestatore informatico potesse monitorare le trasmissioni" e dunque in qualche modo operare sui contenuti ammissibili sulla propria piattaforma[152].

Il risultato del caso è stato fondamentale perché ha costituito, date anche le proteste degli intermediari, la base per la motivazione dell'approvazione della Sezione 230 *del Communications Decency Act* del 1996, volta a consentire ai fornitori di servizi Internet di evitare la responsabilità per i contenuti degli utenti sui loro servizi, pur fornendo loro i mezzi per rimuovere i contenuti illegali.

Negli stessi lavori preparatori alla legge è stato chiarito che uno degli scopi specifici della sezione 230 CDA fosse quello di abrogare *Stratton-Oakmont vs Prodigy* e qualsiasi altra decisione avesse considerato il provider alla stregua di un editore o di un autore dei contenuti immessi dagli utenti.

È stato infatti espressamente chiarito che se "gli sforzi volti a riesaminare o estromettere dalle piattaforme informatiche contenuti inappropriati immessi da terzi dovessero rendere l'intermediario civilmente responsabile per le informazioni pubblicate, allora gli operatori dei siti web e fornitori di servizi Internet abdicherebbero a tali compiti"[153].

"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider": queste le

[151] O. BRAUN, *Internet Publications and Defamation: Why the Single Publication Rule Should Not Apply*, in *Golden Gate U.L. Rev.*, 2002, p. 325 ss.

[152] *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 23 Media L. Rep. 1794 (NY Sup. Ct. 1995).

[153] H.R. Conf. Rep. No. 104-458, 194 (1996). Cfr. R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., pp. 8 e 9.

ventisei parole della sezione 230 CDA che dettano le regola di (ir)responsabilità del provider.

Le protezioni della Sezione 230 non sono illimitate e richiedono ai fornitori di rimuovere materiale illegale a livello federale, come nei casi di violazione del copyright.

Il passaggio e la successiva storia giuridica a sostegno della costituzionalità della Sezione 230 sono stati considerati essenziali per la crescita di Internet durante la prima parte del XXI secolo.

La protezione offerta a condizioni omogenee dalla sezione 230 CDA si riferisce a qualunque fornitore di un servizio informatico interattivo: fornitori di accesso alla rete, motori di ricerca, *social network*, piattaforme on line, forum, produttori di filtri *antispam*, programmatori di *software* antivirus e simili.

Dunque, come ha chiarito la giurisprudenza[154], tale dettato normativo prende le distanze dalla griglia tassonomica della *law of defamation.*

A dimostrazione di questo ventaglio molto ampio di protezione offerta, basti ricordare che nell'elaborazione giurisprudenziale la sezione 230 viene etichettata alternativamente come *"board immunity"* o "*robust immunity*"[155].

La giurisprudenza statunitense, chiamata nel corso degli anni a chiarire, interpretare e delimitare il confine delle disposizioni previste dalla sezione 230 CDA, ha precisato che tali disposizione possono trovare applicazione qualora si accerti che gli operatori, i quali svolgono un ruolo intermedio nel dare diffusione a contenuti altrui, possano essere chiamati ad esercitare le funzioni di *publisher*.

"Decidere se pubblicare, rimuovere o ritardare la pubblicazione" e "rivedere e controllare i contenuti inviati per la pubblicazione"[156] sono tutte "attività comunemente associate all'attività del publisher"[157].

La linea di confine tra irresponsabilità e responsabilità è dunque dettata dalla specifica funzione svolta dall'intermediario informatico: occorre comprendere se si tratta di un mero partecipe dell'informazione altrui o se è autore di una ben precisa porzione di illecito[158].

---

[154] *Zeran v. America Online, Inc*., 958 F. Supp. 1124 (E.D. Va. 1997).

[155] Sul punto v. M. LAVI, *Content Providers' Secondary liability: A Social Network Perspective*, 26 *Fordham Intell. Prop. Media&Ent. L.J.*, 2016, p. 855; S. K. MERHA e M. TRIMBLE, S*econdary Liability, ISP Immunity, and Incumbent Entrenchment*, *62 Am. J. Comp. L.*, 2014, p. 685; D. K. CITRON-B. WITTES, *The Internet Will not Break: Denying Bad Samaritans "Sect" 230 Immunity*, *86 Fordham L. Rev.*, 2017, p. 401 ss.; R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. 14.

[156] *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096 (9th Cir. 2009).

[157] *Zeran v. America Online, Inc*., 958 F. Supp. 1124 (E.D. Va. 1997), cit.

[158] *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC,* 521 F.3d 1157 (9th Cir. 2008).

La sezione 230 CDA garantisce, alla luce di quanto analizzato, un'immunità pressoché totale al provider e l'applicazione giurisprudenziale, come è emerso, ha contribuito a consolidarla. L'influenza del CDA sulle successive pronunce giurisprudenziali è stata dirompente: le Corti, infatti, hanno applicato le disposizioni della sezione 230 in maniera esasperata, non riconoscendo in nessun caso i providers responsabili per le comunicazioni e le informazioni diffuse.

Significativo, in questo senso, è il primo caso successivo all'emanazione dell'*Act*: *Zeran v. America Online (AOL)*[159].

La vicenda è la seguente. Il 25 aprile 1995, pochi giorni dopo l'attentato compiuto contro l'*Alfred P. Murrah Building* di Oklahoma City, era stato diffuso un messaggio all'interno di un *Bulletin Board System* gestito dalla società *AOL*, nel quale era pubblicizzata la vendita di alcune magliette dal contenuto scherzoso relative all'accaduto («*Naughty Oklahoma T-Shirts*», recitava, con un discutibile sense of humor, il messaggio).

Era indicato anche il numero di telefono del (presunto) venditore, che corrispondeva a quello del sig. Zeran, ovviamene ignaro del fatto.

Questi riceveva, nel breve volgere di poche ore, centinaia di telefonate: non si trattava di potenziali acquirenti, ma di persone che, risentite per il contenuto del messaggio, si prodigavano in offese di ogni genere – fino, addirittura, ad alcune minacce di morte – nei suoi confronti. Il malcapitato destinatario di tanta attenzione contattava prontamente la *AOL*: un impiegato lo rassicurava, dicendogli che il messaggio sarebbe stato eliminato. La vicenda, però, non si concluse.

Il giorno dopo, infatti, veniva diffuso un altro messaggio, il cui contenuto era analogo: dopo aver ribadito il numero di telefono (che, ancora una volta, corrispondeva a quello dello Zeran), si chiedeva addirittura alle persone interessare di pazientare e di provare a chiamare più volte nel caso in cui avessero trovato occupato.

La *AOL*, sollecitata ancora ad intervenire, rimosse anche il secondo messaggio. Ma ve ne furono degli altri. Le telefonate ricevute dal sig. Zeran aumentarono (fino ad arrivare ad una ogni due minuti, come ricorda quasi impietosamente la sentenza); questi, per arginare la vicenda cercò rimedio contattando addirittura l'F.B.I.

La situazione, se possibile, peggiorò addirittura, poiché una radio privata (*KRXO*, una radio di Oklahoma City), informata della vicenda, non esitò a diffondere pubblicamente il numero

[159] *Zeran v. America Online, Inc*., 958 F. Supp. 1124 (E.D. Va. 1997), cit.

telefonico dello Zeran, invitando tutti gli ascoltatori a chiamare per manifestare la propria disapprovazione. Questi, in sintesi, i fatti della causa.

Tralasciando l'azione giudiziaria intentata nei confronti della radio, poiché esula dagli interessi della presente ricerca, occorre concentrare l'attenzione sulla vicenda giudiziaria relativa alla responsabilità del provider.

In primo grado, la Corte del Distretto Orientale della Virginia ha deciso che, stante il disposto della sezione 230 del CDA, la *AOL* non può essere considerata responsabile per un messaggio diffuso da altri (sebbene non fosse stato individuato l'autore materiale dell'illecito).

In appello, la decisione è stata confermata. La corte, in particolare, ha rigettato la domanda dello Zeran di considerare il provider come *distributor,* figura non presa in esame dal *Decency Act*, e di considerarlo responsabile dal momento che aveva una *specific knowledge* (ossia era a conoscenza) dell'illecito. La questione si arresta a questo punto, poiché la Corte Suprema, investita del caso, ha negato il *writ of certiorari* e, quindi, ha rifiutato di decidere sul caso. La sorprendente decisione del caso Zeran non ha rappresentato un esempio isolato del nuovo approccio della giurisprudenza alla tematica in questione, anzi, è assurto rapidamente a *leading case*. Infatti, la decisione fu analoga nel caso *Lunney v. Prodigy*[160].

Per di più, nel secondo periodo della sezione 230 (e) (3) è prevista una ulteriore garanzia a favore dei prestatori intermedi, volta a sottrarre il cyberspazio agli interventi normativi dei governi territoriali.

Nella disposizione legislativa si legge infatti che "nessuna *cause of action* può essere accordata e nessuna responsabilità può essere imposta sulla base di disposizioni statali o locali che non siano conformi a questa sezione"[161].

Un'eventuale previsione ultronea di responsabilità avrebbe finito per frustrare la ratio del *Communications Decency Act.*

Le interpretazioni della giurisprudenza sono sempre infatti state a favore dell'incremento delle capacità di autoregolamentazione degli intermediari, in modo da giustificare qualsiasi scelta effettuata con riferimento ai contenuti presenti sugli spazi digitali e di eliminare quanto più possibile la discrezionalità valutativa del giudice al fine di tenere lontano il provider dalla reazione risarcitoria.

---

[160] *Lunney v. Prodigy Services Co.*, 94 N.Y.2d 242 (1999).

[161] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto,* cit., p. 24 ss.

Per il provider sarà sufficiente aggrapparsi ad un appiglio qualsiasi seppur debole per mantenere l'immunità[162].

Come è stato rilevato da attenti studiosi, non stupisce che, in applicazione di tali principi, l'unica tutela spettante a chi abbia subito un danno dalle azioni intraprese dall'intermediario sia individuata in quella di dimostrarne il dolo[163].

Sebbene dottrina e giurisprudenza concordino sul fatto che la sezione 230 CDA non meriti necessariamente una copertura costituzionale ai sensi del Primo Emendamento e che essa sia il frutto di una scelta di policy del legislatore tra le tante altrimenti possibili, una lettura della norma calata nella trama concettuale del presidio costituzionale previsto per la libertà di manifestazione del pensiero aiuta a spiegare le ragioni che hanno indotto la giurisprudenza[164] ad adottare un'interpretazione così estesa delle già importati garanzie offerte dalla norma federale a quanti facilitino la circolazione delle informazioni sulla rete telematica[165].

È con il caso *New York Time Co. v. Sullivan* che si afferma per la prima volta in maniera inequivocabile "la necessità di assicurare alla libertà di espressione una *special and strict protection*" tale da coprire anche affermazioni false che possano ledere la reputazione di pubblici ufficiali[166]. A questa pronuncia ne segue un'altra che erige delle barriere costituzionali a tutela della libertà di espressione anche nel diverso caso i cui la persona diffamata sia un cittadino comune[167].

Come ribadito da una consolidata giurisprudenza "la tendenziale riluttanza verso qualsivoglia attività di bilanciamento o di ponderazione tesa alla individuazione volta per volta di un punto di composizione e coesistenza tra libertà di espressione ed altre situazioni giuridiche soggettive: in tale logica, il rispetto di *ad hoc balancing approach* trova la propria giustificazione in relazione al fatto che la scala di valori è stata già dettata dalla Costituzione e che in cima ad essa, garantendole un posto privilegiato, è stata posta la stampa libera,

---

[162] E. GOLDMAN, *Online User Account Termination and 47 U.S.C.*, in *2 U.C. Irvine L. Rev.*, 2012, p. 659 ss.
[163] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. 15 ss.
[164] *Gucci America, Inc. v. Hall & Associates*, 135 F. Supp. 2d 409 (S.D.N.Y. 2001).
[165] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., pp. 28,29,30.
Cfr. D. K. CITRON-B. WITTES, *The Internet Will not Break: Denying Bad Samaritans "Sect" 230 Immunity*, cit., p. 409 e J. M. BALKIN, *The Future of Free Expression in a Digital Age*, in *36 Pepp. L. Rev.*, 2009, p. 427 ss.
[166] *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964).
[167] *Gertz v. Robert Welch, Inc*., 418 U.S. 323 (1974).

sottratta per il grave pericolo inerente e sicuro in ogni operazione di bilanciamento, alle incursioni del potere esecutivo, legislativo e giudiziario"[168].

In altri termini, nel diritto statunitense la libertà di parola, frutto di dedizione culturale e costituzionale[169], è un diritto incomprimibile e le eventuali restrizioni apposte sono ammesse solo nei casi limite e devono perseguire un "pressante interesse pubblico" ed essere "strettamente cucite intorno ad esso"[170].

Il ragionamento sottostante a questa linea interpretativa giurisprudenziale è spiegabile nella logica di intendere Internet come "luogo più importante per lo scambio di opinioni" e i social network come "moderne piazze pubbliche in cui esprimersi e confrontarsi"[171].

Con un impianto normativo così costruito, si è affermata nel corso degli anni una presunzione di assoluta irresponsabilità del provider che si troverebbe a dover regolare la libertà di espressione negli spazi digitali.

Pertanto, qualsiasi forma di responsabilizzazione, renderebbe gli intermediari inadeguati ed incompetenti a delimitare i confini di tale diritto e "la minaccia di sanzioni penali o civili coarterebbe il soggetto avverso al rischio all'adozione di prassi subottimali e sovra-censorie"[172].

Emblematica è la vicenda dell'esperimento *Wikitorial*, iniziativa lanciata nel 2005 dal *Los Angeles Times* nella sua edizione telematica, nella quale si è testata l'organizzazione delle informazioni affidata alle reazioni degli internauti.

Nell'ambito di tale iniziativa è stato rivolto un invito ai lettori a pubblicare qualsivoglia contenuto in tema con un articolo che riguardava i *pro* e i *contra* della guerra in Iraq.

Il servizio è stato costretto a chiudere dopo pochissimi giorni perché è stato completamente travolto dall'assalto di *spammer*, vandali e *troll* che saturarono di pornografia lo spazio digitale.

Questo esperimento era in perfetta linea con i valori di libera discussione tanto decantato dal Primo Emendamento.

Tre i presupposti che si si sono rivelati completamente errati.

---

[168] *Time, Inc. v. Hill*, 385 U.S. 374 (1967).
[169] E. GOLDBERG, *Free Speech consequentialism*, in *116 Colum. L. Rev.*, 2016, p. 687.
[170] *Chaplinsky v. New Hampshire*, 315 U.S. 568 (1942).
[171] *Packingham v. North Carolina*, 582 U.S. (2017).
[172] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. 50 ricorda il ragionamento della sentenza *Smith v. California*, 361 U.S. 147 (1959).

Anzitutto le comunità presenti sugli spazi digitali non posso di certo operare senza alcuna regolamentazione e la più ampia partecipazione di utenti finali non può essere una garanzia sufficiente per la qualità dei contenuti pubblicati.
In più, anche se si dovesse riconoscere che la moderazione della creatività dell'internauta sia necessaria, di certo non può sorgere su base spontanea.
La sezione 230 CDA, dunque, rifiuta di ammettere un regime di responsabilità basato sul "*knowledge standard*", chiude ad ogni forma di responsabilità per *development* e attribuisce agli intermediari poteri di moderazione dei contenuti che sfuggono ad ogni tipo di controllo nel merito.
Viene data la possibilità all'intermediario di agire e di esercitare il proprio potere nella più assoluta segretezza, non tenendo conto che, anche a voler concedere il beneficio del dubbio circa la buona fede delle operazioni di controllo dell'intermediario, comunque potrebbe trattarsi di un decisore incompetente, impreparato ad arbitrare certe controversie.
Senza tener conto che, come dimostrano i casi che si pongono all'attenzione della giurisprudenza[173], l'intermediario potrebbe essere incentivato alla rimozione di certe informazioni solo per strategie commerciali o potrebbe non essere attento alla rimozione di alcuni contenuti illeciti per ragioni pretestuose o di guadagni.
Grave disattenzione anche nei riguardi della giustificazione valoriale sottesa alla illimitata protezione concessa all'intermediario.
Sono proprio le attività di organizzazione e di controllo dei contenuti che consentono di rendere fruibile il web e di cercare di sottrarlo all'abuso dei terzi e alla commissione di fatti illeciti da parte degli utenti.
Si potrebbe procedere alla moderazione dei contenuti attraverso l'uso di algoritmi (filtri basati su specifiche regole e parole, o su *impronte-hash* o con tecnologie di *finger-printing*), di *flag* (le segnalazioni degli utenti della rete) o meglio con l'impiego tutt'al più incrociato di algoritmi e *flag* ed il monitoraggio incentrato su ben individuati spazi delle piattaforme in maggior misura passibili di abusi.
Occorre tenere ben presente che il *flag* dell'internauta non sempre è una proiezione più ampia dei valori espressi a una data comunità ma spesso può anche avere risvolti patologici. Si tratta pur sempre di uno strumento di reclamo di un singolo relativamente ad un contenuto riprovevole e potrebbe esser inviato anche per sopprimere punti di vista, minacciare

[173] *Ex multis*, *Riggs v. MySpace, Inc.*, 2:09-cv-03073-GHK-CT (C.D. Cal. Sept. 17, 2009) e *Langdon v. Google Inc. et al*, No. 1:2006cv00319 - Document 67 (D. Del. 2007).

l'intermediario o un altro utente o per pregiudicare la relazione di fiducia tra piattaforme ed utente.

Appare condivisibile ritenere che, sebbene i *flags* possano costituire un valido strumento di ausilio al controllo degli spazi digitali, di certo non si può ritenere che siano l'unico strumento o quello più affidabile.

Le tecnologie in continua avanzata di algoritmi certamente contribuirebbero a (ri)stabilire in maniera neutrale la liceità in rete.

I profili analizzati testimoniano quanto sia ampia l'immunità conferita agli operatori della rete e quanto anche i profili potenzialmente aperti ad un'interpretazione più rigida siano stati chiusi dalla giurisprudenza in senso sovra-protettivo, "munendo il prestatore di una corazza pressoché inscalfibile"[174].

Tuttavia, lasciare che fenomeni quali cyberbullismo, Revenge porn, pedopornografia, diffamazioni, sfruttamento sessuale siano affidati alla determinazione incondizionata degli intermediari, che possono agire con intenzioni più o meno ingenue senza rischiare alcunché, appare una soluzione inapplicabile ai tempi odierni e certamente il rifiuto di apportare degli aggiustamenti a tale regola non tiene conto dei bisogni del momento e dell'evoluzione dei tempi e della tecnologia avanzata.

Il provider che decidesse di operare in segretezza e senza la collaborazione di professionisti competenti, rendendo impermeabile qualunque scelta, dovrebbe essere spogliato del regime di favor e dovrebbe essere chiamato a rispondere per la partecipazione del fatto illecito altrui secondo le regole ordinarie in materia di responsabilità.

Il legislatore statunitense nel 1998 emenda il *Copyright Act* del 1976 con il *Digital Millennium Copyright Act* e prevede una sezione, la 512, dedicata alle "*Limitations on liability relating to material online*".

Questa riforma rappresenta un raffinato tentativo di bilanciamento dei diversi interessi giuridicamente rilevanti, con specifico riguardo ai difficili bilanciamenti nel settore dei diritti d'autore in ambiente digitale, prevedendo un meccanismo di esonero di responsabilità per il provider.

Un tale sistema ha previsto 4 macrocategorie:

1) la sezione 512 (a) si occupa dei servizi di trasmissione di contenuti e di fornitura di accesso alla rete;
2) la sezione 512 (b) si occupa dei servizi di memorizzazione intermedia e temporanea;

[174] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. 63.

3) la sezione 512 (c)si occupa dei servizi di memorizzazione a carattere stabile;
4) la sezione 512 (d) si occupa dei servizi diretti a facilitare il reperimento dei contenuti immessi sugli spazi digitali.

Una legislazione federale, quella di cui alla sezione 512 del DMCA del 1998, incentrata su un regime di responsabilità civile del prestatore dei servizi di *hosting,* subordinato all'effettiva conoscenza maturata dall'intermediario dell'illecito da altri perpetrato tramite i propri servizi e sul divieto di obblighi generali di sorveglianza.

Si prevede dunque chiaramente l'esenzione della responsabilità a patto che il prestatore intermedio, il quale sia al corrente del fatto che i contenuti presenti sui propri spazi digitali sono illeciti (*actual knowledge*) o di fatti o di circostanze che rendano palese tale evenienza (*red flag knowledge*), rimuova speditamente il contenuto o ne disabiliti l'accesso.

Un altro importante principio di portata generale che viene sancito (sezione 512 lett. m) riguarda l'esclusione degli obblighi di sorveglianza della rete.

Il beneficio esonerativo della responsabilità non può essere subordinato a che il provider ricerchi in modo attivo fatti o circostanze che indichino la commissione di attività illecite.

Accanto a tale affermazione di carattere generale la sezione 512 prevede sia l'ulteriore deresponsabilizzazione dell'intermediario (*to any person for any claim*), qualora questi abbia rimosso in buona fede o disabilitato l'accesso a contenuti presenti in rete su segnalazione del titolare dei diritti, sia la procedura dettagliata del *notice and take down*.

Si tratta di una procedura di segnalazione degli illeciti di cui può servirsi il titolare dei diritti d'autore per radicare in capo all'intermediario la conoscenza effettiva della violazione.

La segnalazione deve pervenire al rappresentante a tal uopo designato dallo stesso provider, essere formulata per iscritto e corredata di firma, precisare quale sia l'opera (nel caso in cui si tratti di più opere occorre indicare una lista specifica e rappresentativa delle stesse), specificare i contenuti digitali che violino i diritti di esclusiva nonché tutte quelle informazioni che consentano al provider l'esatta individuazione degli stessi.

Deve altresì esserci una dichiarazione da cui si evinca che il richiedente ritenga in buona fede che lo sfruttamento dell'opera non sia stato autorizzato dal titolare o dalla legge (*good faith belif requirement*).

La segnalazione deve contenere anche un'attestazione che le informazioni inoltrate al provider siano accurate e che, agli effetti penali, il richiedente sia autorizzato ad agire nell'interesse del titolare.

Ogni elemento della richiesta di rimozione non è altro che una vera e propria garanzia procedurale posta a favore dell'intermediario e del fornitore del contenuto.

Nel caso in cui il provider resti inerte dinanzi alla segnalazione, l'effetto ricollegato *ope legis* è la riattivazione del normale circuito della responsabilità civile per *copyright infrigement*.
Resta comunque valida l'affermazione secondo la quale il fornitore di servizi telematici, che intenda beneficiare della limitazione di responsabilità, è tenuto comunque a rimuovere laddove abbia maturato l'effettiva conoscenza o abbia notizia di fatti o di circostanze da cui si evince la condotta illecita altrui, indipendentemente dalla proposizione di una segnalazione formale[175].
A favore degli intermediari ricorre una "*exclusionary rule"*, che proibisce di considerare valide le segnalazioni non complete e fa gravare sul danneggiato l'onere di provare che il provider ha maturato in ogni caso la conoscenza indipendentemente dalle carenze della segnalazione [176].
La seconda tipologia di rimedi previsti dal DMCA a favore del titolare dei diritti di autore alberga nella sezione 512 lett. h ove è articolata una procedura volta alla identificazione dell'autore del fatto illecito (*subpoena to identify infringer*): si prevede che il titolare che abbia già inviato la segnalazione possa richiedere alla cancelleria della Corte distrettuale un *subpoena* sotto dichiarazione giurata che tale provvedimento sia richiesto al solo fine di identificare l'autore diretto dell'illecito. Il *subpoena* avrà la conseguenza di autorizzare ed al tempo stesso vincolare l'intermediario a rivelare rapidamente le informazioni in suo possesso allo scopo di identificare l'autore dell'illecito.
Occorre prendere in esame anche il peculiare rimedio posto a salvaguardia delle ragioni di chi abbia immesso in rete i contenuti digitali poi estromessi a seguito della richiesta del titolare dei diritti: la procedura di contro-segnalazione (*counter-notification*), volta a paralizzare l'iniziativa unilaterale del presunto danneggiato, intrapresa fuori dal circuito giudiziale. Anche la contro-notificazione deve possedere, come la segnalazione, dei requisiti di forma e contenuto.
La proposizione di una valida contro-segnalazione produce una serie di conseguenze in capo all'intermediario. Essa ha l'effetto di vincolare il provider a contattare l'originario proponente la rimozione, a fornirgli copia della contro-segnalazione e ad informalo che provvederà a reinserire i contenuti sulla rete a partire dal decimo giorno lavorativo dalla sua

[175] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto,* cit., p. 80 ss.
[176] *UMG Recordings, Inc. v. VEOH Networks, Inc.*, No. CV 07-5744, 2008 U.S. Dist. LEXIS 104980 (C.D. Cal. December 29, 2008).

ricezione, salvo si evinca che il titolare abbia intentato un'azione contro l'autore del fatto illecito.

Il legislatore, ben conscio dei rischi di un tale sistema, ha introdotto un rimedio per arginare derive.

Il riferimento è alla sezione 512 (f)(1) che prevede le *Misrepresentations:* se un soggetto dichiara il falso nel sostenere che un certo contenuto violi i suoi diritti, sarà tenuto a risarcire i danni subiti dal terzo che si è visto rimuovere il contenuto che dal provider che ha attivato i meccanismi di rimozione.

Che tutto l'impianto normativo ruoti intorno a questo meccanismo di *notice and take down*, come è stato messo in luce da taluni studiosi[177], si può verificare mediante una disamina attenta della giurisprudenza che non ha modificato l'impianto in via pretoria.

In linea di principio la sezione 512 del DMCA non prevede che l'unica via per ottenere la rimozione dell'illecito sia la segnalazione di parte.

Al contrario, un fornitore di un servizio telematico che intenda beneficiare della limitazione della responsabilità è tenuto a rimuovere ove abbia comunque maturato l'effettiva conoscenza (*actual knowledge*) o abbia notizia do fatti o circostanze da cui traspaia la condotta plagiaria ed illecita altrui (*red flag knowledge*).

Rileva il criterio del *simple fact of notice*.

Il trinceramento del bilanciamento rinvenuto dal legislatore è stato chiuso ad ogni tentativo di interpretazione ampia del requisito della conoscenza effettiva. Il ricorrere di tale evenienza è stato relegato alle sole ipotesi in cui l'attore fosse riuscito a dimostrare in giudizio una conoscenza autentica, concreta e soggettiva da arte dell'intermediario[178].

La giurisprudenza ha dunque respinto sistematicamente ogni tentativo volto all'allargamento dei confini della nozione di conoscenza imputabile del fatto illecito altrui[179].

A titolo esemplificativo, dalla risoluzione di alcuni casi giurisprudenziali è emerso che le segnalazioni più volte inviate da utenti diversi danneggiati in relazione ai rispettivi diritti violati allo stesso intermediario nell'ambito della stessa azione non basta a dar luogo ad una conoscenza giuridicamente rilevante[180] né si può presumere il provider responsabile di un presunto illecito nell'ipotesi in cui transazioni commerciali degli internauti che acquistano

[177] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto,* cit., p. 80 ss.
[178] *Viacom Int'l, Inc. v. YouTube, Inc.* - 676 F.3d 19 (2d Cir. 2012).
[179] *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9° Cir.2007).
[180] *Viacom Int'l, Inc. v. YouTube, Inc.*, cit.

scatti per adulti sottratti illecitamente sino prestati su siti il cui dominio evoca espressamente le attività illecite perpetrate (*stolencelebritypics.com*)[181].

La sezione 512 (j) disciplina, invece, i rimedi inibitori e le relative misure sono suddivise proprio in relazione ai servizi prestati dagli intermediari informatici.

Se si tratta di un operatore che offre servizi di accesso ad Internet, i provvedimenti ingiuntivi spaziano dall'ordine di inibire l'accesso ad Internet a singoli utenti a quello di impedire il collegamento a specifiche pagine ospitate sui server.

Se invece viene in rilievo un'attività di memorizzazione, il comando del giudice può avere ad oggetto l'ordine di inibire l'accesso a specifici contenuto presenti sugli spazi digitali dell'intermediario, sospendere l'account di utenti identificati o adottare misure ritenute in ogni caso necessarie a limitare le violazioni.

La Corte prima di disporre una misura inibitoria deve verificare anzitutto se l'*injuction* grava in maniera eccessiva il provider, appesantendo il sistema, se sia serio il danno prodotto, se i rimedi disponibili siano adeguati a ristorare il pregiudizio e se l'esecuzione dell'odine sia tecnicamente realizzabile senza che questo interferisca con l'accesso a contenuti leciti.

Molto ampio è dunque il margine di responsabilità lasciato al giudice.

L'imperativo, nel contesto della sezione 512 DMCA, diviene infatti la rimozione incentrata sul *simple fact of notice* e quelle considerazioni di carattere pratico poste al centro della scena nell'elaborazione giurisprudenziale della sezione 230 CDA a presidio della libertà di espressione, tutelata da Primo Emendamento, sembrano più sopite[182].

In realtà occorre sottolineare che le preoccupazioni per la tutela dei valori contemplati dal Primo Emendamento non sono affatto venute meno anzi sono le stesse finalità della tutela dei diritti d'autore a reindirizzare libertà di espressione e proprietà intellettuale su binari paralleli.

Oggi si va sempre di più verso un'automazione e professionalizzazione del processo di invio delle richieste di rimozione, al punto che all'interno delle grandi imprese ci sono dei gruppi specializzati nell'inoltro di segnalazioni.

Le richieste di rimozione sono automatizzate: attraverso la scansione sistematica del web effettuata da software che operano sulla base di algoritmi, incentrati sulla corrispondenza di

[181] *Perfect 10, Inc. v. CCBill LLC,* cit.

[182] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto,* cit., p. 106 ss.

titoli-opere-autori o di altri indicatori, si è ampliata a dismisura la possibilità di contrastare le violazioni su larga scala (*DMCA Auto e Plus*)[183].

Occorre dunque comprendere le modalità attraverso le quali operano tali software allo stato dell'attuale evoluzione tecnologica.

Una delle tecnologie più comuni di filtraggio è quella incentrata sull'utilizzo dei metadati. Questi potrebbero essere definiti come il corredo di informazioni ai contenuti informatici che mirano alla loro descrizione.

Comparando manualmente o automaticamente le informazioni descrittive delle opere che si intendano proteggere con i metadati dei contenuti presenti sulla piattaforma è possibile individuare i file da rimuovere.

Tuttavia, tale tipo di tecnologia, così come è stato rilevato[184], è inaffidabile, in quanto si incentra sulle informazioni inserite dagli stessi utenti a corredo del contenuto caricato, inaccurata, potendo portare ad individuare file che con il contenuto da rimuovere non condividano alcunché se non alcune informazioni descrittive, ed aggirabile, in quanto basta criptare, rinominare abbreviare o ricodificare i metadati per frustare le capacità di eseguire ricerche di questo tipo.

Non a caso è anche il meccanismo più di filtraggio meno costoso.

Sicuramente una tecnologia più sofisticata è quella basata sui filtri di *hash*.

Con questa tecnica si effettua una riproduzione algebrica di un certo contenuto attraverso una sua rappresentazione numerica.

Si tratta di un metodo più affidabile rispetto ai metadati in quanto il valore di *hash* rappresenta in modo univoco il contenuto del file. Occorrerà guardare non al contenuto ma solo alla stringa numerica restituita dal valore di *hash* associata alla specifica opera e conservata in un *database*.

Una terza tipologia fi strumenti di filtraggio è basata sulle "impronte digitali".

In questa ipotesi si guarda direttamente alle caratteristiche contraddistintive del contenuto. Si crea una sorta di impronta digitale di tale contenuto, incentrata su alcune caratteristiche peculiari del bene in oggetto.

Il campione da analizzare è dunque confrontato con un archivio centrale alla ricerca delle somiglianze.

---

[183] J.M. URBAN e J. KARAGANIS, *Notice and Takedown in Everyday Practice*, BerkleyLaw, 2016, p. 60 ss.

[184] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. 122 ss.

Tra tutte, è il riconoscimento automatico dei contenuti più sofisticati questo delle impronte digitali[185].

Alla stregua di quanto sostenuto, la scelta in punto di metodo effettuata dal legislatore nella sezione 512 DMCA consiste nel presumere l'incompetenza dell'intermediario a farsi carico delle difficili questioni che soggiacciono alle violazioni dei diritti di autore e nel fornire una guida certa della condotta da adottare.

Senza dubbio occorrerebbe garantire una maggiore sicurezza e trasparenza per infrangere il muro della segretezza che attanaglia il fenomeno delle rimozioni e delle gestioni dei contenuti affidate ai provider ed occorrerebbe rendere intellegibile il meccanismo di calcolo affidato ali algoritmi.

Insieme al *Digital Millennium Copyright Act* (DMCA) del 1998, la Sezione 230 fornisce ai fornitori di servizi Internet un porto sicuro per operare come intermediari di contenuti senza timore di essere responsabili per le informazioni immesse in rete, purché adottino misure ragionevoli per eliminare o impedire l'accesso a quel contenuto.

Queste protezioni hanno permesso applicazioni sperimentali e nuove nell'area Internet senza timore di ramificazioni legali, creando le basi dei moderni servizi Internet come i motori di ricerca avanzati, social media, streaming video e *cloud computing.*

Se negli anni Novanta tali soluzioni potevano essere pure appaganti, oggi sicuramente l'evoluzione tecnologica ed avanzata della rete rende inammissibile un tale impianto, specie se poi si sostiene che non è possibile controllare l'immissione di contenuti illeciti ma si consentono operazioni molto più complesse per campagna pubblicitarie e guadagni da riscuotere.

L'ampia immunità concessa ai provider non può non lasciar pensare ad una riforma per un'equa partecipazione della cultura democratica.

Infatti, nel 2020, sono stati presentati diversi progetti di legge attraverso il Congresso per limitare le tutele di responsabilità che le piattaforme Internet hanno dalla Sezione 230, anche sulla base degli eventi verificatisi gli anni passati.

Nel marzo 2020 è stato presentato al Senato un disegno di legge *bipartisan* noto come *Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act* (S. 3398), che chiede la creazione di una commissione governativa di 15 membri (tra cui

[185] S.K. KATYAL-J. M. SCHULTZ, *The Unending Search for the Optimal Infringement Filter*, in *112 Colum. L. Rev. Sidebar*, 2012, p. 83 ss.; E. ENGSTROM-N. FEAMSTER, *The Limits of Filtering: A Look at the Functionality & Shortcomings of Content Detection Tools*, 2017, p. 13, disponibile *online* all'indirizzo *https://www.engine.is/the-limits-of-filtering*; L. HELMAN-G. PARCHOMOVSKY, *The Best Available Technology Standard*, in *111 Colum. L. Rev.*, 2011, p. 1194 ss.

funzionari dell'amministrazione ed esperti del settore) per stabilire "migliori pratiche" per l'individuazione e la segnalazione di materiali di sfruttamento minorile.

I servizi Internet sarebbero tenuti a seguire queste pratiche; la commissione avrebbe il potere di sanzionare coloro che non sono in regola, il che può includere la rimozione delle protezioni della Sezione 230.

È stata chiesta l'abrogazione di tale sezione perché se è vero che è nata per permettere la crescita di internet agli albori, quando la maggior parte delle aziende non era stabile, ora non si riescono a regolare bene quelli che sono diventati nel tempo i titani della rete.

Questa preoccupazione è stata avanzata nel febbraio 2020 proprio dal William Barr, procuratore generale del Dipartimento di Giustizia degli Stati Uniti, nel corso di un seminario relativo alla Sezione 230 nell'ambito di un'indagine antitrust in corso sulle società "*big tech*".

Nel luglio 2021, i senatori democratici Amy Klobuchar e Ben Ray Luján hanno introdotto l' *Health Misinformation Act* , che mira principalmente a combattere la disinformazione COVID-19 , ma prevedrebbe anche uno scorporo alla Sezione 230 per rendere le aziende responsabili della pubblicazione di "disinformazione sanitaria" durante un'" emergenza sanitaria pubblica " - come stabilito dal Dipartimento della salute e dei servizi umani - se il contenuto viene promosso agli utenti tramite decisioni algoritmiche.

Un'aria di cambiamento importante si profila dunque all'orizzonte.

A seguito della testimonianza di Frances Haugen al Congresso, ex dipendente di Facebook che ha fatto trapelare parte dei risultati di un'ampia ricerca interna, relativa alla sua denuncia sulla gestione interna dei contenuti del social network, i democratici della Camera hanno introdotto il "*Justice Against Malicious Algorithms Act*" nell'ottobre 2021.

Il disegno di legge eliminerebbe le protezioni della Sezione 230 per i fornitori di servizi relativi agli algoritmi di raccomandazione personalizzati che presentano contenuti agli utenti se tali algoritmi forniscono consapevolmente o incautamente contenuti che contribuiscono a lesioni fisiche o emotive gravi.

Allo stato attuale, il DMCA resta una disciplina specifica disciplina del copyright in rete e della sua violazione senza estendere gli effetti ad altre materie.

L'approccio verticale adottato dal legislatore statunitense rimette infatti la *defamation* all'esclusiva regolamentazione del CDA, visto che tale ultimo dettato normativo è di carattere più generale e dunque meglio si presta ad esercitare influenza su tutte le numerose materie per le quali il legislatore non ha ritenuto necessario o opportuno legiferare.

Nonostante però il DMCA sia una disciplina di settore, più del CDA, ha profondamente influenzato altri legislatori di diversi ordinamenti nel tema generale della responsabilità degli intermediari per ogni tipo di illecito in Internet, probabilmente per la disciplina sostanziale e per la tecnica legislativa adoperata.

3. La responsabilità civile degli intermediari della rete nel modello europeo

L'Unione Europea predispone una regolamentazione di carattere generale in tema di responsabilità degli intermediari della rete telematica.

La disciplina della responsabilità dei provider è stata regolamentata dal legislatore eurocomunitario con la direttiva 2000/31/CE dell'8 giugno 2000 ("Direttiva sul Commercio elettronico") che, pur avendo principalmente ad oggetto gli aspetti contrattuali dell'*E-Commerce*, dedica un'intera sezione alla "Responsabilità dei prestatori intermediari", da intendersi come quei soggetti che esercitano attività imprenditoriale di prestazione di servizi della società dell'informazione[186].

Sebbene possa sembrare quanto meno peculiare la scelta di regolamentare il tema della responsabilità del provider nell'ambito di una direttiva dedicata prevalentemente al commercio elettronico, essa è stata dettata, come emerge dai "*Considerando*", dall'esigenza di stabilire un quadro giuridico chiaro ed uniforme e di innalzare i livelli di fiducia dei consumatori[187].

La scelta di intraprendere la strada di un sistema unitario è frutto probabilmente della circostanza che l'intervento normativo dell'Unione europea si inserisce in un ambito diverso rispetto a quello in cui ha operato il legislatore federale statunitense.

L'obiettivo principale è stato infatti quello di stabilire un punto univoco di riferimento per taluni aspetti giuridici del commercio elettronico e dunque di favorire lo sviluppo di quella

[186] G. COMANDÈ-S. SICA, *Il commercio elettronico. Profili giuridici*, cit. p. 223 ss.; V. ZENO ZENCOVICH, *Note critiche sulla nuova disciplina del commercio elettronico dettata dal d.lgs. n. 70/2003*, in *Dir. inf.*, 2003, p. 505 ss.; E. TOSI, *I problemi giuridici di Internet. Dall'E-Commerce all'E-Business*, Milano, 2003, p. 570 ss., G. COMANDÈ, *Al via l'attuazione della direttiva sul commercio elettronico, ma…serve un maggior coordinamento*, in *Danno e resp.*, 2003, p. 811 ss.; A. PIERUCCI, *La responsabilità del Provider per i contenuti illeciti della Rete*, in *Riv. crit. dir. priv*., 2003, p. 158 ss.; G. PASCUZZI, *Il diritto nell'era digitale. Tecnologie informatiche e regole privatistiche*, cit., p. 100 ss.; F. SIGNORELLI, *Profili di responsabilità del provider nell'E-Commerce*, in V. FRANCESCHELLI (a cura di), *Commercio elettronico*, Milano, 2001, p. 555 ss.; L. MARINI, *Profili giuridici del commercio elettronico nel diritto internazionale e comunitario*, in *Dir. comm. int.*, 2000, p. 329 ss.

[187] M. DE CATA, *La responsabilità civile dell'internet service provider*, cit., p. 185 ss.; E. SANNA, *Il regime di responsabilità dei provider intermediari di servizi della società dell'informazione*, in *Resp. civ. prev*., 2004, p. 279 ss.

particolare forma di commercio di beni e servizi che non prevede la presenza fisica di venditore e compratore e che si svolge interamente su Internet.

La normativa, come si legge nel preambolo della direttiva, si prefiggeva come obiettivo quello di garantire un elevato livello di integrazione giuridica comunitaria al fine di instaurare un vero e proprio spazio senza frontiere interne per i servizi della società dell'informazione.

Che siano lesi interessi privati quali l'altrui reputazione, la riservatezza del singolo, i diritti d'autore e simili o che siano messi a repentaglio interessi pubblici, come nel caso di circolazione di immagini pedopornografiche o di esternazioni di incitamento alla violenza, di discorsi d'odio o di contenuti terroristici, il riferimento normativo per la eventuale responsabilità degli intermediari la si rinviene sempre degli artt. 12,13,14 e 15 della direttiva sul commercio elettronico[188].

Prendendo come modello la normativa statunitense, il legislatore europeo ha previsto ampi spazi di autoregolamentazione ed un sistema graduale di esenzione da responsabilità, incentrato su una valutazione separata dei differenti servizi prestati dagli intermediari a seconda delle possibilità di controllo e di intervento rispetto ai contenuti veicolati dagli utenti e della maggiore o minore prossimità tra il servizio erogato ed il fatto illecito dell'user.

L'art. 12 della direttiva 2000/31 disciplina le attività di fornitura di accesso ad Internet e di trasmissione su rete di comunicazione di informazioni fornite dai destinatari dei servizi telematici (c.d. *mere conduit*).

Per questi intermediari, che si trovano in una pacifica condizione di neutralità, il legislatore ha previsto che il provider non sia responsabile delle informazioni trasmesse a condizione che egli:

a) non dia origine alla trasmissione;

b) non selezioni il destinatario della trasmissione;

c) non selezioni né modifichi le informazioni trasmesse.

Le attività di trasmissione e di fornitura di accesso includono anche 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.

L'art. 13 della direttiva 2000/31 invece si riferisce ai prestatori la cui attività si sostanzia nella memorizzazione temporanea, intermedia ed automatica (detta *caching*).

---

[188] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. 134 ss.

È previsto un generale regime di esenzione di responsabilità. In particolare, secondo il disposto legislativo, nella prestazione di un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, il prestatore non è responsabile della memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta, a condizione che egli:

a) non modifichi le informazioni;

b) si conformi alle condizioni di accesso alle informazioni;

c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore;

d) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni;

e) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione dell'accesso.

Con riferimento al regime previsto per gli intermediari la cui attività consiste nella fornitura di servizi di memorizzazione permanente (c.d. *hosting*), l'art. 14 della direttiva 2000/31 dispone che il prestatore non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto 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 dell'informazione;

b) non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

Questo regime non trova applicazione se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore.

In più, tutti e tre gli articoli relativi alle attività del provider prevedono la facoltà per gli Stati membri di disporre che un organo giurisdizionale o un'autorità amministrativa possa esigere o disporre la fine di una violazione.

Sebbene tali norme siano chiare in tutta la loro portata, il centro nevralgico di tutta la disciplina è contenuto nell'art. 15 della direttiva 2000/31.

Analogamente al modello statunitense previsto nella sezione 512 del DMCA, la direttiva 2000/31 ha sancito, all'art. 15, il divieto di imporre obblighi generali di sorveglianza preventiva o successiva e di ricerca di fatti o di circostanze che possano indicare la commissione di fatti illeciti, a tutela di tutti gli intermediari dei servizi di base di Internet (nella tripartizione legislativa di fornitori di servizi di accesso, di memorizzazione temporanea e di memorizzazione permanente).

Si stabilisce infatti che 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[189].

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.

Ancora, di rilevante importanza è la previsione sancita dall'art. 21 della direttiva. La disposizione si riserva infatti la possibilità, tenuto conto dell'evoluzione tecnologica, di rendere doverose nuove prestazioni dirette a prevenire gli illeciti e l'opportunità di avanzare proposte per adeguare la disciplina dell'evoluzione giuridica, tecnica ed economica dei servizi della società dell'informazione, in particolare per quanto concerne la prevenzione dei reati, la protezione dei minori, la tutela dei consumatori e il corretto funzionamento del mercato interno.

A differenza del modello ispiratore, però, la direttiva 2000/31 concerne qualunque fatto illecito e qualsivoglia tipo di responsabilità (penale, civile e amministrativa), generalizzando gli obblighi di rimozione di contenuti illeciti previsti dall'art. 14, obblighi la cui regolamentazione di dettaglio (in specie sulle procedure di segnalazione), in omaggio al principio di sussidiarietà e dell'autonomia procedurale riservata agli Stati membri, è stata fondamentalmente affidata alla discrezionalità normativa di questi ultimi .

Il tempo trascorso dall'approvazione della direttiva del 2000 ha, tuttavia, fatto emergere che le eccezioni legislative alla responsabilità previste per gli intermediari della rete telematica sono in effetti, almeno nel contesto unitario-europeo, molto meno ampie di quanto a prima vista potesse apparire.

---

[189] R. BOCCHINI, *La responsabilità extracontrattuale del provider*, in D. VALENTINO, *Manuale di diritto dell'informatica*, 2016, p. 539 ss.

Sul piano interpretativo del quadro normativo vigente, i giudici nazionali, chiamati ad applicare le misure di attuazione della direttiva 2000/31, e la Corte europea di FGustizia, interpellata dai primi, con lo strumento della pregiudiziale comunitaria ai sensi dell'art. 267 del TFUE, hanno, infatti, progressivamente circoscritto il regime di irresponsabilità e hanno indicato al danneggiato dalla circolazione in rete di contenuti illeciti sentieri rimediali da intraprendere, alternativamente o cumulativamente, nei confronti degli intermediari di Internet.

In una prospettiva *de iure condendo*, da un canto la diffusione in rete di contenuti tra i più allarmanti per i valori democratici - quali, ad esempio, quelli di incitamento al terrorismo, di istigazione ad azioni xenofobe o razziste, di fomentazione dell'odio e della violenza, di sfruttamento della pornografia minorile, dell'organizzazione della tratta di esseri umani - e, d'altro canto, le novità tecnologiche che facilitano l'individuazione automatica e la rimozione immediata dei contenuti illeciti hanno sollecitato, nell'organo istituzionalmente deputato all'iniziativa legislativa nell'Unione Europea, l'idea della necessità che i gestori delle piattaforme online - considerato anche il « ruolo centrale » da essi ricoperto « nella società» - assumano maggiori responsabilità (nell'accezione stretta del termine inglese "*liability*" ed in quella più lata del termine "*accountability*"), intensifichino gli sforzi volti al contrasto dei « contenuti illegali online in cooperazione con le autorità nazionali, gli Stati membri e i portatori d'interessi pertinenti» e agiscano in maniera « proattiv[a] nell'eliminazione » di tali contenuti.

Sebbene la sezione 512 sia stata fonte d'ispirazione per il legislatore comunitario, le differenze vanno giustificate anche alla luce di un'innegabile diversa tutela accordata nello spazio giuridico europeo alla libertà di espressione e contestualmente del sensibile ampliamento dei diritti fondamentali da prendere in considerazione e da sottoporre a bilanciamento.

Nel leggere la giurisprudenza della Corte europea dei diritti dell'Uomo, risulta immediatamente evidente che le affermazioni offensive e diffamatorie, proferite con il solo intento di insultare, non rientrano nella protezione della libertà di espressione di cui all'art. 10 CEDU.

Questo perché accanto alla libertà di espressione, nella valutazione dei profili rimediali esperibili dai singoli danneggiati dall'uso che terzi fanno dei servizi messi a disposizione dagli intermediari, occorre prendere in esame altri valori che, nel contesto unitario europeo, assurgono al rango di diritti fondamentali. Si pensi ai diritti reputazionali, al diritto alla riservatezza, al diritto alla tutela dei dati personali, ai diritti di proprietà industriale *et similia*.

Ecco perché una prospettiva di favore verso l'interesse pubblico all'accesso all'informazione per mezzo dei free media previsto nel sistema statunitense con il *Communication Decency Act*, a tutela della libertà di espressione, non può trovare il medesimo spazio nel sistema giuridico europeo, dove il bilanciamento con altri diritti rimodula inevitabilmente i confini della libertà di espressione.

Se da un lato, infatti, la Corte Edu mette in risalto le potenzialità comunicative della rete in funzione della sua accessibilità, della capacità di immagazzinare e comunicare grandi quantità di informazioni (*Times Newspapers Ltd (Nos 1 and 2) v. The United Kingdom)*[190], dall'altro segnala in maniera veemente i pericoli che riguardano la lesione di diritti fondamentali concorrenti (*Delfi v. Estonia*)[191].

In *Delfi v. Estonia* si è infatti giustificata la compressione della libertà di informazione e si è condannato il provider per non aver rimosso di propria iniziativa ed in assenza di segnalazione di parte dei contenuti di incitamento all'odio rivolti nei confronti di una persona fisica, apostrofata con frasi ingiuriose e minacciata nella sia incolumità fisica[192].

Nel gennaio 2006, Delfi, uno dei più grandi siti di notizie su Internet nel paese, ha pubblicato un articolo sulla sua pagina web con il quale si criticava la decisione di una compagnia di traghetti di cambiare la rotta dei suoi viaggi verso alcune isole.

Questo mutamento aveva causato la rottura del ghiaccio dove si sarebbero potute creare strade ghiacciate nel prossimo futuro, perdendo così la possibilità di un collegamento più economico e veloce con le isole rispetto ai servizi di traghetto.

Questo articolo è stato commentato da molti lettori, i quali si sono lasciati andare ad affermazioni offensive o minacciose nei riguardi dell'operatore del traghetto e del suo proprietario.

Quest'ultimo ha citato in giudizio Delfi nell'aprile 2006 e ha ottenuto con successo una sentenza di condanna del portale nel giugno 2008.

Il tribunale estone ha infatti ritenuto che i commenti fossero diffamatori e che Delfi ne fosse responsabile.

Il ricorso di Delfi è stato respinto anche dalla Corte Suprema dell'Estonia nel giugno 2009.

Il provider si è difeso affermando che essere ritenuto responsabile per i commenti dei lettori ha violato il suo diritto alla libertà di espressione e pertanto ha adito la Corte Edu.

---

[190] Corte EDU, *Times Newspapers Ltd (Nos 1 and 2) v. The United Kingdom*, 10 marzo 2009, nn. 3002/03 e 23676/03.

[191] Corte EDU, Grande Camera, *Delfi v. Estonia*, 16 giugno 2015, n. 64569/09.

[192] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. 242 ss.

La Corte europea dei diritti dell'uomo ha stabilito che l'Estonia non ha violato l'articolo 10 della Convenzione europea dei diritti dell'uomo (CEDU) quando ha ritenuto l'organo di stampa online responsabile di diffamazione sulla base dei commenti pubblicati nella sezione commenti dei suoi articoli.

La Corte, nel condannare Delfi, ha condotto un vero proprio test di bilanciamento per determinare se i diritti dell'agenzia di stampa fossero stati violati.

Infatti, secondo la Corte EDU, i commenti erano stati insultanti, minacciosi e diffamatori. Data la natura dell'articolo, l'azienda avrebbe dovuto aspettarsi post offensivi ed approntare forme di tutela e cautele maggiori per evitare di essere ritenuta responsabile per danni alla reputazione di un individuo.

In secondo luogo, le misure intraprese da Delfi per impedire la pubblicazione di commenti diffamatori sono risultate deficitarie. Difatti, sebbene la pagina web dell'articolo affermasse che gli autori dei commenti sarebbero stati responsabili del loro contenuto e che i commenti minacciosi o offensivi non sarebbero stati consentiti, gli avvertimenti non sono riusciti ad impedire che venissero formulati un gran numero di commenti offensivi. Peraltro, questi non sono stati rimossi in tempo utile né dal filtro automatico delle parole né dal sistema di notifica di avviso e rimozione.

In terzo luogo, il portale in causa aveva consentito ai lettori di fare commenti in maniera anonima e dunque senza registrare i loro nomi. Pertanto, molti dei post erano anonimi. Ciò rendeva impossibile al proprietario ingiuriato e diffamato poter citare in giudizio direttamente gli autori dei contenuti illeciti.

Come la sezione 512 del *Digital Millennium Copyright Act* statunitense, anche la Sezione IV del capo II della direttiva 2000/31 richiama la possibilità per i danneggiati di esperire nei confronti degli intermediari anche una tutela inibitoria.

Se dunque l'esimente da responsabilità riguarda la reazione aquiliana, ma non impedisce l'esperibilità di rimedi risarcitori, il divieto di obblighi di carattere generale vale anche però per i provvedimenti che possono essere disposti da organi giurisdizionali o da autorità amministrative al fine di impedire o porre fine ad una violazione.

4. La responsabilità del provider nell' esperienza inglese

Il sistema inglese è stato il primo tra quelli europei ad adottare una previsione normativa specifica sulla responsabilità del provider, sia pure nell'ambito della disciplina della diffamazione[193].

Già nel 1996, il *Defamation Act* ha escluso la responsabilità del responsabile di un sistema informatico alla stregua di "*author, editor, publisher of a statement*", qualora il suo ruolo si sia limitato alla sola trasmissione di dati o alla semplice gestione del sistema elettronico che ha veicolato il messaggio[194].

Non vi sono riferimenti ai criteri di imputazione di responsabilità per quanto riguarda le attività di *caching* e di *hosting*[195]. Difatti, rispetto al sistema americano, il sistema inglese non ha raggiunto un grado di sviluppo elevato, anche per la scarsità di formante giurisprudenziale.

Più precisamente, mentre il sistema americano nega a priori, sulla base dell'analisi delle caratteristiche tecniche del servizio, l'equiparabilità del provider all'editore, il sistema inglese non esclude in radice tale ipotesi ma la subordina alla sussistenza in capo all'intermediario di un "*effective control*", la cui nozione non appare facilmente individuabile anche a causa della scarsità di precedenti giurisprudenziali, quanto mai fondamentali in un sistema di Common law.

Una pronuncia dell'*Hight Court*, nel 1999, *Godfrey v. Demon*[196], prima applicazione della riforma del 1996 con riferimento alle comunicazioni digitali, ha interpretato restrittivamente tale requisito, ritenendo il provider responsabile solo nel caso in cui egli abbia un effettivo potere di controllo e dunque nell'ipotesi di mancata rimozione del materiale nel momento successivo alla sua immissione.

Il giudice ha affermato il principio secondo cui il soggetto che memorizzi informazioni provenienti da terzi, le renda disponibili al pubblico e non ottemperi ad una richiesta circostanziata di rimozione, non può essere considerato unicamente un canale di trasmissione dei dati.

---

[193] M. DE CATA, *La responsabilità civile dell'Internet service provider*, cit., p. 131 ss. e G.M. RICCIO, *La responsabilità civile degli Internet providers*, cit., p. 120 ss.

[194] N. BRAITHWAITE, *The United Kingdom Defamation Act 1996*, in *15 Comm. Law.*, 1997, p. 12 ss.; M. SOCHA, *Double Standard: a comparison of British and American defamation law*, in *Penn. St. Int'l L. Rev.*, 2004, p. 271 ss.

[195] Per un primo commento alla legge, v. D.W. VICK-L. MACPHERSON, *An Opportunity Lost: The United Kingdom's Failed Reform of Defamation Law*, in *Fed. Comm. L.J.*, 1996, p. 621 ss.

[196] *Godfrey v. Demon*, [1999] E.W.J. No. 1226 (Q.B.D.). La questione, sebbene fosse stata rimessa alla giurisdizione superiore, si è conclusa con un accordo stragiudiziale tra le parti, in base al quale la società Demon ha versato all'attore una consistente somma di denaro. Cfr. Y. AKDENIZ, *Freedom of expression*: *Laurence Godfrey v. Demon Internet Limited*, in *4 Journal of Civil Liberties*, 1999, p. 260 ss.

Nel 1998 interviene l'*U.K. Design and Patent Act* che riconosce la responsabilità di chi abbia materialmente contribuito alla fattispecie illecita laddove questi, avendo conoscenza del fatto, si sia del tutto disinteressato alla questione della illiceità continuando ad agire o restando inerte[197].

Tale disposizione normativa, sebbene a differenza del DMCA non sia stata espressamente dettata per la regolamentazione in Internet della fattispecie, fa riferimento alle ipotesi di violazioni del *copyright* in generale e pertanto si è ritenuta applicabile anche al cyberspazio ed ai provider.

Si fa dunque applicazione del "*duty of care*" e l'intermediario si considera responsabile ogniqualvolta omette anche la misura minima di diligenza nell'adempimento dell'obbligo di rimozione conseguente alla conoscenza materiale sospetto e illecito.

L'*High Court*, nel 2001, con la pronuncia *Totalise PLC v. Motley Fool*, ha chiarito che "Internet, in quanto medium strutturalmente e funzionalmente diverso non è equiparabile alla stampa, con conseguente inapplicabilità della relativa normativa, e che il provider non può essere assimilato in alcun modo ad un *publisher* o *editor*".

Nel caso di specie il provider, ritenuto poi dalla corte inglese responsabile, non solo era rimasto inerte ma si era rifiutato di rivelare il nome del suo cliente, appellandosi al *Data Protection Act*, che, in materia di stampa, consente all'*author*, al *publisher* e all'*editor*, di non rivelare la fonte dell'informazione.

Sulla base del par. 1 del *Defamation Act*[198], il provider può sempre ricorrere alla difesa della *innocence dissemination* che lo equipara ad un semplice fornitore di informazioni purché non sia a conoscenza del messaggio offensivo e abbia sempre mantenuto un comportamento diligente.

Il legislatore con il *Defamation Act* ha dunque cristallizzato il principio di Common law conosciuto come "*innocent dissemination defence*", il quale, è bene chiarire,

---

[197] M. DE CATA, *La responsabilità civile dell'Internet service provider*, cit., p. 134 ss.

[198] Il Par. 1 (3) dell'*UK Defamation Act* stabilisce che "*a person shall not be considered the author, editor or publisher of a statement if he is only involved (a) in printing, producing, distributing or selling printed material containing the statement; (b) in processing, making copies of, distributing, exhibiting or selling a film or sound recording (as defined in Part I of the Copyright, Designs and Patents Act 1988) containing the statement; (c) in processing, making copies of, distributing or selling any electronic medium in or which the statement is recorded, or in operating or providing any equipment, system or service by means of which the statement is retrieved, copied, distributed or made available in electronic form ; (d) as the broadcaster of a live programme containing the statement in circumstances in which he has no effective control over the maker of the statement; (e) as the operator of or provider of access to a communications system by means of which the statement is transmitted, or made available by a person over whom he has no effective control* ".

nell'elaborazione giurisprudenziale non ha mai assunto i caratteri di un'immunità assoluta[199].

Da questa analisi emerge quanto il modello inglese, sebbene non abbia raggiunto i livelli di elaborazione di quello statunitense e non abbia in alcun modo influenzato il legislatore eurocomunitario, aveva già elaborato il principio dell'assenza dell'obbligo dell'intermediario di servizi telematici di vigilanza preventiva sul materiale immesso in rete dagli users nonché il principio della colpa per l'imputazione della responsabilità al provider per omessa rimozione del materiale illecito.

La direttiva sul commercio elettronico è stata recepita nell'ambito delle *Electronic Commerce Regulations* del 2002. In sede di trasposizione è stata inserita, rispetto alla direttiva 2000/31, un'importante disposizione, rubricata "*notice for the purposes of actual knowledge",* in cui, sebbene non si articoli puntualmente una procedura formale di notifica e rimozione, si forniscono delle linee guida indirizzate al giudice che debba valutare la sussistenza, in capo agli intermediari di memorizzazione, *dell'actual knowledge of unlawful activity or information*.

Quindi il giudice inglese potrà tener conto di *all matters which appear to it in the particular circumstances to be relevant*.

Per tali ragioni assume particolare rilevanza l'accuratezza della segnalazione inviata dal danneggiato al fine di sollecitare la rimozione delle informazioni illecite.

Affinché la *notice* possa sortire i propri effetti e convincere il giudice della sussistenza in capo al provider di un'*actual knowledge,* il giudice dovrà valutare, tra le altre cose, se essa sia corredata delle indicazioni relative al nome ed ai contatti del mittente, della posizione delle informazioni controverse e, soprattutto, dei dettagli circa la natura illecita dell'attività o delle informazioni segnalate[200].

L'applicazione più nota dello schema previsto dalle *Regulations* del 2002 si è avuta con il caso *Davison v. Habeeb*, i cui occorreva decidere, alla stregua della pronuncia *Godfrey v. Demon,* le sorti di un intermediario informatico la cui responsabilità era da rinvenirsi nella circostanza che questi non aveva fatto seguito alcuno alla segnalazione di parte i cui si indicava un dato diffamatorio da rimuovere[201].

---

[199] R. KIDNER, *Casebook on Torts*, Oxford, 2012, p. 352 ss.

[200] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., pp. 176 e 177.

[201] *Davison v Habeeb & Ors* [2011] EWHC 3031 (QB).

Si è ritenuto il provider responsabile perché la mancata rimozione era valsa a cristallizzare una responsabilità per acquiescenza.

Un rilassamento della regola secondo cui il danneggiato, ai sensi della Regulation 22, dovrebbe essere in grado di dimostrare all'intermediario l'esistenza di u fatto illecito reale e concreto si ha, infatti, ove la condotta delittuosa appaia facilmente evincibile. In questi casi la giurisprudenza si accontenta anche di un reclamo credibile.

Ciò che emerge dalla trattazione del sistema inglese è che all'intermediario è richiesto di adottare la decisione rispetto a ciascuna controversia, secondo standard di diligenza, indipendentemente dal fatto che il modello decisionale adottato dalle Corti sia incentrato sui principi di Common law, sulla eccezione prevista dal *Defamation Act* o sulla *Regulation*[202].

Il grado di discrezionalità dell'intermediario si accresce all'aumentare della complessità della decisione da adottare.

Nei casi in cui illecito sia manifesto si richiede che la segnalazione indichi soltanto un reclamo credibile mentre nei casi invece più difficili è necessario che il danneggiato dia la possibilità all'intermediario di verificare l'esistenza di un fatto illecito reale e concreto[203].

Per mezzo del Defamation act nel 2013 viene attuata nel Regno Unita una riforma volta a perimetrare ulteriormente la disciplina degli spazi digitali.

Il nuovo impianto normativo, che non abroga la precedente riforma del 1996 ma si affianca ad essa, si basa su una procedura di segnalazione e rimozione in contraddittorio dei contenuti illeciti immessi in rete e sulla premessa secondo cui l'intermediario possa moderare i dati presenti sui propri spazi digitali senza, perciò, perdere lo scudo protettivo, fatto salvo il caso del dolo.

Le *rationes* che hanno mosso la riforma sono da rinvenirsi nell'intenzione di riformare il *law of defamation*, di assicurare una tutela più marcata alla libertà di espressione in ambiente digitale e di garantire allo stesso tempo rimedi efficaci e rapidi alle vittime dei contenuti diffamatori, cercando di porre un freno alla possibilità per l'intermediario di incorrere in errori, alla probabilità che egli adotti delle strategie di moderazione dei contenuti sovra-censorie ma anche alle incertezze suscitate mei danneggiati sulla spettanza di prospettive rimediali da far valere contro l'intermediario.

---

[202] M. TURNER, *Libel on line: the U. K. Perspective*, in *Comp. L. Ass. Bull.*, 1995, p. 12 ss.

[203] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. 183.

Il Regolamento quindi, come spiegato dall'allora ministro della Giustizia Lord McNally, mira a "difendere la libertà di parola dando a coloro che sono diffamati una ragionevole opportunità di riparazione" e costituisce " un tentativo di garantire che il denunciante e il manifesto siano portati faccia a faccia, per così dire, il più facilmente possibile".

La sezione 5 crea una nuova difesa per un'azione per diffamazione intentata contro il gestore di un sito web che ospita contenuti generati dagli utenti.

Per beneficiare della difesa, l'operatore deve attenersi a un processo prescritto dal Regolamento al ricevimento di un avviso di reclamo relativo a materiale presumibilmente diffamatorio che è stato pubblicato sul sito Web.

La procedura ruota intorno ad una serie di comunicazioni intercorrenti in vari momenti e a diversi fini tra danneggiato (*claimant*), intermediario (*website operator*) e fornitore del contenuto (*poster*).

La parte più importante è la *notice of compliance* del danneggiato indirizzata all'intermediario. Si tratta di un avviso di reclamo che:

a) specifica il nome del denunciante,

b) espone la dichiarazione in questione e spieghi perché è diffamatoria nei confronti del denunciante,

c) specifica dove sul sito web è stata pubblicata la dichiarazione, e

d) contiene altre informazioni che possono essere specificate nei regolamenti[204].

---

[204] *Section 5 - Operators of websites-*
1)This section applies where an action for defamation is brought against the operator of a website in respect of a statement posted on the website.
2)It is a defence for the operator to show that it was not the operator who posted the statement on the website.
3)The defence is defeated if the claimant shows that—
(a)it was not possible for the claimant to identify the person who posted the statement,
(b)the claimant gave the operator a notice of complaint in relation to the statement, and
(c)the operator failed to respond to the notice of complaint in accordance with any provision contained in regulations.
4)For the purposes of subsection (3)(a), it is possible for a claimant to "identify" a person only if the claimant has sufficient information to bring proceedings against the person.
5)Regulations may—
(a)make provision as to the action required to be taken by an operator of a website in response to a notice of complaint (which may in particular include action relating to the identity or contact details of the person who posted the statement and action relating to its removal);
(b)make provision specifying a time limit for the taking of any such action;
(c)make provision conferring on the court a discretion to treat action taken after the expiry of a time limit as having been taken before the expiry;
(d)make any other provision for the purposes of this section.
6)Subject to any provision made by virtue of subsection (7), a notice of complaint is a notice which—
(a)specifies the complainant's name,
(b)sets out the statement concerned and explains why it is defamatory of the complainant,
(c)specifies where on the website the statement was posted, and
(d)contains such other information as may be specified in regulations.

Entro le 48h dalla ricezione, l'intermediario è tenuto ad inoltrare al fornitore la copia del contenuto della segnalazione ricevuta, corredata dall'avviso che le affermazioni controverse potrebbero essere rimosse dal sito a meno che non riceva risposta scritta delle azioni da intraprendere.

Nel caso in cui l'intermediario non abbia la possibilità di contattare il fornitore del contenuto, al fine di mantenere l'esimente, dovrà rimuovere quanto segnalato entro un tempo predefinito.

La mancata attivazione dell'intermediario secondo quanto previsto dal disposto legislativo (a seguito della *notice of compliant*) comporta, ove il danneggiato non sia già in possesso delle informazioni relative all'identità dell'autore diretto dell'illecito, la perdita per il provider della disciplina di favore.

La riforma del 2013 permette dunque di rimodulare i confini tra libertà di espressione e tutela della reputazione del singolo: i bilanciamenti sono stati effettuati a monte dal legislatore e l'intermediario li deve solo mettere in pratica secondo le linee guida del suo agire prescritte in maniera dettagliatissima.

Il meccanismo, articolato su una serie di segnalazioni e controsegnalazioni, "offre all'intermediario la possibilità di rimettere la soluzione delle difficili questioni sottese ad una richiesta di rimozione direttamente alle parti interessate dalla vicenda: il presunto danneggiante ed il presunto danneggiato"[205].

La risposta dell'intermediario è dunque non solo guidata ma anche resa coralmente mediante l'opportunità di replicare, chiarire e correggere da parte di chi ha immesso in rete determinate informazioni.

Secondo autorevoli studiosi, la legge inglese del 2013 potrebbe costituire un possibile modello per la riforma della sezione 230 *CDA* perché, rispetto alla sezione 512 *DMCA* ed

7)Regulations may make provision about the circumstances in which a notice which is not a notice of complaint is to be treated as a notice of complaint for the purposes of this section or any provision made under it.
8)Regulations under this section—
(a)may make different provision for different circumstances;
(b)are to be made by statutory instrument.
9)A statutory instrument containing regulations under this section may not be made unless a draft of the instrument has been laid before, and approved by a resolution of, each House of Parliament.
10)In this section "regulations" means regulations made by the Secretary of State.
11)The defence under this section is defeated if the claimant shows that the operator of the website has acted with malice in relation to the posting of the statement concerned.
12)The defence under this section is not defeated by reason only of the fact that the operator of the website moderates the statements posted on it by others.

[205] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. 188.

alla sua procedura incentrata sul *simple fact of the notice*, il *Defamation Act* sarebbe anche compatibile con il Primo Emendamento[206].

5. La responsabilità del provider nell' esperienza francese

Dal punto di vista sostanziale, l'esperienza francese mostra il graduale passaggio da una posizione favorevole alla responsabilità oggettiva del provider ad un'altra rigorosamente legata al criterio di imputazione della colpa nel giudizio di responsabilità dell'intermediario di servizi telematici.

La questione della responsabilità del provider si pone all'attenzione della giurisprudenza transalpina con il caso *Hallyday*[207].

In un sito web, senza il consenso dell'interessata, erano state immesse da un user anonimo foto osé di un'ex modella, Estelle Lefbure, nota al grande pubblico soprattutto per aver sposato il figlio di Johnny Hallyday, celebre cantante.

L'ex modella aveva adito il *Tribunal de Grande Istance* di Parigi in sede cautelare, chiedendo l'oscuramento del sito contenente le fotografie in questione e la concessione di una provvisionale sul risarcimento dei danni.

Secondo l'ex modella, il provider era responsabile a titolo di colpa per non aver vigilato sul materiale immesso dal suo user e per non aver registrato le generalità dell'autore diretto dell'illecito che era così riuscito a rimanere anonimo ed impunito o, in alternativa, per aver violato le norme sulla stampa[208]che prevedono un regime di responsabilità oggettiva dell'editore[209] e del direttore della pubblicazione per gli illeciti compiuti a mezzo della stessa.

Per contro, il provider sosteneva che nessun addebito potesse essergli mosso in quanto non gravava su di lui alcun obbligo di vigilanza preventivo sui dati immessi in Rete dagli utenti, aveva sollecitamente provveduto a rimuovere i materiali illeciti all'atto stesso della notifica del ricorso da parte dell'ex modella, la comunicazione in forma anonima era di per sé ammessa dalla legge ed, infine, in quanto sito web non era assimilabile ad una testata giornalistica, con conseguente inapplicabilità della severa normativa sulla stampa.

---

[206] A. BENNIS, *Realism about Remedies and the Need for a CDA Takedown: A Comparative Analysis of 230 CDA and the U. K. Defamation Act 2013,* in *27 Fla. J. Int'l L.*, 2015, p. 316.

[207] Trib. gr. inst. Parigi, 10 luglio 1997, disponibile all'URL: *http://www.legalis.net*. In merito a questa pronuncia, v., tra gli altri, A. VOITURIEZ, *Problématique de la responsabilité du fournisseur d'accès sur internet,* in *Gaz. Pal.*, 18-20 avril 1999, p. 22 ss.

[208] Legge del 23 giugno 1982 e del 30 settembre 1986.

[209] La c. d. *"responsabilité en cascade".* M. DE CATA, *La responsabilità civile dell'Internet service provider*, cit., p.136 ss.

Nel ritenere sussistenti i presupposti per la concessione dell'invocata tutela cautelare, il *Tribunal de Grande Istance* non si era però pronunciato sulla domanda di provvisionale, rinviando le parti al giudice del merito per il risarcimento dei danni.

Investita della questione in sede di reclamo, la Corte d'Appello di Parigi ha accolto integralmente le domande dell'ex modella[210].

La Corte d'Appello, infatti, condannando il provider al pagamento della richiesta di provvisionale, ha affermato che: "Il provider che, nell'offrire ospitalità sul sito da lui gestito e creato, consente a chiunque di diffondere segni, scritti, immagini, suoni e messaggi, sprovvisti del carattere di corrispondenza privata, eccede manifestamente il ruolo tecnico di semplice trasmettitore di informazioni e deve, dunque, assumere verso i terzi le conseguenze di tale attività".

La Corte d'Appello dunque, pur accogliendo l'osservazione dell'inapplicabilità della normativa sulla stampa con conseguente esclusione della *responsabilitè en cascade* sull'editore a causa delle differenze strutturali tra giornali, caratterizzati da una struttura gerarchica di controllo sulle notizie pubblicate, ed Internet, acefala e decentralizzata per definizione, ha fondato l'affermazione di responsabilità del provider sul fatto stesso della predisposizione di un servizio di trasmissione non meramente passivo utilizzato da terzi , anche in forma anonima, per l'immissione in rete di contenuti illeciti.

Basando la condanna sulla natura del servizio svolto dal provider, la Corte parigina disattendeva però il rilievo, ormai comunemente accertato, dall'impossibilità per i providers di effettuare in via preventiva il controllo sul materiale immesso in Rete dagli users, adottando così surrettiziamente un criterio di responsabilità oggettivo.

Allo stato della tecnica, stante l'inaffidabilità dei sistemi automatici di controllo che eseguono un filtraggio indiscriminato *par hasard*, i providers dovrebbero controllare milioni di informazioni e ripetere l'operazione di continuo, dato che i materiali immersi in Rete sono modificabili in ogni momento dagli users. In queste condizioni risulterebbe pertanto inesigibile anche per il diritto francese, perché di impossibile adempimento, la vigilanza preventiva di cui si volesse gravare il provider.

La sentenza "*Hallyday*" ha suscitato le accese proteste dei providers e ha prodotto evidenti effetti di *overdeterrence*. Infatti, all'indomani stesso della pubblicazione della sentenza, i maggiori providers francesi oscurarono oltre cinquemila siti sospetti per timore di essere ritenuti responsabili dei contenuti ospitati.

[210] G.M. RICCIO, *La responsabilità civile degli Internet providers*, cit., p. 149 ss.

Il criterio di imputazione di responsabilità adottato nel caso "*Hallyday*", oltre che censurabile, si differenziava radicalmente da quello a carattere colposo, scelto dagli altri ordinamenti occidentali, rischiando così di penalizzare i providers francesi anche a livello di competizione nel mercato globale.

L'impasse creato dal caso "*Hallyday*" ha dato impulso a diverse proposte di legge in favore dei providers e, in particolare, la proposta *Bloche*.

Tale iniziativa legislativa prevedeva l'esonero di responsabilità di tutti i soggetti, pubblici o privati che, a titolo oneroso o gratuito, fornivano accesso ai servizi della Rete, salvo che essi avessero contribuito alla produzione e/o alla creazione del materiale diffuso o non avessero ottemperato all'ordine dell'autorità di rendere impossibile l'accesso ai materiali illeciti.

Per andare esenti da responsabilità gli intermediari avrebbero dovuto fornire le generalità dei loro users all'autorità giudiziaria che ne avesse fatto richiesta.

La proposta *Bloche*, nel risolvere in modo tranchant la questione della responsabilità del provider, non articolava sufficientemente la disciplina normativa in rapporto alle diverse tipologia di intermediari, ed in particolare a quella dei *fournisseurs d'access* (fornitori d'accesso) e *fournisseurs d'hébergement* (fornitori di contenuto). Questi ultimi erano *tout court* equiparati ai semplici fornitori di accesso[211].

Nel caso *"T.I. Communication"* un provider aveva ospitato un sito web in cui erano state riprodotte e diffuse illecitamente da un user opere protette dal diritto d'autore.

Il tribunale di Commercio di Parigi ha escluso la responsabilità del provider sulla base del rilievo che l'obbligo di vigilanza preventiva non sussisteva in capo al fornitore di ospitalità, in quanto il controllo del materiale immesso in rete non era previsto da alcuna norma specifica, né, in base al criterio di imputazione della colpa, poteva considerarsi esigibile da parte del provider.

Il caso *Lacoste*, con la pronuncia del *Tribunal de Grande Istance de Nanterre* dell'8 dicembre 1999, segnò l'avvio di un nuovo indirizzo giurisprudenziale.

Il caso era del tutto simile, nello svolgimento dei fatti, a quello *Hallyday*: su un sito web erano state diffuse immagini osé di una ex modella, senza che questa avesse prestato il proprio consenso.

Anche in questo caso il provider non aveva provveduto a registrare le generalità dell'user autore dell'illecito che, così, era riuscito a rimanere anonimo.

---

[211] G.M. RICCIO, *La responsabilità civile degli Internet providers*, cit., p. 224 ss.; M. DE CATA, *La responsabilità civile dell'Internet service provider*, cit., p.138 ss.

Il Tribunale nanterrino, premessa l'opportuna distinzione tra le tipologia di provider in relazione al tipo di servizio prestato, ricondusse la questione della responsabilità degli intermediari di servizio telematico nell'ambito del criterio di imputazione per colpa.

Il provider, *fournisseur d'hébergement*, è stato condannato per la negligente omissione della registrazione al momento della conclusione del contratto delle generalità degli user autore dell'illecito[212].

Secondo la Corte, infatti, il provider con tale omissione, trascurando le norme di diligenza cui avrebbe dovuto attenersi il buon professionista ex art. 1382/1383 Code Civil, aveva agevolato, con nesso eziologico diretto, il compimento dell'attività illecita e la conseguente verificazione dell'evento dannoso.

Il Tribunale *de Ile-de-France*, infatti, ha qualificato l'obbligo del provider come obbligazione di mezzi, da assolvere con la diligenza del "*bon professionel*".

Pertanto, pur non potendosi configurare a carico del provider l'obbligo di vigilanza sui materiali immessi sul server, non poteva escludersi che sullo stesso gravassero altri obblighi imposti dalla diligenza professionale.

Se la responsabilità del provider fosse stata ricondotta correttamente al criterio di imputazione della colpa, meno condivisibile sarebbe apparito invece l'espressa affermazione dell'obbligo in capo all'intermediario di servizi di registrare e rivelare l'identità dei suoi utenti.

La tutela della privacy dei navigatori veniva così sbrigativamente sacrificata per la semplice presenza di un fatto illecito.

Il criterio di imputazione della colpa in materia di responsabilità del provider, così come delineato dal tribunale di *Nanterre*, è stato successivamente accolto anche da una successiva sentenza della Corte di *Versailles,* la quale ha ribadito che, pur non gravando l'obbligo generale di vigilanza sul provider, non si può ritenere escluso in capo allo stesso quello dell'adozione di altri "*moyens raissonnables"*.

L'affermazione dell'obbligo del provider di adottare, sia pure in assenza di un dovere di controllo preventivo, ragionevoli misure di diligenza ha suscitato le reazioni della dottrina che ha prospettato il pericolo che da una previsione indeterminata e generica di obblighi non ben specificati, ritenuti esigibili in base al principio di diligenza professionale, potessero

[212] G.M. RICCIO, *La responsabilità del provider nell'esperienza francese: il caso Hallyday*, in *Dir. inf.*, 1999, p. 929; A. CAPRIOLI, *Responsabilité du fournisseur d'hébergement*, in *Droit & Patrimoine*, 1999, p. 107 ss. Anche la dottrina italiana si è occupata del caso, v. F. DI CIOMMO, *Internet, diritti della personalità e responsabilità aquiliana del provider*, in *Danno e resp.*, 1999, p. 759 ss.

essere introdotte dalla giurisprudenza fattispecie di responsabilità non collegate all'elemento della colpa.

Sembra tuttavia più corretto ritenere che il tribunale di Nanterre, più che aprire spiragli verso futuri eventuali *revirement* giurisprudenziali favorevoli al criterio di responsabilità oggettiva, non abbia escluso che in capo al provider, in base al principio di diligenza professionale, possono essere individuati, anche a seguito del progresso tecnico, obblighi di prestazione utili a prevenire la commissione dell'illecito o a ridurre gli effetti dannosi.

La stessa direttiva 2000/31/CE, d'altra parte, pur negando espressamente la sussistenza in capo al provider dell'obbligo generale di vigilanza (art.15), si è comunque riservata (art.21), tenuto conto dell'evoluzione della tecnologia di rendere doverose per l'intermediario nuove prestazioni dirette a prevenire illeciti.

I timori espressi a proposto del caso *Lacoste* sul pericolo dell'introduzione surrettizia di forme di responsabilità oggettiva a carico dei providers da parte della giurisprudenza sembrarono prendere corpo nel caso *Yahoo! France*. Su un sito, collocato negli USA gestito da un provider statunitense, venivano pubblicizzati ed offerti in vendita oggetti inneggianti all'antisemitismo ed apologetici dei crimini nazisti. A tale sito era possibile connettersi attraverso un link compreso tra i risultati di un motore di ricerca gestito da un provider francese *Yahoo! France.*

Alcune associazioni antirazziste francesi, non potendo intervenire sul contenuto del sito, in quanto l'ordinamento degli USA dove era collocato il server, assicura tutela assoluta alla libertà di pensiero e parola, avevano chiesto all'Autorità giudiziaria francese di ordinare a *Yahoo! France* di impedire ai cittadini francesi l'accesso al sito denunziato e predisporre appositi "disclaimers" che avvisassero gli utenti dell'illegalità e dell'immoralità dei suoi contenuti. Nell'ordinamento francese, infatti, l'apologia del nazismo non solo costituisce reato ma è valutata dalla coscienza sociale come fatto particolarmente abietto anche a causa del sentimento patriottico che associa il nazismo all'occupazione della Francia da parte dei tedeschi nell'ultimo conflitto mondiale[213].

Il *Tribunal de Grande Istance* di Parigi, disattendendo l'argomentazione della difesa basata su accurate relazioni di prestigiosi periti secondo i quali i sistemi automatici diretti ad individuare la nazionalità o il punto spaziale di connessione alla rete degli utenti erano inaffidabili, ha ordinato al provider di adottare le misure necessarie ad impedire l'accesso a cittadini francesi o dalla Francia al sito denunciato con la conseguenza che, in caso di

[213] M. DE CATA, *La responsabilità civile dell'Internet service provider*, cit., p.142 ss.

insuccesso (preannunciato) dei sistemi di bloccaggio, l'intermediario sarebbe stato ritenuto responsabile.

In realtà la pronuncia del *Tribunal de Grande Istance* di Parigi, più che segnare il revirement della giurisprudenza verso forme di responsabilità oggettiva, è stato più verosimilmente frutto di un'approssimativa valutazione delle risultanze istruttorie.

In casi successivi e del tutto identici nello svolgimento dei fatti a quello di *Yahoo! France*, lo stesso *Tribunal de Grande Instance* di *Versailles* ha precisato che la responsabilità del provider dovesse essere ricondotta nell'ambito della *faute* e si è limitato a raccomandare al provider l'uso delle misure a sua discrezione utili a prevenire la connessione a siti apologetici del nazismo da parte di cittadini francesi o dalla Francia.

Se alla luce di un'approfondita valutazione dello Stato della tecnica, le misure di filtraggio dirette ad individuare la nazionalità o il punto di connessione degli utenti non erano efficienti, e dunque la disabilitazione dell'accesso da parte dei cittadini francesi o dalla Francia non erano esigibili, tale circostanza di per sé, in base al principio della diligenza professionale, non esonera i gestori dei motori di ricerca dall'adottare le misure precauzionali utili, con una singolare rimessione della loro individuazione al provider, ritenuto in virtù delle sue competenze soggetto più idoneo del giudice nella scelta.

Sulla scorta dei risultati maturati dalla giurisprudenza, il legislatore transalpino è infine intervenuto a regolamentare il tema della responsabilità del provider con la legge 1° agosto 2000 (Loi n.719/2000).

La *Loi* n.719/2000 non costituisce attuazione della Direttiva 2000/31/CE.

Il contemporaneo svolgersi dei lavori preparatori tra la legge francese e la Direttiva comunitaria ha tuttavia determinato la similitudine sotto diversi aspetti delle due norme.

Infatti, al pari della Direttiva 2000/31/CE, la legge 1° agosto 2000 ha distinto nella categoria dei providers tra fornitori di accesso (*fournisseurs d'access*), di ospitalità (*fournisseurs d'hébergement)* e di contenuto (*fournisseurs de contenus*) differenziando il regime di responsabilità a seconda del tipo di servizio svolto.

Al pari della Direttiva 2000/31/CE e del TDG tedesco, la legge francese ha adottato la tecnica legislativa della definizione in negativo delle condizioni di esonero da responsabilità degli intermediari di servizi telematici.

Secondo la legge del 1° agosto 2000 i fornitori di accesso sono sempre irresponsabili per i contenuti veicolati, purché si siano astenuti da ogni contatto qualificato con essi, mentre i fornitori di contenuto sono responsabili secondo i principi generali.

Per l'attività di hosting la legge francese ha previsto la responsabilità del *fournisseurs* d'hébergement che, essendo a conoscenza dell'illiceità dell'informazione ospitata, non abbia diligentemente bloccato l'accesso alla stessa.

Un intervento del *Conseil Costitutionnel* ha ristretto il grado di diligenza esigibile nel giudizio di responsabilità sottraendo al provider in quanto soggetto privo di funzioni istituzionali e non perito di diritto il compito di valutare la liceità del materiale ospitato: la responsabilità dell'intermediario è stata infatti limitata all'ipotesi di inottemperanza all'ordine di disabilitazione all'accesso da parte dell'autorità giudiziaria.

Si rileva che la medesima questione si è riproposta all'indomani della promulgazione della legge 21 giugno 2004 (*Loi pour le confiance dans l'economie numérique*), norma che ha recepito la direttiva 2000/31/ CE, c.d. "Direttiva sul commercio elettronico".

Nuovamente, sulla base dei principi consolidati, anche alla luce di una nuova pronuncia del *Conseil Costitutionnel*, dottrina e giurisprudenza hanno ritenuto responsabile il provider solo nel caso non avesse ottemperato all'ordine dell'autorità giudiziaria o non avesse rimosso il materiale dal contenuto manifestamente illecito.

Il legislatore francese, a pari di quello europeo, non ha disciplinato la questione, già peraltro ampiamente risolta dalla giurisprudenza nazionale, della responsabilità del provider per la gestione dei motori di ricerca, ma la legge 1° agosto 2000, a differenza della Direttiva 2000/31/CE, ha regolamentato la problematica dell'anonimato in Rete.

Ai sensi della legge 1° agosto 2000 l'anonimato del navigatore è tutelato con il limite generale della necessità di svolgimento di indagini dell'autorità giudiziaria in caso di gravi illeciti.

Il provider, tuttavia, è tenuto non solo a registrare le generalità dei suoi clienti ma anche a conservare le tracce della loro attività in Internet, mettendo tali dati a disposizione dell'autorità giudiziaria che ne faccia richiesta nell'ambito di attività di indagine relative a fattispecie penalmente rilevanti.

Puntuale è la configurazione di un sistema di segnalazione e rimozione nella legge di recepimento francese.

Il riferimento è in particolare all'art. 6.I.2 della legge sul "*régime dérogatoire de responsabilité*", che riproduce quella parte dell'art. 14 della direttiva 2000/31/CE che richiede la rimozione dei contenuti da parte del prestatore intermedio che sia al corrente del fatto che l'attività o l'informazione è illecita o di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione, e all' art. 6.I.5 che invece guarda alla diversa

domanda inerente al momento a partire dal quale possa essere presunta in campo sull'intermediario l'effettiva "*connaissance des faits litigieux*".

La conoscenza dei fatti contestati si presume in capo all'*hébergeur,* ove sia stata fornita una notifica formale. La procedura vale per qualunque tipo di informazione a patto che sia corredata da analitici elementi:

- l'identità del richiedente la rimozione
- la descrizione dei fatti contestati
- l'esatta localizzazione dei contenuti da rimuovere
- i motivi per cui essi devono essere rimossi
- la menzione delle disposizioni di legge violate
- copia della corrispondenza indirizzata all'autore diretto delle informazioni o delle attività contestate o una dichiarazione che attesto che quest'ultimo non potesse essere contattato[214].

Non mancano nella normativa francese le sanzioni penali per chi abbia rappresentato dolosamente che alcuni contenuti fossero illeciti e sa rimuovere.

Gli intermediari dovranno altresì predisporre un dispositivo facilmente accessibile che consenta a chiunque di segnalare tutta una serie di forme di espressione vietate, quali quelle relative all'apologia di crimini contro l'umanità, a contenuti diffamatori, all'incitamento alla commissione di atti di terrorismo, all'odio razziale o di genere, alla violenza contro le donne, alla pedopornografia, alle violazioni della proprietà industriale o intellettuale[215].

Nell'elaborazione giurisprudenziale, tuttavia, l'art. 6.I.5 è stato per lungo tempo rimpiazzato dalla portata generale applicativa dell'art. 6.I.2, incentrato sul requisito della "*effective connaissance*". La procedura formale di segnalazione ha infatti trovato applicazione solo in tempi recenti[216].

A lungo le Corti di primo e secondo grado hanno riconosciuto la valenza della procedura di notifica e segnalazione solo sul piano probatorio.

---

[214] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto,* cit., p. 151 ss.

[215] C. JESSERAND, *Régime français de la responsabilité des intermédiaires technique,* in *25 Les Cahiers de propriété intellectuelle,* 2013, p. 1135 ss.; P. SAMMARCO, *La posizione dell'intermediario tra l'estraneità ai contenuti trasmessi e l'effettiva conoscenza dell'illecito: un'analisi comparata tra Spagna, Francia e regolamentazione comunitaria*, in *Dir. Inf.*, 2017, p. 285 ss.

[216] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto,* cit., p. 161 ss.

Per la giurisprudenza si sarebbe trattato infatti di una "*procédure facultative*", intesa prevalentemente quale meccanismo processuale volto a fornire un supporto probatorio a chi avesse voluto far valere in giudizio i propri diritti anche nei confronti dell'intermediario[217].
Anche il *Conseil Costitutionelle* ha confermato la priorità assegnata nel derimere i conflitti in rete all'art. 6. I.2[218].
Il *Conseil Costitutionelle* ha ritenuto infatti, in sede di giudizio preventivo di legittimità, che per salvaguardare la libertà di espressione nelle comunicazioni digitali occorresse attribuire a tale norma un'interpretazione restrittiva, dovendosi escludere ogni responsabilità dell'intermediario per la mancata rimozione, salvo nel caso eccezionale in cui l'illiceità delle informazioni segnalate fosse apparsa manifesta o se la disabilitazione dell'accesso fosse stata ordinata dal giudice.
Tuttavia, la prassi giurisprudenziale di merito ha disatteso l'obiettivo previsto dalla pronuncia costituzionale e ha tentato di innalzare il livello delle responsabilità degli intermediari della rete imponendo loro l'adozione "di doveri di diligenza" volti a tutelare sia la riservatezza che la reputazione dei singoli e i diritti di proprietà intellettuale[219].
La giurisprudenza francese è passata quindi da un approccio reattivo, volto a dar rilievo ai doveri di attivazione dell'intermediario a seguito di segnalazioni di parte, ad un approccio decisionale di tipo proattivo, incentrato su oneri di controllo gravanti in capo all'intermediario in relazione ai servizi prestati.
Tale indirizzo giurisprudenziale ha seguito tre strade diverse, come ricordato da autorevoli studiosi della materia[220]:

1) Ritenere il fornitore del servizio non un prestatore intermedio ma l'editore di contenuti pubblicati da terzi.

---

[217] N. VAN EIJK-T. VAN ENGERS-W. ABEL-C. WIERSMA,-C. JESSERAND, *Moving Towards Balance: a Study into Duties of Care on the Internet*, in *Amsterdam Law School Legal Studies Research Paper Series*, 2012, p. 58 ss.; R. HARDOUIN, *La jurisprudence, les textes, et la responsabilité des hébergeurs*, 2008, p. 2 ss.
[218] N. 2004-496 DC, del 10 giugno 2004. H. OBERDORFF, *Le Conseil costitutionelle et l'ordre juridique communautaire: coopération et controle (à propos de la décision du Conseil costitutionelle n. 2004-496 du 10 juin 2004 relative à la loi pour la confiance dand l'économie numérique)*, in *Revue dr. Publ. Sc. Pol.*, 2004, p. 869 ss.; S. STALLA-BOURDILLON, *The flip side of ISP's liability regimes: The ambiguous protection of fundamental rights and liberties in private digital spaces*, in *26 Computer Law & Security Review*, 2010, p. 492 ss.
[219] J. DE BEER-D.C. CLEMMER, *Global Trends in Online Copyright Enforcement: a Non-Neutral Role for Network Intermediaries?*, in *49 Jurimetrics*, 2009, p. 396 ss.; C. ANGELOPOULOS, *Filtering the Internet for Copyrighted Content in Europe*, in *Amsterdam Law School Legal Studies Research Paper No*., 2012, p. 1 ss. Sul punto cfr. anche le sentenze del *Tribunal de Grande Istance* di Nanterre del 28 febbraio 2008, casi *Dehan c. Duperri* e *Oliver c. Aadsoft Com*.
[220] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. 162 ss.

Il riferimento è al caso *Lafesse c. MySpace*[221]*:* il Tribunal de Grande Istance di Parigi ha condannato la piattaforma *MySpace* al risarcimento del danno cagionato dal titolare dei diritti d'autore per non aver rimosso il falso profilo a lui attribuito da cui era possibile visualizzare le sue opera.

Nonostante l'assenza di una segnalazione di parte, per il Tribunale parigino il provider avrebbe dovuto rispondere del danno alla stregua delle ordinarie regole di responsabilità editoriale.

L'intermediario informatico aveva infatti fornito ai propri utenti una complessa piattaforma digitale che avrebbe consentito al suo gestore il conseguimento di importanti profitti grazie ai messaggi pubblicitari abbinati ai contenuti immessi in rete dagli utenti.

2) Condannare l'intermediario in relazione allo specifico disegno impresso alla propria piattaforma che avrebbe indotto l'intermediario al compimento di atti illeciti.

Esemplificativa a tal riguardo è la sentenza *Christian C., Nord Ouest Production c. Dailymotion*[222]. In tal caso si è pervenuti a risultati non proprio dissimili rispetto all'ipotesi considerata in precedenza: per il Tribunal de Grande Istance di Parigi la specifica architettura impressa alla piattaforma, che consisteva nell'ottimizzare la prestazione dei contenuti e nel fornire strumenti per la loro classificazione, aveva avuto l'effetto di agevolare la circolazione non autorizzata delle opere protette e di rendere poco credibile che l'obiettivo del servizio fosse solo quello di fornire mezzi tecnici per consentire a qualsiasi utente di condividere con i propri amici o con la comunità più ampia di Internet solo video amatoriali.

L'intermediario sarebbe stato genericamente consapevole del fatto che i propri spazi digitali fossero utilizzati per plagio e sarebbe stato tenuto ad adottare sistemi di controllo preventivi e soluzioni tecniche sufficienti ad evitare il perpetuarsi delle attività illecite indotte.

3) Considerare bastevole una previa richiesta di rimozione del contenuto immesso dall'internauta a radicare obblighi di controllo per prevenire violazioni future

In tale ipotesi, chiaro è il riferimento al caso *Zadig Proc. c. Google*[223], nel quale la piattaforma di condivisione video di Google è stata condannata per la reiterata pubblicazione da parte di terzi di un documentario cinematografico: in tali circostanze l'intermediario

[221] *Jean Yves Lafesse c. MySpace*, Tribunal de Grande Istance di Parigi, ordonnance de référé del 22 giugno 2007. R. HARDOUIN, *L'hébergeur et la publicité: la neutralité comme condition d'une coexistence*, *RLDI* 2010/62, p. 47 ss.

[222] *Christian C., Nord Ouest Production c. Dailymotion*, Tribunal de Grande Istance di Parigi, del 13 luglio 2007.

[223] *Zadig Proc. c. Google*, Tribunal de Grande Istance di Parigi, 19 ottobre 2007.

avrebbe dovuto attuare una sorveglianza mirata sull'opera indicata a seguito dell'invio della prima segnalazione forma, secondo quanto dispongono gli artt. 6.I.2 e 6.I.5.

Per il Tribunale di Parigi ogni caricamento successivo alla prima notifica non avrebbe costituito un nuovo fatto illecito che avrebbe richiesto un'ulteriore segnalazione ma dalla prima comunicazione sarebbe disceso l'obbligo per l'intermediario di mettere in atto tutti gli accorgimenti necessari e la predisposizione di soluzioni tecniche appropriate per prevenire violazioni future[224].

La volontà di radicare una responsabilità in capo all'intermediario per i contenuti caricati da terzi, con l'assunto che questi abbia maturato conoscenza di fatti e circostanze che lasciavano trasparire il carattere della manifesta illiceità o che non abbia adottato un controllo mirato all'esito di una segnalazione, è tale che fino al 2011 anche la giurisprudenza di merito di secondo grado ha condiviso l'impostazione di riconoscere in capo al provider degli obblighi di controllo finalizzati ad evitare che contenuti già rimossi potessero riapparire in rete, seppur caricati da nuovi utenti.

La *Cour d'Appel* di Parigi ha infatti respinto la tesi della piattaforma Google secondo cui le segnalazione inviate dai titolari dei diritti d'autore sarebbero valse esclusivamente per lo specifico contenuto caricato in una determinata posizione e da utenti individuati[225].

La procedura stabilita all'art. 6.I.5 ha ritrovato centralità solo con le pronunce della Corte di Cassazione.

Il riferimento è a due pronunce della Première chambre civile della *Cour de Cassation*, le quali nel 2011 hanno escluso la configurabilità di doveri di sorveglianza a priori dei prestatori intermedi sui propri spazi digitali e ha ricondotto gli obblighi di rimozione alla notifica prevista dall'art. 6.I.5, intesa come procedura vincolata nelle forme e nei contenuti[226].

La comunicazione sprovvista degli elementi richiesti non sarebbe sufficiente a dimostrare il requisito della conoscenza effettiva.

Sulla stessa scia si collocano le altre due pronunce della Corte di Cassazione francese rese il 12 luglio 2012[227].

---

[224] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. 163 ss.

[225] Il riferimento è alle pronunce rese il 14 gennaio 2011 *Google Inc. c. Compagnie des phares et balises*; *Google Inc. c. Bac Films, the Factory*; *Google Inc. c. Les Films de la Croisade, Goatworks Films* e quella resa nel caso *Google France et Google Inc., Auféminin.com c. H&K SARL, Andrè Rau*.

[226] *Cour de Cassation, Première chambre civile, arrêt* n. 165 del 17 febbraio 2011 (09-67.896).

[227] *Cour de Cassation, Première chambre civile, arrêt* n. 831 del 12 luglio 2012 (11-13.669).

Il *revirement* "giurisprudenziale della Suprema Corte francese, che pone al centro della scena la sola procedura formale di segnalazione intesa come *conditio sine qua non* della responsabilità dell'intermediario, è stato confermato, anche con riferimento alle misure di filtraggio adottate su base volontaria dagli operatori della rete con l'ausilio di algoritmi"[228].
Nel negare la configurabilità della responsabilità dell'intermediario per un obbligo e nel sottolineare come l'attore avrebbe dovuto indicare "*précisément la localisation de nouveaux fichiers litigieux, conformément à l'article 6.I.5 de la loi LCEN*", la Corte ha osservato che nulla modifica, con riferimento ai doveri di attivazione dell'intermediario, il fatto che questi abbia spontaneamente messo in opera un sistema di filtraggio dei contenuti.
Senza dubbio ci troviamo in presenza di una regola semplificatoria che adotta la giurisprudenza di legittimità francese.
Tale sistema è anche cautelato da garanzie procedurali contro la proposizione di richieste di rimozioni affrettate abusive e fraudolente, come testimonia l'aver presidiato con la minaccia della responsabilità penale la proposizione di segnalazioni formali false o abusive[229].

6. La responsabilità del provider nell' esperienza tedesca

Dopo i Paesi scandinavi, la Germania è uno degli Stati con il maggior numeri di utenti attivi su internet e per tale ragione la normativa circa la responsabilità civile degli internet service provider è particolarmente sviluppata rispetto a molti altri membri dell'Unione Europea.
La legge tedesca in materia di responsabilità dell'intermediario informatico ha costituito, con il DMCA statunitense, il modello cui si è ispirato il legislatore comunitario nell'emanare la Direttiva 2000/31.
L'ordinamento tedesco prevedeva già dal 1997 una legge a tutela dei prestatori di servizi: il *Teledienstegesetz* (TDG), contenuto *nell'Informations und Kommunikationsdienste*[230].

[228] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. 166.
[229] R. PETRUSO, *op. cit.*, p. 165 ss.
[230] Questa normativa ha visto un'applicazione importante in un decreto d'archiviazione emesso il 13 febbraio 1998 dalla Procura generale presso la Corte di Cassazione tedesca, relativamente ad un procedimento penale che vedeva coinvolti più provider come imputati d'agevolazione in istigazione e apologia di reati. Nel provvedimento, infatti, si ribadisce il fatto che "la condotta del provider consistente nell'apertura d'accessi ad Internet per gli utenti non è antigiuridica in sé ma anzi, alla luce delle esigenze dell'attuale società dell'informazione e in particolare anche della scienza, risulta socialmente diffusa e auspicata" ma implica un onere di controllo per i provider, che devono essere considerati come destinatari di determinati "doveri per la sicurezza del traffico". Questi doveri si concretizzano nel momento in cui diviene nota l'intenzione o il comportamento illecito, mentre non si può ipotizzare nessun controllo preventivo, che non risulterebbe né possibile né esigibile.

Tale norma, entrata in vigore il primo agosto 1997, risente a sua volta dei lavori preparatori del DMCA ma, a differenza di questo, il quale prevede una normativa circoscritta alla sola violazione del copyright, ricomprende ogni tipo di illecito.

Questo dato appare singolare se si considera che l'ordinamento tedesco adotta notoriamente il principio di tipicità dell'illecito, come previsto nei paragrafi 823 e ss. del BGB. Invero, il TMG non prevede un sistema atipico per gli illeciti commessi in Internet ma, in un sistema tipico che si basa sul modello del DMCA, prevede una serie di exemptions per tutti gli illeciti tipizzati nel BGB[231].

Il TDG al §5 (1) prende in considerazione la responsabilità dei fornitori di contenuto (content provider) ma la disciplina normativa avviene "*per relationem*" mediante il rinvio ai principi genarli sulla responsabilità per fatto proprio.

A differenza del DMCA, che distingue tra attività di *access* e quella di *caching*, il TDG accomuna i due servizi in un'unica previsione normativa.

Il § 5(3) menziona un principio generale di non responsabilità per i providers nel caso in cui il loro apporto sia limitato alla fornitura di un servizio di accesso.

A questa attività è equiparata quella dei soggetti che svolgono il c.d. *caching*, disciplinato dalla direttiva n. 31 del 2000 all'art. 13.

Per quel che riguarda il servizio di *hosting*, il §5(2) TDG sancisce l'irresponsabilità del provider a meno che non sussistano cumulativamente due condizioni:

a) Il provider sia a conoscenza dell'illiceità dell'informazione trasmessa
b) Il provider abbia la possibilità tecnica e la capacità di fermare l'accesso all'informazione.

Quanto al primo presupposto, non solo non grava sul provider alcun obbligo preventivo di vigilanza ma la conoscenza dell'illiceità del materiale deve essere accertata con criteri rigorosi, restando escluso che ad essa possa equipararsi la semplice conoscibilità[232].

Per quanto riguarda il secondo presupposto, ai fini dell'imputazione non è solo necessario che il provider abbia la possibilità di rimuovere le informazioni materialmente ospitate ma anche che la rimozione sia esigibile alla luce del principio di ragionevolezza e dunque l'illiceità del materiale denunciato deve essere evidente e non deve richiedere particolari

[231] G.M. RICCIO, *La responsabilità civile degli Internet providers,* cit., p. 185 ss.; G. SPLINDER - F. SCHUSTER, *Recht der elektronischen Medien: Kommentar,* in *GRUR,* 2011, 7 ss.
[232] C. PELZ, *Die strafrechtliche Verantwortlichkeit von Internet-Providern*, in *ZUM*, 1998, p. 534.

approfondimenti o accurate valutazioni giuridiche, non esigibili da un intermediario tecnico[233].

Le prime sentenze tedesche hanno mostrato qualche incertezza.

Infatti, tanto le sentenze della Corte di Monaco di Baviera del 1998 quanto quelle della Corte di Francoforte, dello stesso anno, riconoscono la responsabilità di un provider per aver consentito tramite un semplice link ad un sito in cui erano ospitati contenuti diffamatori per l'attore e per non essersi dissociato in modo sufficientemente chiaro dai contenuti dei siti cui aveva consentito l'accesso[234].

È con la sentenza del tribunale di Lubecca, successiva di pochi mesi, che iniziano ad essere respinte le richieste risarcitorie avanzate contro il provider, consolidando le posizioni dottrinarie oramai granitiche sull'interpretazione del TDG e dissipando dubbi giurisprudenziali.

La giurisprudenza tedesca ribadisce che sul provider non grava alcun obbligo di vigilanza preventiva e chiarisce che la responsabilità per il materiale illecito contenuto in un sito non potesse essere imputata all'intermediario per il solo fatto di aver stabilito un link[235].

Questo atto normativo è stato, successivamente, sostituito dalla legge *Telemediengesetz* (TMG) del 2007, che recepisce alcune delle norme previste dalla Direttiva 31/2000/CE.

Fra le norme introduttive di maggiore rilevanza, non si può non annoverare il § 3 TMG, il quale introduce la disposizione ex art. 3 della Direttiva comunitaria. In tale disposizione legislativa si prevede che tutti i fornitori di servizi stabiliti nella Repubblica Federale Tedesca devono rispettare la legge tedesca, anche se i servizi erogati sono offerti o forniti esclusivamente ad altri Paesi dell'Unione Europea. Non sono, invece, regolamentate le prestazioni erogate in Germania da provider stranieri. Inoltre, la legge tedesca prevede una differenza fra "contenuti propri" (*eigene Inhalt*) e "contenuti stranieri" (*fremde Inhalt*).

La loro definizione non è molto chiara e ha creato un ampio dibattito dottrinale. Parte di autorevole dottrina ritiene che il mero controllo passivo dei provider non sia idoneo a qualificare delle informazioni provenienti dall'estero come contenuti propri ma questo

---

[233] T.H. STOMER, *Online-recht: Rechtfragen im Internet*, Heidelberg, 1999, p. 216 ss.; F.A. KOCH, *Zivilrechtliche Anbienterhaftung fùr Inhalte in Komminikationetzen*, in *Computer und Recht*, 1997, p. 193 ss.

[234] Amtsgericht München, 28 maggio 1998, in *MultiMedia und Recht*, 1998, p. 429. Sulla vicenda giudiziaria, v., tra gli altri, G. GOUNALAKIS-L. RHODE, *Haftung des Host-Providers: ein neues Fehlurteil aus München?*, in *NJW*, 2000, p. 2168 ss.; T. HOEREN, *Ist Somm ein Krimineller?*, ivi, 1998, p. 2792 ss.; H. KÜHNE, *Strafbarkeit der Zugangsvermittlung von pornographischen Informationen im Internet*, ivi, 1999, p. 188 ss.; B. MAESKE, *Ermittlungen im Internet. Positionen und Dissonanzen: Rechtliche Konfliktpunkte bei der Bekämpfung von Kriminalität im Internet*, in *Kriminalistik*, 2000, p. 245 ss.; D. NATHRATH, *Criminal Liability of Internet Providers in Germany: Convinction of a CompuServe Executive*, in *Jour. of Internet Law*, 1998, p. 1 ss.

[235] M. DE CATA, *La responsabilità civile dell'internet service provider*, cit., pp. 147, 148 e 149.

dipende dal tipo di attività che il fornitore svolge sui dati trasmessi e memorizzati. È anche necessario determinare se l'intermediario abbia un controllo effettivo sui contenuti in oggetto e sugli utenti.

Secondo altra dottrina non importa se il provider possa controllare attivamente la trasmissione dei dati, bensì se questo svolga o meno tale attività: si considera che, solamente quando esso decida di interporsi nel trasferimento delle informazioni, si creino le basi per supporre che un contenuto straniero possa diventare proprio.

Viste tali considerazioni introduttive, bisogna tenere a mente che il TMG non contiene alcuna definizione di Internet provider.

Perciò questa si deve estrapolare dalle caratteristiche di ogni singola attività di fornitura di servizi in internet, le quali devono ricadere nei parametri previsti dal § 8, comma 1, TMG.

Proprio per tale situazione di incertezza, la dottrina ritiene necessaria una modifica alla legge, così da introdurre una definizione per ogni tipo di provider, includendo, tra l'altro, una specifica lista di diritti e di responsabilità, anziché una normativa generica e poco chiara.

La disciplina della responsabilità dei fornitori di servizi è regolata dai §§ 7 a 10 del TMG, che si fondano su un sistema di responsabilità limitata e disciplinano le medesime attività previste nella Direttiva comunitaria.

Il § 7 TMG regolamenta l'attività dell'access provider e stabilisce che la responsabilità è totalmente esclusa in due casi: quando egli fornisce all'utenza il mero accesso alla rete e quando crea copie temporanee nella fornitura del servizio. Queste procedure avvengono automaticamente e, solitamente, i contenuti memorizzate non sono conosciuti dal fornitore. Non vi deve, quindi, essere un controllo diretto su queste informazioni.

La disciplina in analisi, invece, non si applica nei casi in cui il provider collabora volontariamente con un utente al fine di commettere atti illeciti, fornendo servizi diversi da quelli di *mere conduit*.

Per godere della limitazione della responsabilità, l'intermediario non deve essere il creatore del trasferimento di dati, non deve scegliere il destinatario di questi né deve determinare o modificare in alcun modo le informazioni inviate.

Quindi, la responsabilità sorge se il fornitore è coinvolto in qualche maniera nella comunicazione dei dati. Esso potrebbe, invece, essere considerato responsabile nel caso in

cui sia a conoscenza dell'illiceità dei dati trasmessi e abbia le capacità tecnica di bloccarli (*technisch möglich*)[236].

Tale capacità non deve essere considerata solamente in senso tecnico ma anche tenendo in considerazione il principio di ragionevolezza. Infatti, data la neutralità del servizio erogato, il blocco può essere esigibile solo in una serie di casi estremamente residuale, come quello in cui il fornitore sia l'unico collegamento all'accesso a siti che siano manifestatamente illeciti.

Il secondo comma del § 8 TMG precisa che le informazioni da comunicare per l'accesso non devono essere conservate per un tempo superiore a quello ragionevolmente necessario per la trasmissione stessa.

La disciplina riguardante l'*hosting* provider viene introdotta al § 10 TMG. La prima parte di questo dettato normativo prevede l'esclusione della responsabilità se il fornitore non è effettivamente a conoscenza dell'illiceità dell'attività o delle informazioni ospitate e, in caso di azioni risarcitorie, se egli non era a conoscenza dei fatti e delle circostanze alla base di queste violazioni.

Successivamente, viene stabilito l'irresponsabilità in casi di immediata rimozione di informazioni illecite o di blocco dell'accesso a queste, a seguito di un'apposita notificazione al provider.

Viene, inoltre, specificato che per "informazione illecita" si deve intendere un contenuto che è già stato oggetto di reclamo.

Sono, invece, considerate "azioni illecite" quei casi in cui sono oggetto di reclamo attività di utilizzo di informazioni senza il necessario permesso degli aventi diritto.

La limitazione della responsabilità è subordinata a diversi requisiti che sono stati chiariti e, talvolta estesi, dalla giurisprudenza tedesca.

La conoscenza dell'illecito debba essere effettiva. La mera negligenza non fa, quindi, sorgere alcun tipo di responsabilità in capo all' intermediario.

Infine, il § 9 TMG tratta la disciplina della responsabilità dei *caching* provider, riprendendo integralmente la Direttiva 31/2001/CE.

[236]Cfr. N. WIMMER, *Die Verantwortlichkeit des Online-Providers nach dem neuren Multimediarecht- zugleich ein Überblick über die Entwicklung der Rechtsprechung seit dem 1.8.1997*, in *Zeitschrift für Urheber-und Medienrecht*, 1999, p. 439.

Secondo la norma in analisi, gli intermediari non sono responsabili quando non modificano le informazioni, rispettano le condizioni di accesso a queste e si conformi alle disposizioni di aggiornamento delle informazione, indicate dalle imprese del settore.

Inoltre, l'intermediario informatico deve agire prontamente al fine di rimuovere le informazioni memorizzate o di disabilitarne l'accesso nel momento in cui venga effettivamente a conoscenza che le informazioni sono state rimosse dal luogo dove inizialmente erano allocate, oppure nel caso in cui una corte o un'autorità amministrativa di vigilanza ne abbia disposto la rimozione o la disabilitazione.

Pertanto, si può concludere che in Germania la trasposizione della direttiva è stata realizzata riproducendo il contenuto del regime esonerativo da responsabilità previsto dal legislatore eurocomunitario[237].

Il § 10 del *Telemediengesetz* del 26 febbraio 2007 relativo alla responsabilità dei fornitori di servizi di *hosting* ha modificato, sulla base dell'art. 14 della Direttiva sul commercio elettronico, la precedente impostazione adottata con il *Teledienstegesetz* del 1 agosto 1997, che prevedeva un regime di irresponsabilità dei fornitori di servizi di memorizzazione permanente, salvo che per le ipotesi in cui essi fossero a conoscenza dell'illiceità delle informazioni trasmesse e avessero la possibilità e le capacità tecniche di fermare l'accesso alle stesse.

Proprio perché l'implementazione nazionale della normativa dell'Unione europea è rimasta fedele all'impianto della direttiva da recepire, la legislazione tedesca è rimasta muta sul punto circa l'instaurazione di un meccanismo di segnalazione e rimozione e, dunque, circa il momento a partire dal quale possa presumersi integrato il requisito della conoscenza effettiva in capo al provider di servizi di *hosting*[238].

[237] D. DÖRR-S. JANICH, *The Criminal Responsability of Interbet service Providers in Germany, 80 Miss. L. J.*, 2011, p. 1247 ss.

[238] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto,* cit., pp. 147 e 148.

CAPITOLO TERZO

La responsabilità degli intermediari informatici nell'ordinamento italiano.
Verso la "responsabilizzazione" del provider…

SOMMARIO: 1. Le posizioni della giurisprudenza italiana prima del recepimento della direttiva europea. - 2. Il Decreto 70/2003 e il recepimento della Direttiva europea: un quadro d'insieme. - 2.1 La normativa italiana in materia di intermediazione informatica: criterio della neutralità e carattere compromissorio della disciplina. - 3. Profili di responsabilizzazione del provider: il requisito della conoscenza e il superamento del sistema qualificato. - 4. *Segue*. Profili di responsabilizzazione del provider: host provider attivo, sistemi di algoritmi e filtraggio e onere della prova. - 5. I poteri inibitori esperibili in ambiente digitale. Quali i doveri dei provider? - 6. Il "*Revenge Porn*": i primi passi concreti del legislatore. - 7. Profili conclusivi.

1. Le posizioni della giurisprudenza italiana prima del recepimento della direttiva europea

Il percorso giurisprudenziale che ha condotto alle tendenze più attuali in materia di responsabilità degli ISP è stato piuttosto contorto e difficoltoso.

Le prime sentenze si sono caratterizzate per la tendenza ad equiparare l'intermediario *online* all'editore, con importanti ricadute sul piano della responsabilità.

La prima pronunzia giurisprudenziale italiana in tema, quella del Tribunale di Napoli del 9 agosto 1997, individuava un fondamento di natura oggettiva della responsabilità del provider[239].

In particolare, il provider era stato ritenuto responsabile di compartecipazione colposa per aver autorizzato o comunque consentito il comportamento dell'utente, creatore dei contenuti illeciti.

[239] Trib. Napoli, 9 agosto 1997, in *Riv. dir. ind*., 1999, p. 38 ss. M. DE CATA, *La responsabilità civile dell'Internet service provider*, cit., p. 157 ss.

La conseguenza era stata la chiusura del sito, motivata con l'equiparazione di un sito Internet ad un organo di stampa, con relativi doveri di controllo sul materiale pubblicato.

Nella fattispecie si trattava di atti di concorrenza sleale in Internet mediante diffusione su un sito web di messaggi promozionali, in cui veniva fatto uso non più autorizzato di segni distintivi appartenenti ad altra impresa.

Nella motivazione della condanna dell'intermediario telematico, il giudice partenopeo argomentava che "il proprietario di un canale di comunicazione destinato ad un pubblico di lettore - e certamente oggi la rete Internet, quale sistema internazionale di interrelazione tra piccole e grandi rete telematiche, è equiparabile ad un organo di stampa - ha l"obblighi precisi di vigilanza sul compimento di atti di concorrenza sleale eventualmente perpetrati attraverso la pubblicazione di messaggi pubblicitari"[240].

Alla base di tale orientamento del giudice napoletano, orientamento forse non sorretto da una conoscenza e un'analisi adeguata delle caratteristiche del nuovo "*medium*", tanto da confondere Internet con il sito web, si ponevano sostanzialmente considerazioni basate più che su argomentazioni di carattere squisitamente giuridico, su ragioni di politica del diritto.

Secondo questa posizione, poiché la *ratio* della severità della normativa di stampa è dettata dalla necessità di sottoporre a controlli accurati l'esercizio di un'attività potenzialmente fonte di enormi danni a causa della diffusione e dell'elevato numero di destinatari, *a fortiori* analoga ratio avrebbe dovuto essere individuata nella disciplina del sito web[241].

Infatti, secondo tale impostazione, la necessità di una regolamentazione severa non poteva che essere acuita per la Rete, la quale, essendo un mezzo di comunicazione aperto, globale e delocalizzato, non solo era fornita di potenzialità diffusive e lesive ben maggiori di quelle della stampa ma poneva delicate questioni di prevenzione e repressione dell'illecito, legate alle difficoltà di individuazione e punizione dell'autore diretto.

Sulla base di tali argomentazioni questa posizione traeva corollari estremi individuando una similitudine dagli effetti decisamente gravi.

La pronuncia del giudice napoletano, secondo un'attenta ricostruzione dottrinale, tradiva una visione ancora approssimativa di Internet, lasciava zone d'ombra ed ignorava le posizioni che proprio sulla base dell'analisi dei caratteri del Web, si erano mostrate caute nell'individuare identità di ratio tra la disciplina della stampa e quella del nuovo *medium*[242].

---

[240] Trib. Napoli, 9 agosto 1997, cit.

[241] M. DE CATA, *La responsabilità civile dell'Internet service provider*, cit., p. 158 ss.

[242] M. FRANZONI, *La responsabilità del provider*, in *Ann.it. dir. autore*, 1997, p. 250 ss.; V. ZENO ZENCOVICH, *La pubblicità nei mezzi di comunicazione*, in *AIDA*, 1996, p. 256 ss.; P. COSTANZO, *Aspetti evolutivi del regime*

Anche il Tribunale di Teramo, l'11 dicembre 1997, ha confermato l'equiparazione tra sito Internet ed organo di stampa, precisando che "*il mezzo non modifica l'essenza del fatto*"[243].
Tra queste ultime due sentenze citate se ne colloca una del Tribunale di Cuneo che invece escludeva ogni responsabilità del provider rispetto ad una violazione del diritto d'autore attuata attraverso un sito ospitato dal suo server[244].
La motivazione era che il provider in questione si era limitato a concedere solo il servizio di connessione ed accesso alla rete ed uno spazio di pubblicazione, per questo nella sentenza il suo ruolo "con una certa approssimazione può assimilarsi a quello di un centro commerciale che abbia concesso in locazione la bancarella sulla quale l'autore ha esposto i prodotti incriminati".
Più centrata sull'analisi delle caratteristiche della rete in uno con quella sulle caratteristiche dei sevizi offerti dal provider è la seconda pronuncia del Tribunale di Cuneo[245].
In tale sentenza il Tribunale piemontese si è dedicato all'analisi delle caratteristiche della rete, rilevandone i caratteri fondamentali e, in particolare, l'apertura al pubblico e la diffusione dal basso.
Notava il giudice del Tribunale di Cuneo che chiunque può accedere ad un sito ed immettervi, senza controllo, limitazioni o informazione di qualsivoglia genere, osservando altresì il numero rilevantissimo di dati che in ogni momento ed in tempo reale vengono immessi in rete da milioni di utenti.
Tali caratteristiche portavano ad escludere che l'autore delle pubblicazioni illecite potesse essere considerato il provider, la cui responsabilità andava valutata in base alla possibilità di impedire l'illecito.
Secondo il giudice piemontese, le caratteristiche della rete e del servizio di *hosting* impedivano la possibilità di controllo preventivo.
Quest'ultimo, ove fosse stato possibile, avrebbe prodotto effetti deleteri, rallentando il flusso di informazioni in Internet, che per la natura e la vita stessa del medium doveva restare mezzo velocissimo.
Con argomentazioni di analisi economica del diritto, il giudice piemontese argomentava la propria posizione facendo rilevare altresì che un eventuale controllo sul materiale immesso in rete avrebbe comportato costi inaccettabili.

---

giuridico di Internet, in *Dir. inf.*, 1996, p. 831 ss.; G. GHIDINI, *Della concorrenza sleale*, in *Il Codice civile. Commentario*, diretto da P. SCHLESINGER, Milano, 1991, p. 186 ss.
[243] Trib. Teramo, 11 dicembre 1997, in *Dir. inf.*, 1998, p. 370 ss.
[244] Trib. Cuneo, 23 giugno 1997, in *De Jure.*
[245] Trib. Cuneo, 19 ottobre 1999, in *Aida*, 2000, p. 705 ss.

Pertanto, con questa pronuncia il Tribunale di Cuneo abbandonava la posizione di responsabilità oggettiva e concludeva che la responsabilità del provider avrebbe potuto configurarsi a titolo di colpa e solo nel caso in cui l'intermediario, a conoscenza dell'illecito, avesse cooperato con l'autore diretto con una condotta, positiva o omissiva, casualmente correlata al danno.

Si delineavano, sulla base dell'analisi delle caratteristiche della rete e dei servizi offerti dal provider, i termini della questione.

Alla luce del criterio di imputazione per colpa era a quel punto necessario stabilire se in capo al provider sussistesse un obbligo di vigilanza o, meglio, se fosse esigibile il controllo preventivo sul materiale immesso in rete, e, ancora, se sussistesse un obbligo di intervento successivo, se questo fosse esigibile, mentre restava sullo sfondo la questione della fonte di tali obblighi di intervento, preventivo e successivo.

In questa linea evolutiva sempre più orientata verso il principio della colpa come criterio di imputazione della responsabilità del provider, si colloca un'importante pronuncia de Tribunale di Roma, che dà una svolta definitiva al cambio di tendenza della giurisprudenza italiana[246].

La controversia traeva origine dall'invio da parte di un utente di un messaggio sul newsgroup *it.economia.analisi-tech.*

Il newsgroup era gestito dalla società Pantheon ed ospitato sul sito Internet di Agorà Telematica. Il messaggio conteneva osservazioni e considerazioni rivolte contro una banca locale così critiche da essere considerato diffamatorio e lesivo dell'"onore, decoro e reputazione" della banca stessa.

La banca decideva allora di agire nei confronti dell'autore del messaggio, dell'amministratore del sistema che ospitava il newsgroup e dello stesso responsabile della Pantheon.

Il Tribunale di Roma ha escluso la responsabilità del prestatore intermediario dal momento che questi si limiterebbe «a mettere a disposizione degli utenti lo spazio "virtuale" dell'area di discussione». Inoltre, a giudizio dell'organo giudicante, non sarebbe imponibile un controllo o una vigilanza sui messaggi diffusi, dal momento che si tratterebbe di un *newsgroup* non moderato.

[246] Trib. Roma, 4 luglio 1998, in *Dir. inf.*, 1998, p. 807 ss., nota P. COSTANZO, *I newsgroups al vaglio dell'Autorità giudiziaria (ancora a proposito della responsabilità degli attori d'Internet)*. G.M. RICCIO, *La responsabilità civile degli Internet providers*, cit., p. 126 ss.

Il gestore di un sito Internet non ha, secondo il Tribunale di Roma, "nessun potere di vigilanza e controllo sui messaggi immessi in rete"[247].

Tale decisione rappresenta certamente una svolta fondamentale nella definizione della responsabilità del provider.

Si escludeva così anche in Italia un obbligo di controllo e monitoraggio per il provider sui dati inviati da terzi sul proprio server.

Il Tribunale di Roma non risolve tutte le questioni relative alla responsabilità del provider.

Nulla era stato detto infatti con riguardo ad eventuali responsabilità successive dell'Internet provider per non aver provveduto a cancellare il messaggio lesivo quando ne viene a conoscenza.

La decisione di Roma è stata determinante nella misura in cui ha negato quel principio di identità tra testata giornalistica e sito Internet che sembrava essere la soluzione comune adottata dai giudici italiani.

La pronuncia precisa, tuttavia, che "ciò non significa affatto che il gestore del server possa comunque mantenere sul server materiale potenzialmente dannoso senza risponderne. Nel momento stesso in cui il provider viene avvisato da chi si ritiene danneggiato da qualcosa posto sul server che ciò gli procura un danno, la sua posizione cambia radicalmente. (...) Dal momento in cui è stato avvisato che attraverso il suo server è in atto un comportamento dannoso, egli deve quindi scegliere se sospendere prudenzialmente la visibilità del messaggio incriminato, o mantenerlo in linea, contribuendo così ad incrementare il danno provocato dal messaggio diffamatorio"[248].

Il provider è in grado di cancellare il messaggio registrato sul proprio server.

Escludere quindi in ogni modo una responsabilità del *provider* per il materiale inviato da terzi comporterebbe che il danno inizialmente causato dal comportamento dell'utente possa essere ulteriormente aggravato da una eventuale "inerzia" del *provider*.

Lo stesso Tribunale di Roma, già il 22 Marzo 1999, aveva precisato il principio secondo cui il provider ha una responsabilità concorsuale nella violazione qualora siano chiare le intenzioni illecite dell'utente, ossia "se dalle circostanze nelle quali si è concretizzato il rapporto tra operatore neutro e utente fornitore di contenuto risulta palese che quest'ultimo intende utilizzare il sito per la commissione di un illecito, la responsabilità del provider deve essere affermata a titolo concorsuale".

[247] Trib. Roma, 4 luglio 1998, cit.
[248] Trib. Roma, 4 luglio 1998, cit.

Risulta quindi applicata all'ISP, che abbia dato un apporto causale all'illecito, la disposizione dell'art. 2055 c.c., in un'ottica che anticipa i provvedimenti dell'Unione Europea (art.14 direttiva 2000/31/CE).

Sulla base delle premesse gettate dai precedenti, la riflessione sulla responsabilità del provider per omesso controllo preventivo pare giungere a piena maturazione con la pronunzia del Tribunale di Monza del 14 maggio 2001[249].

Si trattava nella fattispecie di atti di concorrenza sleale e contraffazione di marchio compiuti da un user.

Il Tribunale brianzolo ha escluso la responsabilità dell'host provider, richiamandosi ai principi generali di diritto, ai precedenti italiani ed argomentando sulla base dei risultati delle principali esperienze straniere, in primis di quella tedesca.

Particolarmente significativa la motivazione del provvedimento del Tribunale brianzolo che ha rigettato la domanda nei confronti del provider.

Secondo il giudice di merito lombardo, "la tesi della responsabilità incondizionata del provider per ogni illecito commesso sulla Rete non appare tuttavia convincente.

In primo luogo, è stata sottolineata in dottrina la improprietà di qualsiasi richiamo diretto o indiretto ai principi enunciati dalla normativa in materia di stampa, dal momento che detta normativa opera nel campo della responsabilità penale introducendo una forma di responsabilità che continua ad essere oggetto di perplessità per la sua natura "paraoggettiva", resa accettabile solo tramite una interpretazione costituzionalmente orientata al principio di colpevolezza.

In secondo luogo, non si può evitare – pena una valutazione astratta e del tutto disgiunta dal dato economico – di considerare quella che è la situazione del provider.

Quest'ultimo, infatti, si limita a consentire l'accesso alla Rete, è il tramite di cui gli utenti (professionali o meno) di internet si avvalgono per "navigare" ed operare nella stessa.

Se si considera la crescita letteralmente esponenziale che la Rete ha avuto non solo in Italia ma in tutto il mondo, pretendere dal provider un controllo sulle informazioni che per suo tramite vengono smistate agli utenti di internet, significa semplicemente entrare in palese conflitto con il principio *ad impossibilia nemo tenetur*.

Anche volendo mascherare la responsabilità del provider sotto l'etichetta della culpa in vigilando, detta responsabilità sarebbe di fatto una responsabilità oggettiva legislativamente non tipizzata, non potendosi in alcun modo immaginare mezzi concreti attraverso i quali il

[249] Trib. Monza, 14 maggio 2002, in *Corriere. giur*., 2001, p. 1625 ss.

provider potrebbe effettuare la propria vigilanza, considerato anche che il monitoraggio dovrebbe essere costante, visto che ogni sito è modificabile in qualsiasi momento.
Si pensi al solo caso della violazione di marchi: per ogni *domain name* il provider dovrebbe verificare l'assenza non solo in Italia ma anche all'estero di marchi o domain names simili appartenenti a soggetti esercenti attività imprenditoriale in settori affini a quello in cui opera il titolare del sito.
Neppure può essere sottaciuta una considerazione basata su una semplice analisi costi - benefici.
La maggior parte dei providers attuali fornisce alla generalità degli utenti un servizio di accesso gratuito. L'introduzione di una forma di responsabilità del provider per tutti gli illeciti commessi tramite o comunque in internet, comporterebbe una lievitazione dei costi del servizio del provider, lievitazione che verrebbe di fatto riversata sulla generalità degli utenti (sotto forma di costi di abbonamento).
Ciò per tacere del pericolo che il (prevedibile) incremento delle azioni di responsabilità nei confronti del provider (spessissimo assai più solvente del titolare del sito, che in molti casi è un privato con scarsissime risorse), comporti di fatto il blocco della Rete.
Appare quindi condivisibile quella giurisprudenza più recente (Trib. Roma, 22 marzo 1999; Trib. Cuneo, 23 giugno 1997; Trib. Roma, 4 luglio 1998) che ha escluso la responsabilità del provider salva l'eccezione dei casi in cui l'illecito sia palese e rilevabile con l'ordinaria diligenza (si pensi al caso di utilizzo come domain name di un nome costituente marchio celebre)"[250].
Il giudice, ritenendo non applicabile, neppure in via analogica, la disciplina sulla stampa ad Internet affrontava la questione sulla base dell'analisi delle caratteristiche di Internet e delle funzioni del provider.
La considerazione della funzione di un semplice intermediario di servizi telematici svolta dal provider, della crescita esponenziale di Internet, della mole enorme di informazioni caricate quotidianamente sui servers, palesava agli occhi del giudice l'inesigibilità del controllo preventivo e dunque l'insussistenza dell'obbligo di vigilanza in capo al provider, salvo entrare in contrasto con il principio *ad impossibilia nemo tenetur* o introdurre una forma di responsabilità oggettiva.

[250] Trib. Monza, 14 maggio 2002, cit.

La conclusioni del tribunale di Monza venivano corroborate da considerazioni di analisi economica del diritto, le quali evidenziavano che soluzioni diverse da quella raggiunta, oltre ad essere infondate, avrebbero condotto ad effetti deleteri sullo sviluppo della rete.

In tema di responsabilità per omesso controllo preventivo potevano ormai ritenersi acquisiti i risultati maturati sulla base dell'analisi dei caratteri tecnici della rete, dei servizi offerti dal provider e dell'applicazione dei principi giuridici.

In tal senso era infatti necessario stabilire, ai fini del giudizio di responsabilità, se il controllo preventivo sulle informazioni immesse in rete dagli users, con il conseguente obbligo di impedire l'ingresso sul sito di materiale illecito, fosse esigibile.

Agli occhi della giurisprudenza dei primi anni del secolo in corso, i caratteri tecnici della rete e del servizio di hosting deponevano in senso negativo[251].

A conferma di quanto la posizione della giurisprudenza prima della direttiva europea e del suo recepimento fosse altalenante, si segnala che sulla scia del "precedente" partenopeo si poneva espressamente una pronuncia del Tribunale di Bologna, che ha fatto applicazione esplicita dell'art. 11 della l. 47/48 per il reato commesso "a mezzo web"[252].

Il giudice felsineo, nell'affermare la responsabilità dell' host provider, sosteneva che "il soggetto che produce o gestisce l'informazione a causa del ruolo che riveste, non può ritenersi esonerato dal dovere di controllo sulla legittimità delle informazioni immesse sul proprio sito, obbligo di controllo che rientra nel più ampio dovere di diligenza professionale che incombe su ogni operatore economico, quale componente del rischio d'impresa" e, richiamandosi espressamente alla pronunzia del tribunale di Napoli dell'8 agosto 1997, riteneva che "il proprietario di un canale di comunicazione ed il gestore del sito Internet recante messaggi on line sono stati correttamente equiparati agli organi di stampa in quanto, anch'essi, al pari degli organi di stampa, riproducono un'opera o uno scritto rendendoli accessibili ad un pubblico di lettori"[253].

Nessun approfondimento veniva dedicato alla questione della possibilità di controllo preventivo da parte del provider sul materiale immesso in rete e, dunque, dell'esigibilità della condotta rimproverata.

Sebbene tale pronuncia si ponga in rotta di collisione con le precedenti, resta isolata nella misura in cui la giurisprudenza maggioritaria aveva già risolto la questione dell'obbligo di controllo preventivo, oramai ritenuto insussistente, e l'attenzione era prevalentemente

[251] M. DE CATA, *La responsabilità civile dell'Internet service provider*, cit., pp. 180 e 181.
[252] Trib. Bologna, 14 giugno 2001, in *Dir. aut.*, 2002, p. 332 ss.
[253] M. DE CATA, *La responsabilità civile dell'Internet service provider*, cit., p. 160.

concentrata sulla questione della responsabilità del provider per l'omissione di un controllo successivo.

La responsabilità degli intermediari della rete era subordinata alla conoscenza e non alla conoscibilità dell'illecito.

Correva il 26 novembre 2001 quando il Tribunale di Bologna si è pronunciato nuovamente, stavolta in linea di continuità con quell'orientamento che proponeva l'esonero del mero gestore del sito che "si limiti a mettere a disposizione degli utenti lo spazio virtuale"[254].

Il Tribunale di Bologna ha qualificato come fornitore di contenuti un provider che, "pur limitandosi a fornire l'accesso al sito gestito (anche in piena autonomia) da altri, non consenta d'identificare il soggetto in questione né fornisca prova del contenuto degli accordi di utilizzazione dello spazio web con tale soggetto identificato".

Questo comportava una responsabilità, in via analogica (possibile in quanto ai soli fini civilistici), ai sensi dell'art. 11 legge 8 febbraio 1948, n. 47, secondo la quale «per i reati commessi con il mezzo della stampa sono civilmente responsabili, in solido con gli autori del reato e fra di loro, il proprietario della pubblicazione e l'editore».

Bisogna dire però che "in quest'ottica la responsabilità del provider si ricollega soprattutto alla protezione (oggettiva) dell'anonimato del gestore del sito, più che all'attività di hosting vera e propria".

Nonostante fosse pacifica oramai la considerazione che in capo al provider non sussistesse un obbligo di ricerca attiva dei materiali illeciti presenti sul server, restava da stabilire in quali termini si ponesse l'obbligo di intervento del provider e se il provider, una volta messo a conoscenza dell'esistenza del materiale illecito, fosse responsabile per il semplice fatto della mancata rimozione o se la responsabilità dell'intermediario informatico fosse subordinata ad altre condizioni[255].

Le pronunce della giurisprudenza di merito, in materia di concorrenza sleale, hanno confermato la natura colposa della responsabilità del provider, respingendo la possibilità di adozione di criteri d'imputazione alternativi.

In particolare, il Tribunale di Firenze nel 2001 ha affermato la responsabilità dell' *host* provider per l'uso di terzi di un sito recante nome lesivo del marchio noto altrui, nel momento in cui l'attività di registrazione del *domain name* sia stata curata dal provider medesimo: in questo caso la responsabilità comunque è per un'azione direttamente compiuta dall'ISP, anche in necessario collegamento con l'attività del gestore terzo del sito (in mancanza della

[254] Trib. Bologna, 26 novembre 2001, in *Dir. aut.*, 2002, p. 448 ss.
[255] M. DE CATA, *La responsabilità civile dell'Internet service provider*, cit., p. 183.

quale la mera creazione di un *domain name* - che restasse inutilizzato - resterebbe irrilevante in quanto inidonea a ledere l'altrui diritto)[256].

Ancora, il Tribunale di Napoli nel 2002 ha distinto rigorosamente la posizione del *content* provider da quella dell'*host* provider e ha stabilito che il *banner* pubblicitario era idoneo a produrre responsabilità ove esso stesso fosse direttamente illecito, mentre restava irrilevante ove l'illecito riguardasse il sito su cui il banner sia ospitato[257].

Dunque, l'aver consentito di pubblicizzare la propria società su di un sito altrui non determinava che la società pubblicizzata potesse rispondere di tutta l'attività svolta sul sito medesimo, dal quale è per così dire solo ospitata, né che avesse l'obbligo giuridico di accertare o d'impedire le eventuali immissioni di messaggi illeciti da parte del gestore dell'altro sito.

Da questa analisi emerge che l'approdo della giurisprudenza maggioritaria, già prima del recepimento della direttiva europea, sembrano essere inclini all'affermazione della natura colposa della responsabilità del provider[258].

Infatti, non soltanto l'elemento psicologico richiesto in capo al provider veniva individuato nella conoscenza effettiva e non nella conoscibilità dell'illecito ma il grado di diligenza necessario alla configurazione di responsabilità, stabilito secondo il parametro dell'agente modello, veniva valutato con particolare attenzione, giungendo alla conclusione che la responsabilità del provider sarebbe stata configurabile in caso di particolare evidenza dell'illecito e comportamento tollerante ed inerte del provider.

2. Il Decreto 70/2003 e il recepimento della Direttiva europea: un quadro d'insieme

A livello nazionale, con il Decreto legislativo 70 del 2003, emanato sulla base della legge delega comunitaria, 39/2002, agli artt. 14-17 si sono recepiti, in modo pressoché invariato, gli artt. 12-15 della Direttiva comunitaria 2000/31/CE, sul commercio elettronico[259].

Il Decreto ha infatti stabilito un tendenziale regime di irresponsabilità del provider.

Oltre a statuire il principio dell'assenza di un obbligo generale e preventivo di sorveglianza, tale normativa nazionale disciplina le esenzioni di responsabilità del provider per i contenuti memorizzati e/o trasportati a richiesta del destinatario del servizio.

[256] Trib. Firenze, 21 maggio 2001, in *Foro it.*, 2001, I, c. 2031 ss.
[257] Trib. Napoli, 14 giugno 2002, in *Corriere giur.*, 2003, p. 75 ss.
[258] M. DE CATA, *La responsabilità civile dell'Internet service provider*, cit., p. 184.
[259] S. SICA, *Recepita la direttiva sul commercio elettronico*, in *Corriere giur.*, 2003, p. 1247 ss.

In tal modo si è voluto evitare di scoraggiare l'investimento e l'innovazione degli operatori della rete, ma anche salvaguardare la libertà di espressione in ambito digitale.

Si è offerto agli intermediari della rete quello che viene definito un "*safe harbour*", ovvero un porto sicuro[260].

Lo scopo è da rivenirsi nella volontà del legislatore di incoraggiare e preservare il libero e incontaminato flusso di informazioni e per tale via garantire una piena libertà di espressione.

Siamo nel 2003, in un contesto in cui la principale esigenza avvertita dal Legislatore era quella di favorire la diffusione di Internet e delle prestazioni correlate all'erogazione dei servizi connessi ad Internet e quindi si voleva evitare che un'eccessiva responsabilizzazione dell'Internet service provider potesse ostacolare il commercio elettronico e i servizi della società dell'informazione.

La scelta fatta dal Legislatore comunitario e, sulle sue orme, dal Legislatore nazionale è netta: il principio della tendenziale irresponsabilità dell'Internet service provider e soprattutto l'affermazione in base alla quale egli non ha un obbligo di controllo preventivo di quello che viene immesso nella rete.

Relativamente al servizio di *mere conduit*, che consiste nel trasmettere su una rete di comunicazione informazioni fornite da un destinatario del servizio o nel fornire un accesso alla rete di comunicazione, l'art. 14 del d.lgs. 70/2003 stabilisce che il prestatore non è responsabile delle informazioni trasmesse a condizione che:

a) non dia origine alla trasmissione;

b) non selezioni il destinatario della trasmissione;

c) non selezioni né modifichi le informazioni trasmesse.

Nelle attività di trasmissione e di fornitura di accesso vanno incluse anche 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.

Si pensi ai servizi offerti dalle compagnie telefoniche per l'accesso alla rete e la trasmissione di informazioni ai fornitori di connettività, ai gestori di dorsali informatiche come i *network backbone provider*.

Per tale genere di operatori, la normativa prevede l'assenza di un obbligo di verifica del contenuto delle informazioni che vengono trasmesse e, come anticipato, subordina la responsabilità alla sussistenza di diverse condizioni.

---

[260] J.A. SHEDD, *Salt from my Attic*, in F.R. SHAPIRO (a cura di), *The Yale Book of Quotation*, in *Yale University Press*, 2006, p. 75.

Tale scelta, sia a livello europeo che nazionale, è frutto della considerazione che l'intermediario di servizi Internet di accesso, che svolge quindi un ruolo assimilabile a quello svolto dagli operatori dei servizi di telecomunicazione nella diffusione delle conversazioni telefoniche, non possa avere alcun controllo su una eventuale comunicazione digitale lesiva dei diritti di terzi e non possa, dunque, essere ritenuto responsabile dei contenuti di tale comunicazione[261].

L'art. 15, relativo al *caching*, dispone che nella prestazione di un servizio della società dell'informazione, consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, il prestatore non è responsabile della memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta, a condizione che:

a) non modifichi le informazioni;

b) si conformi alle condizioni di accesso alle informazioni;

c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore;

d) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni;

e) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione.

Lo standard di diligenza richiesto al prestatore che voglia fruire del regime di protezione è più rigoroso di quello previsto in relazione all'attività di semplice trasporto, come si evince dall'articolata serie di condizioni che gli sono imposte.

Non è un caso che il legislatore, per contrassegnare l'attività di memorizzazione del caching provider, la definisce come "temporanea" e non "automatica, intermedia e transitoria", come nel caso di mere conduit.

Il fornitore dei servizi di caching deve astenersi dall'instaurare un contatto qualificato con i dati che memorizza e per questi il requisito della neutralità si traduce nell'obbligo di conformarsi alle condizioni di accesso e memorizzazione stabilite per le informazioni

[261] E. BASSOLI, *Giurisprudenza italiana e comunitaria sulla responsabilità civile del service provider e la sentenza della Corte di Appello di Milano nel caso Yahoo vs. RTI*, cit., p. 233.

originali dal titolare delle medesime e agli standard di aggiornamento delle informazioni ampiamente riconosciuti e utilizzati dalle imprese del settore[262].

Nell'ambito dei servizi della società dell'informazione, la responsabilità dell'hosting provider è prevista dall'art. 16, d.lgs. n. 70/2003.

Nella prestazione di un servizio della società dell'informazione, consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore:

a) non sia effettivamente a conoscenza 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'illiceità dell'attività o dell'informazione;

b) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

Dunque, a differenza delle attività precedenti, l'attività di hosting implica una memorizzazione, per conto dell'utente e per sua espressa richiesta, che non è né transitoria né temporanea, bensì duratura.

Le condizioni di esenzione richiedono un grado di diligenza decisamente più alto, in ragione dell'elevato rischio che deriva dalla permanenza di dati in Internet e dalla significativa incidenza del prestatore nella catena causale che dalle informazioni dell'utente conduce alla commissione dell'illecito.

Ai sensi dell'art. 16 del decreto, il prestatore non sarà responsabile delle informazioni memorizzate, a condizione che non sia effettivamente a conoscenza, nel caso dell'illecito penale, del fatto che l'attività o l'informazione siano illecite, e non sia al corrente, nel caso dell'illecito civile e delle azioni risarcitorie, di fatti o circostanze che rendano manifesta l'illiceità dell'attività o dell'informazione.

In ogni caso, una volta acquisita tale conoscenza, il prestatore deve agire immediatamente per rimuovere le informazioni o per disabilitare l'accesso al materiale lesivo, conoscenza che, nel caso della legislazione italiana, si dovrebbe considerare acquisita su comunicazione delle autorità competenti[263].

Come ricordato dal considerando 45 della direttiva, la norma nazionale prescrive che per tutte le tipologie di provider non è esclusa la possibilità per gli Stati membri di imporre precisi obblighi in capo agli intermediari informatici, che si vedono obbligati a cooperare

[262] M.L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, cit., p. 93.
[263] M.L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, cit., pp. 94 e 95.

attivamente e prontamente con le autorità giudiziarie e amministrative che abbiano individuato un illecito, al fine di provi fine e impedire che venga reiterato, facendo ricordo a strumenti tecnologici a disposizione.

Facendo riferimento alla conoscenza che si acquisisce a seguito della comunicazioni delle autorità competenti, l'art. 16 del decreto legislativo aggiunge un *quid novi* rispetto sia all'art. 14 della direttiva eurounitaria che all'art. 31, lett. f, n.3 della legge delega[264] e sembra dunque escludere la semplice comunicazione al prestatore effettuata da qualsiasi soggetto interessato.

È la mancata previsione nel quadro normativo dell'Unione di specifiche procedure di segnalazione e rimozione e la conseguente riespansione delle scelte discrezionali affidate agli ordinamenti giuridici nazionali a far sì che il legislatore italiano, nel caso di intermediari della rete i cui servizi si sostanzino nell'attività di host, abbia previsto questa conoscenza ufficializzata e qualificata, tanto da escludere la possibilità che sia sufficiente a radicare oneri di intervento la semplice segnalazione di parte indirizzata al prestatore di servizio.

"L'allocazione del potere di prendere questo tipo di decisioni non è rimessa al privato non è attribuita al privato ma è attribuita al decisore pubblico (alle "autorità competenti")"[265].

Sebbene il dettato legislativo sia chiaro nella sua portata, la genericità dell'art. 16 ha indotto gli studiosi della materia e la giurisprudenza, a ritenere plausibile la possibilità di ricomprendere un novero di soggetti più ampio rispetto alle sole autorità competenti, come meglio si approfondirà in seguito.

È quanto mai importante sottolineare che, in riferimento a tutte le tipologie di provider, ai sensi dell'art. 17 del decreto legislativo 70/2003, l'intermediario informatico non ha un obbligo di controllo preventivo di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.

Più precisamente, fatte salve le disposizioni di cui agli articoli 14, 15 e 16, il prestatore è comunque tenuto:

a) ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione;

---

[264] T. ONOFRIO, *L'impresa di content, host e access providing*, in *AIDA*, 2007, p. 355 ss.

[265] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. 168.

b) a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite.

Quindi evidentemente egli non è responsabile per omesso controllo, secondo scelta legislativa di analisi economica del diritto: non esiste un obbligo di controllo preventivo sulle informazioni ospitate, trasmesse e/o memorizzate dagli Internet service provider e semmai c'è un obbligo diverso, che è quello di rimuovere il contenuto lesivo, diffamatorio, denigratorio, nel momento in cui ci sia l'effettiva conoscenza dell'esistenza e del carattere illecito di questo contenuto.

Il prestatore è civilmente responsabile del contenuto dei servizi nel caso in cui, su richiesta dell'Autorità giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non ha provveduto ad informarne l'autorità competente.

La ratio della previsione è evidente: poiché l'illecito che avviene su Internet è una sorta di illecito permanente, essendovi una permanente ritrasmissione del dato, senza la possibilità del danneggiato d'impedirla, la legge richiede al provider un intervento diretto per impedire la continuativa consumazione del reato.

Pertanto, nel momento in cui il provider viene avvisato che attraverso il suo server si sta realizzando un comportamento lesivo, egli deve verificare il contenuto del messaggio ed eventualmente interrompere la visibilità del messaggio incriminato. Ciò dipende dal fatto che il provider è l'unico soggetto in condizione d'intervenire tempestivamente, provvedendo alla cancellazione di quanto registrato sul proprio server.

La responsabilizzazione sia civile che penale del provider, sia che si configuri una condotta attiva che omissiva, postula dunque l'effettiva conoscenza, comunque essa sia acquisita, e la mancata rimozione del dato illecito.

La disciplina italiana di recepimento espressamente richiede congiuntamente i detti due elementi, sicché sembra escludere che la conoscenza dell'illecito possa essere una conoscenza semplice, resa magari dal soggetto danneggiato che richieda – anche solo personalmente e via e–mail – la rimozione del dato illecito, così come potrebbe essere insufficiente anche una vera e propria denuncia o querela dello stesso, richiedendosi nella detta fonte normativa una conoscenza acquisita da fonte qualificata, proveniente da una pubblica amministrazione, dal pubblico ministero ovvero da un giudice.

La disciplina su richiamata sembra infatti escludere la responsabilità del provider fino al momento in cui non sia intervenuta l'autorità competente a comunicare il dato illecito, richiedendone così la rimozione.

La ragione del richiamo alla necessità di uno specifico intervento dell'autorità giudiziaria o amministrativa è individuata nel fatto che non possono essere rimesse al privato, che si assume esser stato danneggiato, o al provider medesimo, le modalità attraverso le quali il processo di rimozione del dato avrebbe dovuto essere eseguito, dovendosi per converso ridursi al minimo la discrezionalità del provider che applica il blocco o la rimozione dei dati ed occorrendo che l'intero processo comunque sia trasparente e, soprattutto, proporzionato e limitato dal fine perseguito.

Tale conclusione sembra essere ribadita anche dalla Raccomandazione CM/Rec (2014) 6 del Comitato dei Ministri agli Stati Membri del Consiglio d'Europa, su una Guida per i diritti umani per gli utenti di Internet, la quale ricorda che ogni utente di Internet, nell'esercizio del suo diritto a un equo processo, dovrebbe essere in grado di richiedere un riesame della misura presa dal provider da parte di un'autorità amministrativa o giudiziaria competente.

Lasciare le decisioni di rimozione dei dati alla discrezione dei soggetti privati, che non hanno la capacità di pesare i diritti e di interpretare la legge in conformità con la libertà di parola e di altri standard dei diritti umani, è situazione in grado di mettere in serio pericolo il diritto alla libertà di espressione garantita dalla Convenzione europea dei diritti dell'uomo.

Infatti, se il provider è libero nel decidere come i contenuti devono essere filtrati o rimossi, è verosimile che la tendenza sarà quella espansiva della censura al fine di evitare ogni responsabilità (in altri termini, in assenza di criteri coerenti, il provider probabilmente sceglierà di bloccare e rimuovere il contenuto ogni volta che lo stesso sia controverso), il che può ben aprire la strada a pratiche abusive che limitano il diritto alla libertà di espressione e di accesso alle informazioni.

Infine, la Dichiarazione intende escludere l'imposizione di obblighi vaghi o sproporzionati sui providers, e prevede che la rimozione del dato – il cui mancato rispetto implichi la responsabilità del provider – sia ancorata a previsioni chiare della legge ed a previo ordine di un tribunale o di simili autorità che operino con sufficienti garanzie per l'indipendenza, l'autonomia e l'imparzialità, e che abbia la capacità di valutare i diritti in gioco e di offrire le necessarie garanzie per l'utente, in vista della tutela della sua libertà di manifestazione del pensiero.

Sebbene la giurisprudenza di merito si sia confrontata lungamente con la *vexata quaestio* della responsabilità dell'intermediario, anche per dati illeciti diversi dalla violazione del

diritto d'autore, per avere delle pronunce rilevanti da parte della giurisprudenza di legittimità occorrerà attendere anni più recenti.

In tema di responsabilità penale del provider, la Corte di cassazione, facendo propri i ragionamenti che avevano portato all'emanazione della direttiva europea e del decreto legislativo di recepimento, ha affermato, intervenendo nella vicenda *Google c. Vividown*, che non è configurabile il reato di trattamento illecito di dati personali a carico degli amministratori e dei responsabili di una società fornitrice di servizi di "*Internet hosting provider*", che memorizza e rende accessibile a terzi un video contenente dati sensibili (nella specie, un disabile ingiuriato e schernito dai compagni in relazione alle sue condizioni), omettendo di informare l'utente che immette il "file" sul sito dell'obbligo di rispettare la legislazione sul trattamento dei dati personali, qualora il contenuto multimediale sia rimosso immediatamente dopo le segnalazioni di altrui utenti e la richiesta della polizia[266].

In motivazione, la Corte ha evidenziato che l'attività svolta dal "*provider*", anche secondo quanto dispone il d.lgs. 9 aprile 2003, n. 70, consiste nell'offrire una piattaforma sulla quale i destinatari del servizio possono liberamente caricare i loro video senza che il gestore abbia alcun potere decisionale sui dati sensibili in essi inclusi, e, quindi, possa essere considerato titolare del trattamento degli stessi, finché non abbia l'effettiva conoscenza della loro illiceità.

Non incombono a suo carico un obblighi generali di sorveglianza, di ricerca dei contenuti illeciti o di avvertimento della necessità di rispettare la disciplina sulla "privacy".

La sentenza ha sottolineato infatti che "il gestore del servizio di *hosting* non ha alcun controllo sui dati memorizzati, né contribuisce in alcun modo alla loro scelta, alla loro ricerca o alla formazione del file che li contiene, essendo tali dati interamente ascrivibili all'utente destinatario del servizio che li carica sulla piattaforma messa a sua disposizione"[267].

Dunque, ha ribadito che "finché il dato illecito è sconosciuto al service provider, questo non può essere considerato quale titolare del trattamento, perché privo di qualsivoglia potere decisionale sul dato stesso; quando, invece, il provider sia a conoscenza del dato illecito e non si attivi per la sua immediata rimozione o per renderlo comunque inaccessibile esso assume a pieno titolo la qualifica di titolare del trattamento ed è, dunque, destinatario dei precetti e delle sanzioni penali del Codice Privacy"[268].

[266] Cass. pen., Sez. III, 3 febbraio 2014, n. 5107, in *De Jure.*
[267] Cass. pen., Sez. III, 3 febbraio 2014, cit.
[268] Cass. pen., Sez. III, 3 febbraio 2014, cit.

Di pari rilevanza è la sentenza della Cassazione penale del 14 luglio del 2016, n. 2166, dal momento che è la prima a quanto consta ad affermare la responsabilità penale del provider per il dato diffamatorio postato da terzi specificamente individuati.

In sede di legittimità, non vi sono precedenti specifici con riferimento al reato di diffamazione.

Questa sentenza segna il punto di arrivo o meglio di partenza di una giurisprudenza sempre più impegnata negli illeciti telematici e nella responsabilizzazione degli intermediari e rappresenta un trampolino di lancio verso considerazioni dottrinali e giurisprudenziali sempre più mosse da esigenza di tutela in rete.

La vicenda esaminata dalla Cassazione riguardava il gestore di un sito Internet (*www.agenziacalcio.it*) che aveva ospitato un commento sulla *Community* del sito, ossia su apposito spazio lasciato ai commenti del pubblico.

Il commento definiva il presidente della Federazione calcistica giovanile di allora, tale Tavecchio, come «emerito farabutto» e «pregiudicato doc», allegando al messaggio il certificato penale del Tavecchio.

Il gestore del sito era stato quindi citato in giudizio per concorso nel reato di diffamazione.

Il tribunale di Bergamo, con sentenza del 10.11.2014, aveva assolto l'imputato.

Con sentenza del 24.06.2015, la Corte d'appello di Brescia aveva però riformato la decisione di primo grado, affermando la penale responsabilità dell'imputato.

Con l'arresto in commento la Cassazione ha rigettato il ricorso dell'imputato.

In particolare, la Corte Suprema ha rilevato che la sentenza di merito aveva ritenuto il gestore responsabile non per l'inserimento del *file* diffamatorio, cioè per il suo *upload*, effettuato nel caso autonomamente dall'autore, ma per il suo mantenimento *on line* dalla data in cui aveva avuto consapevolezza del *file* (per aver ricevuto sulla casella postale mail dell'autore del messaggio contenente il certificato penale del diffamato) fino alla data del sequestro preventivo del sito.

La Corte, quindi, escludeva da un lato l'allegata contraddittorietà della sentenza impugnata e, per altro verso, la possibilità in sede di legittimità di un riesame della vicenda nel merito, tanto più che nessuna deduzione specifica risultava fatta dal ricorrente (che pur pacificamente si trovava all'estero essendo in periodo feriale) in ordine alle ragioni ostative della lettura della casella postale e quindi della sua consapevolezza del messaggio diffamatorio.

Il nodo centrale posto dalla sentenza è costituito dal fatto che la stessa dà per scontato che il gestore di un sito Internet, che ospiti commenti del pubblico, sia responsabile per il solo fatto

della conoscenza del messaggio ospitato (nel caso, peraltro, come detto piuttosto potenziale), a prescindere dall'esistenza di una richiesta di rimozione del dato da parte del presunto diffamato e dell'autorità giudiziaria.

Il caso, dunque, pone il problema della responsabilità del gestore di un sito Internet per messaggi diffamatori altrui.

È bene soffermarsi, seppur brevemente, su tale profilo: non si tratta del caso della responsabilità di chi direttamente fornisce un contenuto diffamatorio telematicamente veicolato[269] ma della possibilità di chiamare a rispondere il soggetto che gestisce un sito che ospita commenti postati direttamente da terzi.

Qui, peraltro, va evidenziato che non si tratta della responsabilità per fatto altrui, quanto della configurabilità di una responsabilità per fatto proprio (di natura commissiva o, secondo altri, omissiva) in concorso con il fatto (commissivo) del terzo.

Infatti, l'illecito che avviene su Internet è una sorta di illecito permanente nella misura in cui si caratterizza per la sua permanente ritrasmissione del dato, senza la possibilità del danneggiato d'impedirla, sicché la legge richiede al provider un intervento diretto per impedire la continuativa consumazione del reato.

Nel momento in cui il provider è edotto che attraverso il suo server si sta realizzando un comportamento lesivo permanente, egli concorre nel fatto altrui se non interrompe la visibilità del messaggio illecito, rimuovendo il dato informatico in questione o bloccando l'accesso allo stesso.

Con il recepimento della direttiva sul commercio elettronico, ed in particolare degli articoli da 12 a 15 della direttiva comunitaria 2000/31/CE, entrati nel nostro ordinamento con il decreto legislativo n. 70/2003, per l' *host* provider, ossia colui che presta un servizio consistente nella memorizzazione di informazioni fornite da un altro soggetto (*hosting*), la disciplina esclude un obbligo di sorveglianza del provider, stabilendo che nella prestazione dei servizi di *hosting*, il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.

Il prestatore è comunque tenuto ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione, ed a fornire senza indugio, a richiesta delle autorità competenti, le

[269] Il c.d. *content provider* è chiaramente responsabile per fatto proprio: v. Cass., Sez. III, 25 agosto 2014, n. 18174, in *www.altalex.com.*

informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite.

Non deve destare meraviglia, dunque, la generale esclusione di responsabilità del provider per tutti i messaggi qualificabili come posta elettronica, ossia come messaggi telematici recanti comunicazione individuale (se del caso verso una pluralità anche ampia di individui), in quanto la tutela della corrispondenza che protegge anche le e-mail esclude del tutto un potere di intervento censorio del provider e dunque ogni sua responsabilità per l'illecito commesso via e-mail[270].

Le norme in materia (direttiva comunitaria e relativo decreto di recepimento, così come pure il codice di autoregolamentazione dei providers) pongono dunque una regola di comportamento ed un modello di diligenza (obbligo di comunicare le generalità dell'utente ospitato che ha compiuto l'illecito, obbligo di attivarsi per rimuovere l'illecito ricorrendo dati presupposti) che fonda una posizione di garanzia del provider per tutto quanto accade successivamente alla scoperta del dato illecito ed a condizione che il provider possa incidere giuridicamente sullo stesso.

Non essendo previsto un generale obbligo di controllo preventivo, l'art. 16 generalmente non fa scattare automaticamente in capo al provider la posizione di garanzia.

Tuttavia, quest'ultima può configurarsi quando il provider ha una conoscenza effettiva della notizia e non la rimuove.

In altri termini, nel momento in cui l'Internet service provider acquista l'effettiva conoscenza del fatto che è stato pubblicato un contenuto illecito, egli ha l'obbligo di rimuoverlo e la mancata rimozione può dare vita ad una responsabilità sia civile che penale.

In tal caso, siamo di fronte ad un concorso omissivo nel fatto illecito altrui e quindi ai fini della responsabilità del prestatore occorre che la condotta insista nell'inerzia (non ha rimosso i contenuti, pur dovendolo fare).

L'evento è rappresentato da un fatto pregiudizievole antidoveroso altrui.

[270] Cass. pen., Sez. V, 11 febbraio 2009, n. 6046, in *De Jure*, afferma: "non sussiste la responsabilità del gestore di un punto Internet, cosiddetto "Internet point", a titolo di diffamazione per non avere impedito l'evento - art. 40, comma secondo, e 595 c.p. - qualora l'utente invii una e-mail avente contenuto diffamatorio, in quanto il gestore non solo non ha alcun potere di controllo e, quindi, alcuna conoscenza sul contenuto della posta elettronica inviata, ma gli è addirittura impedito di prenderne contezza - ex art. 617 quater cod. pen. che vieta l'intercettazione fraudolenta di sistemi informatici e telematici - mentre ha l'obbligo di identificare gli utenti che facciano uso del terminale ai soli fini della prova dell'utilizzazione e non per impedire l'eventuale reato".

Come in tutti i casi di concorso omissivo nel fatto illecito altrui, invero, ai fini del giudizio di responsabilità del prestatore, occorre l'accertamento degli elementi costitutivi della fattispecie:

- la condotta, consistente nell'inerzia;
- l'evento, quale fatto pregiudizievole ed antidoveroso altrui;
- il nesso causale, mediante il cd. giudizio controfattuale, allorché l'attivazione avrebbe impedito l'evento, anche con riguardo, come nella specie, alla sua protrazione;
- l'elemento soggettivo della fattispecie.

Si potrebbe facilmente obiettare che, nel caso di diffamazione, sarebbe difficile immaginare un'ipotesi di concorso: la diffamazione è un reato istantaneo, si consuma nel momento in cui c'è la pubblicazione della notizia diffamatoria e dunque non si può concorrere in un reato già consumato.

Il concorso eventuale trova il limite nel fatto che il reato è in fase di esecuzione: se il reato è istantaneo, non si può concorrere ex post.

Il contenuto diffamatorio è il principale elemento di illiceità per configurare la responsabilità dell'Internet service provider che non rimuove il contenuto diffamatorio.

In realtà su questa fattispecie la giurisprudenza - nei precedenti che stanno emergendo negli ultimi anni sia nella giurisprudenza di merito che di legittimità - ha accolto una soluzione innovativa, affermando un principio in base al quale l'omessa rimozione del contenuto diffamatorio, comunque illecito, implica una sorta di approvazione da parte dell'Internet service provider che in qualche modo è come se facesse propri quei contenuti, ne agevolasse la permanenza e quindi rinnovasse il reato di diffamazione.

Così facendo, non si ammette una responsabilità per concorso mediante omissione postuma in una diffamazione già commessa.

Al contrario, si sostiene che l'omessa rimozione è come se - dopo che il soggetto ne ha avuto effettiva conoscenza - determinasse una forma di reiterazione della diffamazione di cui a quel punto l'internet service provider diventa responsabile.

Quindi, per superare la criticità della difficoltà di concepire un obbligo impeditivo postumo, a fronte di un reato istantaneo già commesso, la Cassazione ha prospettato il ricorso alla figura di elaborazione dottrinale della pluralità di reati.

Al reato di diffamazione commesso dal sito che utilizza il servizio erogato dal provider ci sarebbe in capo al provider la commissione di un ulteriore reato che consiste nel fatto che attraverso l'omessa rimozione egli farebbe proprio il contenuto diffamatorio e la sua

condotta sarebbe una condotta di ulteriore diffamazione. Qui si ammette una diffamazione mediante omissione molto particolare dove l'omissione che si contesta non è l'omesso controllo ma l'omessa rimozione e si tende ad equiparare - sia pure attraverso la figura della reiterazione del reato - in qualche modo, l'omesso controllo preventivo all'omessa rimozione successiva.

La Cassazione ha affermato qualcosa di analogo anche con riferimento al *blogger*.

Pur avendo nettamente distinto la figura di chi ha un blog rispetto all'Internet service provider, si è detto che la posizione è analoga: entrambi non hanno un obbligo di controllo preventivo ma hanno un obbligo di rimozione, (se conoscono) e se non rimuovono fanno propri i contenuti diffamatori ed è come se reiterassero la diffamazione.

Dunque, si ammette una diffamazione mediante omissione molto particolare dove l'omissione che si contesta non è l'omesso controllo ma l'omessa rimozione e si tende ad equiparare - sia pure attraverso la figura della reiterazione del reato - in qualche modo, l'omesso controllo preventivo all'omessa rimozione successiva.

Si introduce un'ipotesi di diffamazione mediante omissione estranea sia all'art. 57 c.p. che evidentemente non trova applicazione, sia all'art. 110 c.p.

2.1 La normativa italiana in materia di intermediazione informatica: criterio della neutralità e carattere compromissorio della disciplina

Le esimenti della responsabilità previste dalla normativa, per quanto diversamente articolate in base alle specifiche attività svolte dagli intermediari, si caratterizzano per avere come comun denominatore il criterio della neutralità, destinato a modularsi diversamente a seconda del grado di rischio dell'attività svolta e della tipologia di provider preso in considerazione.

Al di là delle differenze strutturali evidenziate tra i vari prestatori informatici, così come affermato anche dal considerando 42 della Direttiva sul commercio elettronico, resta costante la natura meramente tecnica, passiva ed automatica delle attività poste in essere dall'intermediario informatico ed è proprio tale natura a rappresentare l'elemento dirimente dell'imputazione di responsabilità.

Un ulteriore elemento che accomuna gli articoli 14,15,16 del decreto è il carattere compromissorio della disciplina, che introduce una regola di immunità che contempla al tempo stesso la possibilità di fissare una responsabilità in presenza di circostanze "controllabili" ed "evitabili" dallo stesso prestatore con una condotta di diligenza, e così facendo realizza una soluzione intermedia tra l'esclusione di responsabilità – invocata dai

prestatori di servizi anche in nome di esigenze di libertà connesse al funzionamento della rete – e, in senso opposto, una rigorosa regola di responsabilità, richiesta da tutti coloro che possono essere pregiudicati da contenuti presenti in rete per effetto dei servizi offerti dagli intermediari[271].

L'ambito della responsabilità dei prestatori informatici costituisce dunque una conferma della necessità di garantire un giusto equilibrio tra le esigenze di compensazione e deterrenza, tra riparazione del danno sofferto dalla vittima e incentivo a migliorare in termini di sicurezza e qualità l'attività posta in essere dal danneggiante.

In più avvertita pare essere l'esigenza di evitare patologie di *overdeterrence* che rischierebbero di pregiudicare i valori costituzionali.

Come efficacemente rilevato, la responsabilità del provider rappresenta quel "puto nodale dell'infrastruttura […] in cui libertà d'impresa, esigenze di mercato e diritti della persona si incontrano e si scontrano"[272].

Le regole analizzate ed esaminate della Direttiva e del Decreto sono peculiari in quanto costruite in modo singolare: non si tratta infatti di regole di responsabilità bensì di irresponsabilità perché identificano non gli elementi di fattispecie della responsabilità quanto fattispecie aliene da responsabilità, ipotesi di esonero, regimi di irresponsabilità, individuando una serie di fatti impeditivi della non-responsabilità, che impediscono di beneficiare dell'esonero.

Questa operazione è stata ritenuta "frutto di un insonne e tenace interventi di gruppo di pressione, ritenuto fisiologico a Bruxelles, preoccupato di deresponsabilizzare il più possibile i soggetti interessati" che avrebbero almeno inizialmente voluto instaurare un regime in cui la responsabilità è da intendersi come esito eccezionale in un più ampio contesto di irresponsabilità[273].

Particolare è da notare come nell'attuale sistema della responsabilità civile è raro trovare un'area di esonera da responsabilità così ampia.

Si può ritenere che il decreto legislativo 70/2003 e la Direttiva europea 31/2000/CE è da interpretarsi come una significativa inversione di tendenza rispetto ai più recenti sviluppi della responsabilità civile: a fronte della tendenza dell'ultimo secolo di ampliare la responsabilità dell'operatore economico, in quanto "*best risk avoider*", meglio in grado di evitare il danno, dotato di maggiori disponibilità finanziarie e per prassi di adeguata

[271] M.L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, cit., pp. 85 e 86.
[272] D. BIANCHI, *Internet e il danno alla persona: i casi e le ipotesi risarcitorie*, 2012, p. 367 ss.
[273] C. CASTRONOVO, *La nuova responsabilità civile*, 2006, p. 271 ss.

copertura assicurativa, l'esonero in esame " ha spazzato via tutto il meccanismo di presunzioni costruito nel corso di un secolo, quali la culpa in vigilando e la culpa in eligendo con il risultato di gravare a monte i fornitori dei servizi dell'informazione o a valle degli utenti finali del servizio"[274].

3. Profili di responsabilizzazione del provider: il requisito della conoscenza e il superamento del sistema qualificato

Se questo delineato è il quadro normativo vigente, adottato sulla base di una tecnica legislativa molto complessa, numerosi sono i problemi applicativi che si sono posti all'attenzione della giurisprudenza e rilevante è stata l'attività concretizzatrice delle Corti.

In altri termini spiccata è la vocazione dei giudici italiani, pienamente condivisibile, a responsabilizzare gli intermediari dei servizi di memorizzazione con il risultato di "allontanare la regola operativa applicata nel nostro ordinamento dalla regola declamata dal legislatore nazionale"[275].

Due in particolare sono le linee di tendenza che possono essere sintetizzate all'esito dell'analisi del quadro interpretativo fornito dalla giurisprudenza dell'ultimo decennio.

Anzitutto di particolare rilevanza è il passaggio da un sistema di rimozione "qualificato", affidato alle autorità competenti, ad un sistema di rimozione affidato alla diffida di parte.

Viene superata dunque l'espressa previsione dell'art. 16, lett. b, del d.lgs. 70/2003 che richiede una comunicazione delle autorità competenti quale presupposto necessario perché il provider sia obbligato alla rimozione dei contenuti.

Un ruolo sempre più rilevante assume infatti il ruolo dell'internauta che vede ampliarsi in maniera significativa le opportunità relazionali con i servizi di memorizzazione.

Il primo indirizzo giurisprudenziale che ben riassume l'obbligo di immediata rimozione gravante sull'intermediario a partire dall'acquisita consapevolezza dell'illiceità lo si rinviene nelle ordinanze cautelari rese dal Tribunale di Roma nel 2009[276] e 2010[277].

Tale conoscenza è riconducibile ad una semplice comunicazione ricevuta dal titolare dei diritti ed anche ad una semplice comunicazione generica.

Questo primo orientamento si accontenta dunque di una diffida anche molto generica.

---

[274] V. ZENO ZENCOVICH, *Profili attivi e passivi della responsabilità dell'utente in Internet*, in A. PALAZZO-U. RUFFOLO (a cura di), *La tutela del navigatore in Internet*, 2002, p. 137 ss.

[275] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. 168.

[276] Trib. Roma, 16 dicembre 2009, in *Foro it.*, 2010, c. 1348 ss.

[277] Trib. Roma, 11 febbraio 2010, in *Dir. inf.*, 2010, p. 275 ss.

Una conferma di tale orientamento arriva anche dal Tribunale di Milano nel 201[278] con un caso avente ad oggetto la violazione dei diritti d'autore: si è giunti a ritenere che l'obbligo di pronta attivazione dell'intermediario discenderebbe anche da una diffida stragiudiziale contenente l'indicazione di un "campionario indicativo" di alcune delle opere violate.

Secondo un diverso orientamento, invece, sarebbe necessaria una comunicazione di parte dettagliata e corredata da precise informazioni al fine di radicare in capo al provider un obbligo di rimozione dei contenuti illeciti. Lo scopo di un onere più gravoso, così come descritto, è da rinvenirsi nella necessità di consentire all'intermediario un'univoca individuazione dei contenuti da rimuovere[279].

L'attività di preventiva individuazione del contenuto web dal carattere illecito non può essere rimessa la provider "essendo viceversa tale attività il risultato di una valutazione rimessa in primo luogo al titolare del diritto che si afferma leso, in ossequio al principio generale dell'onere di allegazione che impone a chiunque chiede la tutela giudiziale di un diritto asseritamente leso, di indicare le concrete circostanze nelle quali sarebbe avvenuta la lesione"[280].

Tale orientamento trova conferma anche in una pronuncia della Corte d'Appello di Milano nel 2015, che ha ritenuto sufficiente, al fine di risvegliare la "responsabilità a posteriori dell'hosting provider, una richiesta analitica e circostanziata proveniente dalla parte che assume essere titolare dei diritti"[281].

Dunque, la diffida per essere efficace deve essere specifica e deve individuare i contenuti illeciti da rimuovere, non potendo il provider essere oberato di un obbligo di ricerca ed estrapolazione prima di procedere ad una pronta rimozione. La diffida deve infatti contenere gli indirizzi specifici compendiati nei singoli URL[282].

Un importante arresto arriva anche dal Tribunale di Napoli Nord con una sentenza che mette in luce le criticità di un sistema di responsabilità così come costruito in materia di illeciti telematici dalla normativa europea ed italiana.

Il caso in esame faceva riferimento alla presenza su Facebook di collegamenti a filmati amatoriali ritraenti scene sessualmente esplicite, la cui condivisione incontrollata da parte degli utenti del social network portò la persona ritratta al suicidio.

[278] Trib. Milano, 9 settembre 2011, n. 10893, in *Riv. dir. ind.*, 2011, p. 559 ss.
[279] Trib. Roma, 11 giugno 2011, in *Riv. dir. ind.*, 2012, p. 19 ss.
[280] Trib. Roma, 11 giungo 2011, cit.
[281] App. Milano, 7 gennaio 2015, n. 29, in *Riv. dir. ind.*, 2017, p. 4 ss.
[282] Nello stesso senso il Trib. di Torino, 3 giugno 2015, in *De Jure*.

La pronuncia mette in risalto come "appare irrazionale dover attendere un ordine dell'autorità il quale potrebbe intervenire quando oramai i diritti in questione sono irrimediabilmente pregiudicati e non più suscettibili di reintegrazione […]. Pur non sussistendo a carico dell'hot provider un obbligo preventivo di sorveglianza dei contenuti memorizzati né una posizione di garanzia, egli è assoggettato ad un obbligo successivo di attivazione, con la conseguenza che la sua responsabilità a posteriori sorge per non aver ottemperato – come per l'appunto verificatosi nella fattispecie in esame – ad una richiesta […] di rimozione dei contenuti illeciti proveniente dalla parte che assume essere titolare dei diritti"[283].

Un sistema di rimozione qualificato implicherebbe dunque una lungaggine che rischierebbe di vanificare le tutele dell'internauta più di quanto già la normativa non abbia fatto, esonerando il provider della gran parte delle ipotesi di commissione dell'illecito on line.

Un terzo e più recente indirizzo giurisprudenziale, che trova esemplificazione nella sentenza della Corte d'Appello di Roma nel 2018, individua come efficace una segnalazione che si adegui alle procedure di rimozione regolamentate nelle condizioni di utilizzo del servizio dallo stesso intermediario[284].

Sebbene sia copiosa la produzione della giurisprudenza in materia, è l'arresto giurisprudenziale della Suprema Corte nel 2019, *Reti Televisive Italiane S.p.a. c. Yahoo Inc. e Yahoo Italia S.r.l.*, a rappresentare una vera pietra miliare nel sistema della responsabilità dell'Internet Service Provider, in evoluzione applicativa al D.lgs. n. 70/2003, chiarificando una serie di aspetti[285].

Nell'ambito dei servizi della società dell'informazione, come si legge nella sentenza, la responsabilità dell'*hosting* provider sussiste in capo al prestatore dei servizi che non abbia provveduto alla immediata rimozione dei contenuti illeciti, oppure abbia continuato a pubblicarli, quando ricorrano congiuntamente le seguenti condizioni:

a) sia a conoscenza legale dell'illecito perpetrato dal destinatario del servizio, per averne avuto notizia dal titolare del diritto leso oppure *aliunde*;

b) sia ragionevolmente constatabile l'illiceità dell'altrui condotta, onde l'*hosting* provider sia in colpa grave per non averla positivamente riscontrata, alla stregua del grado di diligenza

[283] Trib. di Napoli Nord, 4 novembre 2016, in *Resp. civ. prev.*, 2017, p. 529 ss.
[284] App. Roma, 19 febbraio 2018, n. 1065, in *De Jure.*
[285] Cass. civ., 19 marzo 2019, n. 7708, in *Giur. it.*, 2019, p. 2608 ss. con nota di R. BOCCHINI, *La responsabilità civile plurisoggettiva, successiva ed eventuale dell'ISP.*

che è ragionevole attendersi da un operatore professionale della rete in un determinato momento storico;

c) abbia la possibilità di attivarsi utilmente, in quanto reso edotto in modo sufficientemente specifico dei contenuti illecitamente immessi da rimuovere.

È questione fondamentale individuare la nozione giuridica di "conoscenza effettiva" dell'altrui illecito manifesto realizzato mediante il servizio di hosting, di cui parla l'art. 16, comma 1, lett. a), D.lgs. n. 70/ 2003, come già l'art. 14, comma 1, lett. a), della direttiva sul commercio elettronico per escludere l'operatività dell'esenzione da responsabilità posta dalla disciplina in favore dell'hosting provider; e, più in generale, risolvere il problema della "conoscenza legale" del carattere illecito o anche solo pregiudizievole per un terzo che l'art. 17, commi 2, lett. b) e 3, d.lgs. n. 70/2003 pone quale elemento costitutivo della responsabilità civile dei prestatori di servizi della società dell'informazione, facendone discendere l'obbligo di informare l'autorità competente che, se violato, rende il prestatore civilmente responsabile del contenuto dei servizi prestati. La Suprema Corte, consapevole delle difficoltà interpretative che discendono dal fatto che "certamente si tratta di nozione ab origine psicologica afferente al c.d. foro interno, e ciò tanto più in presenza di soggetti collettivi, in cui lo stato psicologico rilevante viene desunto da quello del legale rappresentante (art. 1391 c.c.)", interviene sul punto.

La conoscenza effettiva dell'altrui illecito, quale elemento costitutivo della responsabilità del prestatore stesso, si radica quando il provider ne ha avuto notizia dal titolare del diritto leso oppure aliunde e la sentenza sottolinea la non necessità di un ordine giudiziale di rimozione.

A ben vedere si ampliano le ipotesi di conoscenza dell'illecito ad ogni forma di reperimento dell'informazione della commissione dell'illecito.

L'art. 16, d.lgs. n. 70/2003 restringe l'obbligo di immediata rimozione e disabilitazione gravante sull'hosting provider alla sola ipotesi in cui sia stati informato dalle autorità competenti dell'illiceità delle informazioni o dell'attività dell'utente (comma 1, lett. b); laddove, invece, la conoscenza effettiva di una situazione di illiceità manifesta (nelle azioni di risarcimento del danno), comunque raggiunta- quindi anche grazie alla segnalazione di un soggetto non qualificato - che è di per sé sola sufficiente a sottrarre il fornitore di ospitalità al regime di irresponsabilità descritto dalla norma (comma 1, lett. a), fa sorgere a suo carico il diverso obbligo di informare senza indugio le autorità competenti - esteso dall'art. 17, comma 2, lett. a anche a presunte attività o informazioni illecite - la cui violazione è fonte di responsabilità civile, ai sensi del comma 3 del medesimo art. 17.

L'onere della prova a carico del mittente riguarda, in tale contesto, solo l'avvenuto recapito all'indirizzo del destinatario, posto che il pervenire della comunicazione in forma scritta a tale indirizzo opera per il solo fatto oggettivo dell'arrivo dell'atto nel luogo indicato.

La presunzione *iuris tantum* di conoscenza è superabile mediante la prova contraria, da fornirsi da parte del prestatore del servizio, concernente l'impossibilità di acquisire, in concreto, l'anzidetta conoscenza per un evento estraneo alla sua volontà.

L'esistenza di detta conoscenza è oggetto dell'apprezzamento demandato al giudice di merito, incensurabile in sede di legittimità.

Ne deriva che il sorgere dell'obbligo in capo al prestatore del servizio non richiede una "diffida" in senso tecnico - quale richiesta di adempimento dell'obbligo di rimozione dei documenti illeciti - essendo a ciò sufficiente la mera "comunicazione" o notizia della lesione del diritto.

Emerge evidentemente da questa epocale sentenza che l'intermediario risponde di una responsabilità per dolo e colpa grave (e dunque attenuata).

L'hosting provider è chiamato quindi a delibare, secondo criteri di comune esperienza, alla stregua della diligenza professionale tipicamente dovuta, la comunicazione pervenuta e la sua ragionevole fondatezza (ovvero, il buon diritto del soggetto che si assume leso, tenuto conto delle norme positive che lo tutelano, come interpretate ad opera della giurisprudenza interna e comunitaria), nonché, in ipotesi di esito positivo della verifica, ad attivarsi rapidamente per eliminare il contenuto segnalato.

L'aggettivo "manifesta" di illiceità vale, in sostanza, a circoscrivere la responsabilità del prestatore alla fattispecie della colpa grave o del dolo: se l'illiceità deve essere "manifesta", vuol dire che sarebbe possibile riscontrarla senza particolare difficoltà, alla stregua dell'esperienza e della conoscenza tipiche dell'operatore del settore e della diligenza professionale da lui esigibile, così che non averlo fatto integra almeno una grave negligenza dello stesso.

Il menzionato bilanciamento, da parte del legislatore, degli interessi coinvolti nel fenomeno Internet è stato così realizzato sancendo un regime di irresponsabilità del prestatore sino al limite del suo diretto coinvolgimento oppure della sua conoscenza dell'illecito: in tal modo perciò circoscrivendo, ma non annullando del tutto, il controllo circa i contenuti immessi che possano integrare illeciti telematici.

Quanto al contenuto della notizia dell'illecito, ed in particolare alla questione dell'indicazione dell'url o link relativo, la Suprema Corte specifica che resta affidato al giudice del merito l'accertamento in fatto se, in riferimento al profilo tecnico-informatico,

l'identificazione di video, diffusi in violazione dell'altrui diritto, sia possibile mediante l'indicazione del solo nome o titolo della trasmissione da cui sono tratti, oppure sia indispensabile, a tal fine, la comunicazione dell'indirizzo url, alla stregua delle condizioni esistenti all'epoca dei fatti.

I giudici ermellini, considerato che il prestatore del servizio è chiamato a rispondere dei danni solo a posteriori, cioè, quando, reso edotto di specifici contenuti manifestamente illeciti, non li rimuova prontamente - ottemperando, nel senso sopra chiarito, o ad un ordine dell'autorità o ad una diffida di rimozione proveniente dal soggetto leso, ove essa sia specifica e circostanziata e comunque idonea a porre un operatore professionale diligente in uno stato di conoscenza effettiva dell'illecito - affrontano l'ulteriore questione relativa alle indicazioni che il titolare del diritto violato debba fornire sulla localizzazione dei contenuti illeciti, in altri termini, in merito al contenuto della notizia dell'illecito.

Al riguardo, la pronuncia in commento stabilisce che la comunicazione al prestatore del servizio deve essere idonea a consentirgli la comprensione e l'identificazione dei contenuti illeciti, secondo la diligenza professionale da questi dovuta.

Chiarisce altresì che quella dell'identificabilità degli illeciti è questione squisitamente di merito, che presuppone un ineludibile accertamento in fatto, coinvolgente profili tecnico-informatici, che potrebbero rendere necessario un ausilio esperto, trattandosi di stabilire se, alla stregua del grado di diligenza che è ragionevole attendersi da un operatore professionale della rete, in un determinato momento storico, sia a ciò sufficiente la mera indicazione del nome o del titolo o dell'opera illecitamente riprodotta e diffusa e simili elementi descrittivi, ovvero occorra anche l'esatta indicazione dell'url o link relativo, alla stregua dello sviluppo tecnologico e delle condizioni esistenti all'epoca dei fatti[286].

Nell'enucleare la responsabilità dell'Internet Service Provider (ISP) derivante dalla mancata rimozione del segnalato contenuto illecito (*rectius* conosciuto o conoscibile contenuto illecito) la Suprema Corte evidenzia la necessità che la segnalazione dell'illiceità del contenuto sia sufficientemente specifica ovvero idonea a consentire all'ISP il reperimento del contenuto illecito lamentato dal soggetto leso.

[286] M. GAMBINI, *La responsabilità dell'Internet service provider approda al vaglio della Cassazione*, in *Corriere giur.*, 2020, p. 195 ss.

4. Segue. Profili di responsabilizzazione del provider: host provider attivo, sistemi di algoritmi e filtraggio e onere della prova.

Una seconda linea di tendenza attraverso cui la giurisprudenza italiana ha inasprito le condizioni di fruibilità del regime di favore previsto per gli intermediari è da rinvenire nella creazione in via pretoria della figura del fornitore di servizi di "hosting attivo"[287].

L'arresto giurisprudenziale del 2019 della Suprema Corte italiana[288] rappresenta una vera pietra miliare nel sistema della responsabilità dell'Internet Service Provider, in evoluzione applicativa al d.lgs. n. 70/2003.

Infatti, a seguito del dibattito giurisprudenziale e dottrinario, viene definitivamente specificata la figura dell'hosting provider attivo[289].

Il riferimento è a quel 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 in essere una condotta attiva, concorrendo con altri nella commissione dell'illecito.

Si ha un hosting provider attivo quando sostanzialmente il provider, l'hosting, pone in essere condotte che abbiano l'effetto di completare ed arricchire in modo non passivo la fruizione di contenuti da parte di utenti determinati.

In tale ipotesi l'intermediario resta sottratto al regime generale di esenzione di cui all'art. 16, d.lgs. n. 70/2003, dovendo la sua responsabilità civile atteggiarsi secondo le regole comuni[290].

---

[287] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. 171 ss.

[288] Cass. civ., 19 marzo 2019, n. 7708, cit.

[289] R. BOCCHINI, *La responsabilità civile plurisoggettiva, successiva ed eventuale dell'ISP,* cit., p. 2606. Sulla ricostruzione della figura soggettiva dell'ISP attivo si segnalano, *ex multis*, in giurisprudenza: Trib. Catania, 29 giugno 2004, in *Dir. inf.*, 2004, p. 466; Trib. Milano, 2 marzo 2009, "caso RTI c. RCS", in *Dir. inf.*, 2009, p. 521 ss.; Trib. Roma, 15 dicembre 2009, "caso RTI c. YouTube", in *Dir. inf.*, 2009, p. 521 ss.; Trib. Roma, 11 febbraio 2010, in *Dir. inf.*, 2010, p. 275 ss.; Trib. Milano, 24 febbraio 2010, n. 1972, "caso Vividown c. Google", in *Riv. dir. ind.*, 2010, 328 ss.; Cass., 23 dicembre 2009, n. 49474, "caso *Pirate Bay*", in *Dir. inf.*, 2010, p. 437; Trib. Milano, Sez. Spec. Prop. Ind. e Intellettuale, 7 giugno 2011, n. 7680, "caso RTI c. Italia Online (IOL)", in *Dir. inf.*, 2011, p. 660 ss.; Trib. Roma, Sez. Spec. Prop. Ind. e Int., 20 marzo 2011, in *Riv. dir. ind.*, 2012, p. 44 ss., con nota di E. TOSI, *La responsabilità civile per fatto illecito degli Internet Service Provider e dei motori di ricerca a margine dei recenti casi "Google Suggest" per errata programmazione del software di ricerca e "Yahoo! Italia" per "link" illecito in violazione dei diritti di proprietà intellettuale*; Trib. Milano, Sez. Spec. Prop. Ind. e Intellettuale, 7 giugno 2011, in *Dir. inf.*, 2011, p. 660; Trib. Milano, Sez. Spec. Prop. Ind. e Intellettuale, 9 settembre 2011, in *Riv. dir. ind.*, 2012, p. 364 ss., con nota di P. SARACENO, *Note in tema di violazione del diritto d'autore tramite Internet: la responsabilità degli Internet Service Provider*; Trib. Roma, 27 aprile 2016, e Trib. Roma, 5 maggio 2016, in *www.altalex.com* ; da ultimo, tutte in *AIDA*, 2018, App. Roma, Sez. specializzata in materia di imprese, 29 aprile 2017; Trib. Firenze, Sez. Specializzata in materia di impresa, 26 febbraio 2018; App. Roma, 19 febbraio 2018.

[290] Per due primi didascalici commenti alla presente sentenza vedi R. PANETTA e A.M. ROVATI, in *Diritto di Internet*, 2019, p. 261 e G. CASSANO, in *Vita Notarile*, 2019, p. 557.

L'intermediario si troverebbe a rispondere, condivisibilmente, in solido con l'autore dell'illecito ai sensi dell'art. 2055 c.c.

Si tratta, infatti, di una figura che va ricondotta alla fattispecie della condotta illecita attiva di concorso.

In altri termini, i giudici del Supremo Collegio riconducono alla bipartizione host provider attivo e passivo la nota partizione elaborata nell'ambito della teoria della condotta illecita, tra azione e omissione: nel senso che il comportamento dell'hosting provider passivo viene sussunto nello schema della responsabilità omissiva e quello dell'hosting provider attivo in quello, invece, della responsabilità omissiva impropria per concorso nella condotta di azione (illecita) altrui.

Non è agevole individuare la linea di separazione tra le attività di hosting "protette" dai benefici d'esonero di legge e le altre attività "non protette", che prevedono un certo grado di intervento sulle informazioni memorizzate, soprattutto in considerazione della continua evoluzione dei servizi offerti da tali intermediari, di cui non può non tenersi conto.

Eppure, tracciare tale linea di separazione è determinante visto e considerato che dalla qualificazione dell'attività prestata ne discende l'individuazione del principio applicabile.

La figura dell'host attivo è dunque apparsa come un *tertium genus*[291], come una figura ibrida tra il fornitore passivo – mero vettore di informazioni che si limita a esercitare in maniera neutrale e passiva i servizi tecnici di trasporto, memorizzazione – e il fornitore di contenuti – che si ritrova a svolgere funzioni editoriali[292].

Non è possibile ricondurre un intermediario a priori ad una categoria piuttosto che ad un'altra.

Si faccia il caso di figure degli aggregatori dei contenuti di terzi, dei motori di ricerca o delle reti sociali: per comprendere il coinvolgimento del provider nella presunta attività illecita si rende necessario svolgere una valutazione del caso concreto e decidere di volta in volta il grado di interferenza ravvisabile.

La giurisprudenza ha individuato alcuni elementi idonei a delineare la figura o "indici di interferenza", da accertare in concreto ad opera del giudice del merito: le attività di filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione o promozione dei contenuti, operate mediante una gestione imprenditoriale del servizio, come pure l'adozione di una tecnica di valutazione

[291] L. BUGIOLACCHI, *Ascesa e declino della figura del provider attivo? Riflessioni in tema di fondamento e limiti del regime privilegiato di responsabilità dell'hosting provider*, cit., p. 1265 ss.
[292] M.L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, cit., pp. 102 e 103.

comportamentale degli utenti per aumentarne la fidelizzazione: condotte che abbiano, in sostanza, l'effetto di completare ed arricchire in modo non passivo la fruizione dei contenuti da parte di utenti indeterminati.

Si tratta di un elenco a titolo esemplificativo di elementi che non necessariamente devono essere tutti compresenti.

Deve trattarsi, in ogni caso, di condotte che abbiano in sostanza l'effetto di completare ed arricchire in modo non passivo la fruizione dei contenuti da parte degli utenti.

Risulta, pertanto, evidente che la verifica riguardo al ruolo dell'hosting provider rispetto ai contenuti memorizzati dagli utenti debba essere necessariamente compiuta dal giudice di merito, con l'ausilio di un consulente tecnico specializzato, attraverso un'attenta disamina del caso concreto e la massima valorizzazione delle particolarità del fatto sottoposto alla sua attenzione, muovendo, in particolare, dalla considerazione del o dei servizi di volta in volta prestati, della complessità delle attività svolte, delle circostanze e delle concrete modalità tecniche di erogazione degli stessi.

Ciò al fine di stabilire se essi si traducano o meno in un'effettiva possibilità (anche dal punto di vista tecnico) di conoscenza o di controllo sui contenuti memorizzati, che è necessaria per il superamento di quel limite di neutralità sul quale si fondano le esenzioni di responsabilità poste dalla direttiva sul commercio elettronico e dalla normativa di recepimento[293].

I giudici costruiscono la figura dell'hosting provider attivo con lo scopo di escludere l'applicazione del regime speciale di responsabilità dettato dall'art. 16, D.lgs. n. 70/2003, desunto dall'art. 14 della direttiva sul commercio elettronico per i fornitori del servizio di ospitalità.

In particolare, l'avvio del florido filone giurisprudenziale, che ha condotto alla costruzione dogmatica della figura dell'hosting attivo, viene generalmente fatto risalire al noto caso *RTI contro Yahoo*, con il quale veniva affermato il principio secondo cui l'associazione di messaggi pubblicitari ai contenuti immessi in rete dagli utenti, i cui proventi concorrono a finanziare l'attività del prestatore di servizi, dovevano essere qualificati come servizi di hosting attivo, così esorbitando da qualsiasi posizione di pretesa neutralità del prestatore e rendendo inapplicabile la disciplina di cui all'art. 16, d.lgs. n. 70/2003 a favore di una valutazione della sua condotta secondo le comuni regole della responsabilità civile.

Secondo R.T.I., Yahoo Italia S.p.A. e Yahoo Inc. erano responsabili per aver illecitamente diffuso nella sezione del proprio portale dedicata ai video (ad oggi non più esistente) taluni

[293] M. GAMBINI, *La responsabilità dell'Internet service provider approda al vaglio della Cassazione*, cit., p. 187 ss.

filmati tratti da vari programmi televisivi su cui l'attrice vantava diritti d'autore e connessi (quale emittente televisiva).

In specie, R.T.I. aveva inoltrato un'apposita diffida chiedendo la rimozione dei contenuti compresi in apposito elenco e sui quali deteneva diritti esclusivi, sicché - dietro il rifiuto di Yahoo di ottemperare alla richiesta - la prima si era rivolta al Tribunale di Milano[294].

Si deve infatti alla pronuncia del 9 settembre del 2011 l'elaborazione più compiuta della figura in esame.

Il giudice meneghino aveva ritenuto che, sebbene i filmati fossero stati caricati sul portale dagli utenti, Yahoo Italia (e non anche l'altra convenuta) era responsabile per averli aveva gestiti, organizzati e indicizzati, assumendo dunque un ruolo attivo circa la possibilità di collegare i contenuti fra loro e di sfruttarli commercialmente.

Questo ruolo faceva transitare la fattispecie al di fuori della sfera di applicazione delle norme del d.lgs. n. 70/2003 che circoscrivono la responsabilità del c.d. hosting provider passivo.

In realtà già prima di tale sentenza, riconosciuta in dottrina quale vero e proprio leading case, un'altra precedente pronunzia del tribunale meneghino era giunta alle medesime conclusioni ed aveva riconosciuto l'ISP, quale hosting attivo, quando:

a) forniva e organizzava un sistema automatico di servizi pubblicitari che permetteva l'associazione di messaggi promozionali ai video degli utenti;

b) faceva sottoscrivere ai suoi utenti dei contratti che prevedevano una licenza non esclusiva per l'esercizio dei diritti di riproduzione e adattamento inerenti ai video caricati, una manleva in caso di richieste risarcitorie dovute all'illiceità degli stessi e il diritto di rimuoverli se in violazione dei diritti di terzi;

c) predisponeva un servizio di ''segnala abuso'' tramite il quale i detentori dei diritti potevano indicare i video ospitati e richiedere una rimozione selettiva;

d) forniva un servizio automatico di ''video correla ti'' consistente nella visualizzazione, a lato o sotto il video in riproduzione, di altri contenuti ad esso in qualche modo associati.

Di contro, la Corte d'Appello di Milano aveva ribaltato la sentenza di primo grado e deciso che la presenza di sofisticate tecniche di intercettazione e organizzazione del contenuto dei file caricati nonché uno specifico interesse del gestore a conseguire vantaggi economici non fossero sufficienti a ricondurre il servizio a quello di un hosting provider attivo[295].

Inoltre, sebbene sia obbligo dell'hosting provider quello di rimuovere i contenuti illeciti o impedire l'accesso ai medesimi non appena riceva notizia della loro presenza sul sito che

[294] Trib. Milano, 9 settembre 2011, n. 10893, in *Riv. dir. ind.*, 2011, p. 559 ss.
[295] App. Milano, 7 gennaio 2015, n. 29, in *Riv. dir. ind.*, 2017, p. 467 ss.

gestisce, a dire del secondo giudice Yahoo Italia non era tenuta ad agire in base a una diffida, la quale elencava solo genericamente i contenuti e non anche, specificamente, gli URL dei file da rimuovere.

D'altronde - rilevava la Corte d'Appello - in corso di causa Yahoo Italia aveva agito prontamente ai fini della rimozione degli illeciti dopo aver ottenuto da R.T.I. dati idonei a rintracciare con esattezza i file.

Nel cassare la decisione di seconde cure con rinvio - demandando a giudice del merito di rivalutare il profilo afferente alla idoneità di una comunicazione priva della indicazione degli URL, su quale ovviamente ci si soffermerà nel prosieguo - la Suprema Corte offre una vera e propria summa circa la responsabilità dell'host provider attivo[296].

In particolare, come ribadito, gli ermellini riconoscono la categoria dell'hosting provider attivo, sebbene abbiano ritenuto Yahoo! Video un hosting provider passivo, di cui però sono stati ridefiniti i lineamenti generali.

Nel caso di specie, l'esenzione di responsabilità di cui al decreto viene meno al verificarsi delle seguenti condizioni:

a) l'hosting è in qualsiasi modo giunto a conoscenza dell'illecito in questione;
b) l'illiceità è ragionevolmente constatabile;
c) l'hosting è stato informato in modo specifico dei contenuti controversi.

La Cassazione, dunque, riconosce l'esistenza della distinzione tra host provider attivo e passivo, considera la nozione di quest'ultimo un approdo ormai acquisito in ambito europeo e ne afferma, in via generale, la configurabilità quando sia ravvisabile una condotta di azione in capo al prestatore[297].

---

[296] Sul punto, vedi anche App. Roma, 29 aprile 2017, n. 2833, in *Il Diritto industriale*, 2018, con nota di G. CASSANO, *Caso Break: confermata in appello la responsabilità del provider*, p. 182 ss.: "Il provider che non si limiti a svolgere un'attività di tipo neutro, automatico e meramente tecnico, non può in nessun caso invocare a proprio vantaggio il regime di limitazione della responsabilità previsto dall'art. 14 della Dir. 2000/31 CE e dall'art. 16 del d.lgs. n. 70/2003".
Questo il principio espresso dalla Corte d'Appello di Roma che, ribadendo l'orientamento espresso dai giudici di primo grado, ha confermato che i gestori della piattaforma su cui erano diffusi i contenuti i cui diritti di sfruttamento economico erano di titolarità dell'operatore televisivo, non potessero invocare il regime di responsabilità agevolata previsto dalla normativa comunitaria e dal decreto con cui la medesima è stata attuata nel nostro ordinamento. Si tratta di un orientamento ormai consolidato.

[297] CGUE, 7 agosto 2018, C-521/17 *Cooperatieve Vereniging SNB-REACT UA v. DeepakMehta*, in *D&G*, 2018, p. 78 ss.; CGUE, 14 giugno 2017, C-610/15, *Stichting Brein*, in *Foro it.*, 2017, voce Unione europea, c. 345 ss.; CGUE, 11 settembre 2014, C-291/13, *Sotiris v. Papasavvas*, in *http://pluris-cedam.utetgiuridica.it*; CGUE, 12 luglio 2011, C-324/09, *L'Oreal c. Ebay International*, in *AIDA*, Milano, 2011, p. 480 ss.; CGUE, 23 marzo 2010, cause riunite da C-236/08 a C-238/08, *Google France SARL, Google Inc. c. Louis Vuitton Mallettier - Google France SARL c. Viaticum SA, Luteciel SARL - Google France SARL, c. Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL*, in *Dir. ind.*, 2010, p. 429 ss., con nota di M. TAVELLA-S. BONAVITA, *La Corte di Giustizia sul caso "Adwords": tra normativa marchi e commercio elettronico.*

Già la giurisprudenza di merito nello stesso anno aveva affermato che l'hosting provider perde il suo carattere "passivo" qualora i servizi offerti si estendano ben al di là della predisposizione del solo processo tecnico che consente 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", ma interviene nell'organizzazione e selezione del materiale trasmesso, finendo per acquisire una diversa natura di prestatore di servizi - quella di hosting "attivo" - non completamente passivo e neutro rispetto all'organizzazione della gestione di contenuti immessi dagli utenti, dalle quali trae anche sostegno finanziario in ragione dello sfruttamento pubblicitario connesso alla presentazione organizzata di tali contenuti[298].

Affinché l'attività del prestatore di servizi perda il suo carattere di neutralità e, con esso, l'esenzione di responsabilità, non è necessaria una conoscenza personale e diretta del contenuto illecito, ma è sufficiente che i mezzi tecnologici dallo stesso utilizzati siano comunque idonei a conferirgli la conoscenza o il controllo dei dati memorizzati.

Pertanto, anche se il prestatore di servizi si avvale di un software per indicizzare, organizzare, catalogare, associare ad altri o alla pubblicità i video caricati dagli utenti, egli viene comunque a svolgere un ruolo attivo di ingerenza nei contenuti memorizzati, tale da permettergli di conoscere o controllare e di fornire un importante contributo all'editing del materiale memorizzato.

Ai fini dell'affermazione della responsabilità dell'hosting provider "attivo" occorre in ogni caso dimostrare che questi fosse a conoscenza o potesse essere a conoscenza dell'illecito commesso dall'utente mediante l'immissione sul portale del materiale audiovisivo in violazione dei diritti di sfruttamento economico detenuti dal titolare dei diritti lesi.

Ciò in quanto anche all'hosting provider "attivo" si applica il divieto, previsto dall'art. 15 della direttiva 31/2000 (e dall'art. 17 del decreto attuativo n. 70/2003), di un obbligo generalizzato di sorveglianza preventiva sul materiale trasmesso o memorizzato e di ricerca attiva di fatti o circostanze che indichino la presenza di attività illecite da parte degli utenti del servizio.

Correlativamente, neppure può essere esclusa la responsabilità dell'hosting provider "passivo" ogniqualvolta sia stato messo a conoscenza, da parte del titolare dei diritti lesi, del contenuto illecito delle trasmissioni e ciononostante non si sia attivato prontamente per

[298] Trib. Roma, 10 gennaio 2019, n. 693, *Reti Televisive Italiane s.p.a. c. VIMEO LLC*, in *Dir. ind.*, 2019, p. 362 ss.

rimuovere le stesse e abbia proseguito, invece, nel fornire agli utenti gli strumenti per la prosecuzione della condotta illecita[299].

Tuttavia, precisa anche tale giurisprudenza, sia di merito che di legittimità, che nemmeno l'hosting "attivo" può essere assoggettato ad un obbligo generalizzato di sorveglianza e di controllo preventivo del materiale immesso in rete dagli utenti (destinatari del servizio), in quanto ciò si risolverebbe in una inammissibile compressione del diritto di informazione e della libertà di espressione e comprometterebbe il necessario equilibrio che deve esserci tra la tutela del diritto d'autore e la libertà d'impresa nel campo della comunicazione.

A livello nazionale, invece, certamente degno di nota è un provvedimento cautelare del Tribunale di Milano del 19 ottobre 2020 (confermato in sede di reclamo con ordinanza in data 12 gennaio 2021), che ha innanzitutto ricordato che, ai sensi del considerando 42 della Dir. 2000/31/CE, viene meno il regime privilegiato di cui possono godere gli Internet Service Provider nel caso in cui "l'attività di memorizzazione delle informazioni sia posta in essere da un hosting provider attivo", ed accertato, in concreto, tale qualità in capo alla resistente (Amazon) nel caso specifico, in quanto, tra l'altro:

a) "gestisce lo stoccaggio e la spedizione dei prodotti",
b) "gestisce un servizio clienti per le inserzioni di vendita di terzi, che costituisce l'unico servizio di cui il cliente dispone per potersi interfacciare con il venditore",
c) "è responsabile di un'attività promozionale anche tramite inserzioni su siti internet di terzi" e
d) "permette ai consumatori di inferire l'esistenza di un legame tra Amazon" e le aziende produttrici dei prodotti venduti sulla piattaforma.

La conseguenza è che ad essa non sono applicabili le esenzioni di responsabilità previste dalla normativa innanzi citata in quanto, per l'appunto, l'attività da essa prestata è qualificabile in termini di fornitura di un servizio di hosting "attivo", "avendo conoscenza e controllo dei dati che vengono inseriti dai terzi venditori", ragion per cui all'esito del giudizio è stato inibito "con effetto immediato a Amazon Europe Core SARL, Amazon Eu

[299] Conforme: CGUE, 23 marzo 2010, C-236/08, *Google c. Louis Vuitton*, in *De Jure*; Trib. Milano, 7 giugno 2011, n. 7680, in *De Jure*.; CGUE, 12 luglio 2011, C-324/09, *L'Oreal c. eBay*, in *De Jure*; CGUE, 24 novembre 2011, C-70/2010, *Scarlet c. Extended*, in *De Jure*; Trib. Roma, 24 novembre 2011, in *De Jure*; CGUE, 16 febbraio 2012, C-360/2010, *Sabam vs. Netlog*, in *De Jure*; Trib. Milano, 25 maggio 2013 e 5 settembre 2013, in *De Jure*; CGUE, 11 settembre 2014, C-291/13, *Papasavvas c. Fileleftheros*, in *De Jure*; Trib. Roma, 27 aprile 2016, confermata da App. Roma, 29 aprile 2017, Trib. Roma, 5 maggio 2016, Trib. Roma, 15 luglio 2016, in *De Jure*; CGUE, 15 settembre 2016, C-484/14, *Mc Fadden vs. Sony Music*, in *De Jure*; Trib. Milano, 23 giugno 2017, in *De Jure*; Trib. Roma, 28 giugno 2018, in *De Jure.*
Difforme Cass., Sez. III, 3 febbraio 2014, n. 5107, in *De Jure*; App. Milano, 7 gennaio 2015, *Yahoo c. RTI*, in *De Jure.*

SARL e Amazon Services Europe SARL, di commercializzare e/o offrire in vendita e/o promuovere e/o pubblicizzare tramite il proprio sito www.amazon.it i prodotti recanti i marchi" delle ricorrenti.

Nell'ordinanza di reclamo, poi, lo stesso Tribunale ha ulteriormente specificato che nei confronti di società che "partecipano all'immissione in commercio dei prodotti", assumendo "in sostanza buona parte dei compiti propri del venditore e nell'esercizio di tali attività tengono un comportamento attivo ed esercitano un controllo, diretto o indiretto", ben può essere imposto un ordine di inibitoria che presupponga anche un monitoraggio attivo, teso ad individuare e impedire la messa a disposizione del pubblico di prodotti(o servizi, o contenuti digitali, ecc.) che violano i diritti di terzi: infatti, "lo svolgimento di tutte le attività di commercializzazione innanzi evidenziate implicherebbe l'onere in capo alle reclamanti di porre in essere una particolare cura e diligenza quanto al controllo della liceità dei beni che immettono in commercio".

In questi stessi termini sono poi alcune pronunce del Tribunale di Roma, tra cui le sentenze n. 14757 del 12 luglio 2019 (*RTI c. Dailymotion*) e n. 18727 del 2 ottobre 2019 (*RTI c. Bit Kitchen*), ove l'Autorità ha "vietato" ai fornitori dei servizi di video-sharing interessati "ogni ulteriore violazione, perpetrata in qualunque forma e con qualunque mezzo", avente ad oggetto brani audiovisivi estratti dai programmi televisivi della società attrice.

A queste hanno fatto eco, ancor più recentemente, due pronunce "gemelle" - del Tribunale di Roma del 20 e 22 gennaio 2021, rispettivamente n. 1049 (*RTI c. Veoh*) e n. 1194 (*RTI c. Dailymotion*) - con cui il Tribunale ha dichiarato la natura di hosting provider "attivi" in capo ai gestori delle due video-sharing platform convenuti, condannandoli alla rimozione ed all'inibitoria dal futuro ricaricamento di numerosi estratti di opere audiovisive, evidenziando (tra i tanti passaggi di interesse in esse contenuti) come ai fini della identificazione di tali opere sia sufficiente la conoscenza di "titolo e provenienza" (trattandosi, anche in questo caso specifico, di contenuti video estratti dai programmi TV dell'attrice).

Sempre sullo specifico tema della responsabilità diretta del fornitore di servizi di "hosting", e della natura "attiva" o "passiva" dello stesso, è nuovamente intervenuta, recentemente, una sentenza della Corte di Giustizia UE del 22 giugno 2021, che nelle cause riunite C-682/18 e C-683/18 ha preso in esame (tra l'altro) il servizio fornito tramite la piattaforma di video-sharing più nota in assoluto: YouTube.

Non senza aver premesso che le interpretazioni fornite in risposta alle questioni pregiudiziali sottoposte non avrebbero tenuto in considerazione il regime normativo istituito dall'art. 17, Dir. UE 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale (in fase

di recepimento in Italia nel momento in cui si scrive), la Corte ha quindi stabilito che il gestore di una piattaforma di condivisione di video, sulla quale utenti possono mettere illecitamente a disposizione del pubblico contenuti protetti, non effettua "direttamente" un atto di comunicazione al pubblico di detti contenuti, ameno che "tale gestore sia concretamente al corrente della messa a disposizione illecita di un contenuto protetto sulla sua piattaforma e si astenga dal rimuoverlo o dal bloccare immediatamente l'accesso ad esso, o nel caso in cui detto gestore, anche se sa o dovrebbe sapere che, in generale, contenuti protetti sono illecitamente messi a

disposizione del pubblico tramite la sua piattaforma da utenti di quest'ultima, si astenga dal mettere in atto le opportune misure tecniche che ci si può attendere da un operatore normalmente diligente nella sua situazione per contrastare in modo credibile ed efficace violazioni del diritto d'autore su tale piattaforma, o ancora nel caso in cui esso partecipi alla selezione di contenuti protetti comunicati illecitamente al pubblico, fornisca sulla propria piattaforma strumenti specificamente destinati alla condivisione illecita di siffatti contenuti o promuova scientemente condivisioni del genere, il che può essere attestato dalla circostanza che il gestore abbia adottato un modello economico che incoraggia gli utenti della sua piattaforma a procedere illecitamente alla comunicazione al pubblico di contenuti protetti sulla medesima".

Quanto, poi, alla natura "attiva" o "passiva" del fornitore di un servizio di condivisione di video da parte dei suoi utenti, la CGUE ha determinato che ai fini dell'esclusione dell'esenzione di responsabilità prevista dall'art. 14, Dir. 2000/31/CE "un siffatto gestore deve essere al corrente degli atti illeciti concreti dei suoi utenti relativi a contenuti protetti che sono stati caricati sulla sua piattaforma", ulteriormente precisando inter alia che "la circostanza che il gestore di una piattaforma di condivisione di contenuti online proceda ad un'indicizzazione automatizzata dei contenuti caricati su tale piattaforma, che detta piattaforma contenga una funzione di ricerca e che essa consigli video in funzione del profilo o delle preferenze degli utenti non può essere sufficiente per considerare che detto gestore sia 'concretamente' al corrente di attività illecite realizzate sulla medesima piattaforma o di informazioni illecite ivi memorizzate"[300].

La creazione interpretativa di tale figura, di origine pretoria, viene giustificata sulla base del 42º Considerando della Direttiva 2000/31/CE secondo cui le esenzioni di responsabilità per i contenuti di terzi possono riguardare solo il provider la cui attività è di ordine meramente

[300] R. TRAINA CHIARINI, *L'evoluzione della responsabilità degli Internet Service Provider*, in *Corriere giur.*, 2021, p. 1435 ss.

tecnico, automatico e passivo il che implica che il prestatore di servizi non conosce, né controlla le informazioni trasmesse o memorizzate.

Più precisamente si legge che: "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''[301].

Secondo l'interpretazione della giurisprudenza europea, infatti, il servizio fornito dal prestatore di servizi di hosting di siti Internet, consistente nella memorizzazione d'informazioni, si caratterizza perché dura nel tempo.

Di conseguenza, detto prestatore di servizi di hosting può "venire a conoscenza del carattere illecito di talune informazioni da esso immagazzinate in un momento successivo rispetto a quello in cui si procede a detto immagazzinamento e nel quale esso è ancora in grado di intraprendere un'azione volta a rimuoverle o a disabilitarne l'accesso" mentre normalmente questa possibilità non l'ha chi esercita un mero servizio di trasporto delle informazioni ove, la registrazione dei dati non si prolunga nel tempo[302].

I prestatori di servizi sono, tuttavia, obbligati ad alcune incombenze informative ed operative che introducono di per sé delle responsabilità per gli stessi intermediari, pur non comportando l'obbligo di esaminare preventivamente le informazioni trasmesse o memorizzate sulle proprie macchine per valutarne la potenzialità lesiva per i terzi.

È preclusa dunque anche a livello europeo la fruizione dello scudo normativo in tutte quelle ipotesi in cui l'intermediario non si è limitato ad attività esclusivamente tecniche.

Già nel 2010 la Corte di Giustizia in *Google c. Louis Vuitton*, pur lasciando al giudice del rinvio l'indagine concreta circa il ruolo del provider, ha introdotto un filtro preventivo di valutazione della fattispecie legato allo svolgimento delle attività poste in essere concretamente dall'intermediario, ritenendo possibile l'applicabilità dei benefici di esonero solo nell'ipotesi in cui "il ruolo svolto da detto prestatore sia neutro, in quanto il suo

[301] 42° Considerando della Direttiva 2000/31/CE.
[302] CGUE, 15 settembre 2016, C-484/14, *Mc Fadden vs. Sony Music*, in *http://pluris-cedam.utetgiuridica.it.*

comportamento è meramente tecnico, automatico e passivo, comportante una mancanza di conoscenza o di controllo sui dati che memorizza"[303].

Nel 2011 la CGUE in *L'Oreal c. eBay*, pietra miliare che ha segnato una svolta nell'iter processuale della responsabilità del provider, ha cristallizzato il principio di diritto in virtù del quale il regime di favore della direttiva "si applica al gestore di mercato online qualora non abbia svolto un ruolo attivo che gli permetta di avere conoscenza o controllo circa i dati memorizzati"[304].

La Corte di Giustizia, interrogata sull'applicabilità dello scudo normativo espressamente previsto dall'art. 14 della Direttiva 2000/31, ha specificato che il regime di esonero dalla responsabilità non viene certamente intaccato dalla presenza di indici di attività meccanica e non manipolativa nel trattamento dei dati immessi, mentre la responsabilità del prestatore di servizi hosting sorge ogni qual volta vi sia un'attività di gestione, di qualsiasi natura, anche se limitata alla mera ottimizzazione o promozione delle informazioni di tali contenuti[305].

La Corte di giustizia ha infatti riconosciuto che la mera circostanza che il gestore di un mercato online memorizzi sul proprio server le offerte di vendita, stabilisca le modalità del suo servizio, sia ricompensato per quest'ultimo e fornisca informazione di ordine generale ai propri clienti, non può avere l'effetto di privarlo delle deroghe in materia di responsabilità previste dalla direttiva 31/2000, essendo necessario, ai fini dell'esclusione di tali deroghe, che il gestore abbia prestato un'assistenza consistente segnatamente nell'ottimizzare la presentazione delle offerte in vendita e nel promuovere le stesse.

In altri termini, la Corte di giustizia ha precisato che, affinché il prestatore di servizi della società dell'informazione possa godere del regime di esonero di responsabilità, è necessario che egli sia un "prestatore intermediario" che si limiti ad una fornitura neutra del servizio, mediante un trattamento puramente tecnico, automatico e passivo dei dati forniti dai suoi clienti, senza svolgere un ruolo attivo atto a conferirgli una conoscenza o un controllo dei medesimi dati e, quindi, a condizione che non abbia dato un pur minimo contributo all'editing del materiale memorizzato lesivo di diritti tutelati.

---

[303] CGUE, 23 marzo 2010, C-236/08, *Google France SARL e Google Inc. c. Louis Vuitton Mallettier SA*; CGUE, 23 marzo 2010, C-237/08, *Google France SARL c. Viaticum SA e Luteciel SARL* e CGUE, 23 marzo 2010, C-238/08, *Google France SARL c. Centre national recherche en relations humaines (CNRRH) SARL e altri*.

[304] CGUE, 12 luglio 2011, C-234/09, *L'Oréal SA e altri c. eBay International AG e a.*

[305] Questo è ribadito anche in CGUE, 11 settembre 2014, C-291/13, *Sotiris Papasavvas c. O Fileleftheros Dimosia Etaireia Ltd e a.*

In più la giurisprudenza europea ha altresì ribadito che il prestatore informatico non può usufruire dell'esonero da responsabilità se è al corrente di fatti o circostanze in base ai quale "un operatore economico diligente avrebbe dovuto constatare l'illiceità di cui trattasi"[306].

Per valutare la correttezza della decisione adottata dall'operatore economico diligente ed accertare se esso sia al corrente del fatto illecito altrui, il giudice europeo ha ulteriormente precisato che occorre prendere in esame "qualsiasi situazione nella quale il prestatore viene ad essere, in qualunque modo, al corrente di tali fatti o circostanze. […] Sarebbero infatti da contemplare tanto le ipotesi in cui il gestore di un mercato online scopra l'esistenza di un'attività o di un'informazione illecita a seguito di un esame effettuato di propria iniziativa quanto l'ipotesi in cui gli sia stata notificata l'esistenza di un'attività o di un'informazione siffatte"[307].

Anche con riferimento a questa seconda ipotesi, concernente direttamente il valore da attribuirsi, nel contesto della direttiva 2000/31, alla eventuale segnalazione effettuata dal danneggiato, il giudice europeo ha assunto una posizione che evita accuratamente rigidi automatismi e che appare emendabile e rivedibile sul terreno dell'applicazione concreta[308].

Piuttosto che semplificare l'azione dell'intermediario, si è giunti così ad aumentare la serie dei fatti che dovranno guidare la sua decisione.

Il vero punto focale della questione è dunque individuare - al di fuori dei soggetti di cui gli artt. 14, 15 e 16 e al di fuori di un vero obbligo di sorveglianza - quegli intermediari della rete che, effettuando delle attività, esemplificativamente individuate dalla Suprema Corte, traggano un vantaggio economico nell'attività di filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione o promozione dei contenuti in rete.

In tali casi, infatti, l'Internet Service Provider, lungi dallo svolgere un'attività di mera trasmissione, memorizzazione ovvero "ospitalità" del contenuto in rete, realizza una vera e propria gestione imprenditoriale del servizio che, quindi, genera ricchezza al pari di una qualunque attività lucrativa. Questa ricchezza illecita fa uscire l'intermediario informatico dal "*sicherenhafen"*, individuato della dottrina tedesca, per farlo "scontrare" con l'ordinario regime di responsabilità.

---

[306] *L'Oréal SA e altri c. eBay International AG e a*, cit.
[307] *L'Oréal SA e altri c. eBay International AG e a*, cit.
[308] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto,* cit., p. 156.

Ai fini del riconoscimento dell'hosting provider attivo devono essere tenute in considerazione innanzitutto l'organizzazione e la selezione dei contenuti forniti dagli utenti che siano operate al fine di ricavarne un profitto economico superiore a quello generalmente conseguibile con il mero servizio di hosting.

Un ruolo chiave è esercitato dall'inserzione di messaggi pubblicitari correlati alle ricerche condotte in rete dagli utenti.

Un importante rilievo, ai fini della qualificazione dell'attività del provider, deve essere attribuito anche all'esistenza di strumenti di ricerca che permettano agli utenti di reperire i contenuti desiderati per parole chiave, nonché alle funzioni di suggerimento dei contenuti basati sulle ricerche da questi precedentemente effettuate; all'esistenza di spiegazioni sul funzionamento della piattaforma e del linking; alla presenza di clausole contrattuali da cui possa dedursi un controllo sui contenuti degli utenti[309].

La Corte di Giustizia ha segnalato anche altri indici rilevanti ai fini della valutazione del grado di neutralità del prestatore, quali la redazione del messaggio promozionale che accompagna i link sponsorizzati nel servizio di posizionamento offerto da un motore di ricerca[310].

Infatti, la piattaforma crea valore supportando le interazioni fra i diversi gruppi. Il valore cresce nella misura in cui attira un maggior numero di utenti (c.d. effetto di rete). Tali piattaforme sovvenzionano un segmento di clientela che usufruisce del servizio a basso costo o gratuitamente per aumentare gli utenti e creare valore per attrarre utenti appartenenti ad un altro segmento di clientela: utenti paganti. Esse costituiscono un valore per un gruppo di utenti solo se è presente anche l'altro gruppo di clienti. In tale contesto, l'accesso ai video per cui è causa era gratuito, infatti il generico utente non doveva sostenere alcun costo per poter fruire degli stessi, fintantoché sono stati on line.

Sicché, in considerazione dell'"effetto rete", i video pubblicitari, considerata la loro popolarità, potrebbero aver aumentato gli utenti della piattaforma attirandone di nuovi, quantomeno nella sezione italiana del sito, e quindi creando valore per la società convenuta e per gli utenti paganti.

Affinché l'attività del prestatore di servizi perda il suo carattere di neutralità, e, con esso, l'esenzione di responsabilità, non è necessaria una conoscenza personale e diretta del

[309] Cass., 3 febbraio 2014, n. 3672, *Google-Vividown*, in *De Jure;* CGUE, *L'Oréal vs eBay* (C 324-09), 12 luglio 2011, cit.

[310] *Google France SARL and Google Inc.* v. *Louis Vuitton Malletier* SA (C-236/08), cit.

contenuto illecito, ma è sufficiente che i mezzi tecnologici dallo stesso utilizzati siano comunque idonei a conferirgli la conoscenza o il controllo dei dati memorizzati[311].

Pertanto, anche se il prestatore di servizi si avvale di un software per indicizzare, organizzare, catalogare, associare ad altri o alla pubblicità i video caricati dagli utenti, egli viene comunque a svolgere un ruolo attivo di ingerenza nei contenuti memorizzati, tale da permettergli di conoscere o controllare e di fornire un importante contributo all'editing del materiale memorizzato.

È evidente che se l'intermediario riesce a monitorare i contenuti immessi in rete per ricavare introiti economici mediante messaggi pubblicitari o operazioni a pagamento, è altrettanto chiaro che il suo ruolo gli consente un controllo dei dati e dunque sarebbe irragionevole sottrarlo al comune regime di responsabilità e far sì che lo stesso possa avvantaggiarsi dei meccanismi di esonero previsti.

Se questo regime "benevolo" nei confronti del provider poteva essere compreso negli anni passati, dato lo scarso sviluppo della tecnologia, oggi risulta difficile pensare che gli algoritmi, capaci ormai di controllare ed influenzare la vita, le informazioni e le comunicazioni degli utenti, non riescano ad intellegere un dato illecito, stesso dato che riescono a captare per trarne vantaggio economico.

Se l'algoritmo gestito dall'intermediario informatico rintraccia un elemento immesso in rete per ricavarne un tornaconto finanziario, sembra plausibile ritenere che possa farlo anche per evitare la commissione di fattispecie illecite.

Dunque, la mancata attivazione in tale ultimo senso non potrebbe che comportare l'affermazione della responsabilità del provider stesso, in concorso con l'utente ex art. 2055 c.c.

Quantomeno l'utente, che non può vedere i suoi diritti fondamentali sacrificati sull'altare dei bisogni sociali, dovrebbe poter beneficiare di un'inversione dell'onore della prova.

Sarebbe ragionevole ritenere che nel caso in cui l'attività dell'intermediario sia di natura passiva, si presumerà l'assenza di conoscenza e conoscibilità e sarà quindi il titolare del diritto a dover dimostrare il contrario.

Nel caso in cui il provider sia attivo, si presumerà la conoscenza o conoscibilità delle attività o dei contenuti illeciti e quindi l'*onus probandi* graverà sul prestatore informatico stesso.

Non può tuttavia non considerarsi che far gravare sull'internauta l'onore della prova, significherebbe sottoporlo ad una *probatio diabolica*.

[311] Trib. Roma, 10 gennaio 2019, n. 693, cit.

Il funzionamento degli algoritmi e la conoscenza dei meccanismi di operazione degli intermediari informatici sono imperscrutabili agli occhi di un soggetto danneggiato che non abbia conoscenze tecnico-scientifiche e specialistiche in campo informatico[312].

Chiedere al *quisque de populo* di dimostrare il coinvolgimento del prestatore nella commissione dell'illecito o la conoscibilità dell'evento-danno significherebbe cristallizzare un regime di assoluta e generale irresponsabilità degli intermediari.

Se è vero che un regime di responsabilità oggettiva rischierebbe di gravare troppo il provider e di alterare la libertà del *marketplace of idea* del web, è parimenti squilibrato a sfavore dell'user ipotizzare un regime di imputazione a carattere colposo che mantenga il riparto degli oneri probatori previsto dall'art. 2043 c.c.

Sarebbe pertanto auspicabile un meccanismo di inversione dell'onere della prova: in tal caso graverebbe sul provider, soggetto sicuramente dotato di uno status qualificato e di competenze tecniche e scientifiche, provare la sua non interferenza con la commissione dell'illecito da parte di un utente ai danni di un altro.

D'altra parte, se il provider può monitorare ed organizzare la gestione dei contenuti immessi dagli utenti, per trarne sostegno finanziario in ragione dello sfruttamento pubblicitario connesso alla prestazione di tali contenuti, non può non essere in grado di provare il suo eventuale mancato coinvolgimento.

Anche la giurisprudenza recente della Corte di giustizia dell'Unione europea ha dunque accolto la nozione di "hosting provider attivo", riferita a tutti quei casi che esulano da un' "attività dei prestatori di servizi della società dell'informazione che sia di ordine meramente tecnico, automatico e passivo, con la conseguenza che detti prestatori non conoscono né controllano le informazioni trasmesse o memorizzate dalle persone alle quali forniscono i loro servizi", mentre "(p)er contro, tali limitazioni di responsabilità non sono applicabili nel

---

[312] Questa argomentazione non è lontana da quanto autorevole dottrina ha magistralmente affermato per contestare l'applicabilità del regime della responsabilità da prodotto difettoso alle Intelligenze Artificiali: "La prova a carico del danneggiato non può riguardare, invece, lo specifico difetto del prodotto, che molto spesso potrà rimanere ignoto agli stessi soggetti che hanno partecipato, a vario titolo, alla catena di produzione, ma deve avere ad oggetto la dimostrazione di circostanze e fatti attinenti all'uso del prodotto dai quali sia possibile pervenire ad una prova presuntiva circa la sua dannosità. Infatti, è proprio il carattere "imperscrutabile" dell'intelligenza artificiale animata da algoritmi deep learning ad impedire che il soggetto danneggiato possa essere in grado di dimostrare in via diretta "il difetto" del prodotto e, eventualmente, il nesso eziologico con il danno. Allo stato delle attuali conoscenze, gli stessi scienziati che concorrono all'ideazione dell'algoritmo e i tecnici specializzati che provvedono alle operazioni di training non sempre sono in grado di spiegare «sulla base di quale iter e per quale ragione algoritmi di deep learning addivengano ad una particolare decisione o inducano a determinate condotte», soprattutto con riguardo alle cc.dd. "reti neurali". Non è possibile richiedere al danneggiato di provare un qualcosa (il difetto) che l'ideatore dell'algoritmo e/o lo stesso produttore della macchina potrebbero non essere in grado di conoscere".
Il riferimento è ad A. PROCIDA MIRABELLI DI LAURO, *Intelligenze artificiali e responsabilità civile*, cit., p. 530, 531 ss.

caso in cui un prestatore di servizi della società dell'informazione svolga un ruolo attivo", richiamando a tal fine il considerando 42 della direttiva.

La Comunicazione della Commissione europea COM (2017) 555 del 28 settembre 2017, intitolata "Lotta ai contenuti illeciti online. Verso una maggiore responsabilizzazione delle piattaforme online", ha preso parimenti atto dell'orientamento della Corte di giustizia, secondo cui la deroga alla responsabilità di cui all'art. 14 della direttiva è disponibile solo per i prestatori di servizi di hosting "che non rivestono un ruolo attivo".

Tale Comunicazione della Commissione ha offerto alcuni orientamenti alla luce del quadro giuridico vigente.

Essa rileva come le piattaforme online, ad oggi, "dispongono solitamente dei mezzi tecnici per identificare e rimuovere" i contenuti illeciti e che, alla luce del "progresso tecnologico nell'elaborazione di informazioni e nell'intelligenza artificiale, l'uso di tecnologie di individuazione e filtraggio automatico sta diventando uno strumento ancora più importante nella lotta contro i contenuti illegali online".

Attualmente, come sostenuto anche dalla suprema Corte (nella già ricordata sentenza 7708/2019), molte grandi piattaforme utilizzano una forma di algoritmo di abbinamento basata su una serie di tecnologie, dal semplice filtraggio dei metadati fino all'indirizzamento calcolato e alla marcatura (*fingerprinting*) dei contenuti[313].

Gli strumenti tecnologici possono essere usati con un maggiore livello di affidabilità per marcare e filtrare (rimozione permanente) i contenuti che sono stati identificati e valutati come illegali, mediante riconoscimento automatico dei contenuti e procedure automatiche di rimozione permanente: insomma, mediante procedure automatiche, volte a prevenire la ricomparsa di contenuti illegali online[314].

Tale attività di rintraccio telematico del contenuto digitale tutelato può essere tecnicamente effettuata mediante specifici programmi software, basati sull'utilizzo di "impronte digitali" (c.d. *fingerprint*) abbinate univocamente al contenuto digitale tutelato[315].

Quello in esame è, peraltro, un profilo squisitamente di merito, che presuppone un ineludibile accertamento in fatto, con l'ausilio di un esperto in ragione dei profili tecnici coinvolti, mediante consulenza tecnica d'ufficio.

---

[313] Nel settore del diritto d'autore, per esempio, il riconoscimento automatico dei contenuti si dimostra uno strumento efficace da diversi anni, addirittura in funzione "proattiva", escludendo però che questo possa di per sé implicare, ex adverso, la perdita della deroga alla responsabilità.

[314] Questo si evince chiaramente anche dalla Comunicazione della Commissione europea COM (2017) 555 del 28 settembre 2017.

[315] E. TOSI, *Obblighi di filtraggio ex post di contenuti illegali illeciti equivalenti e responsabilità civile degli hosting provider*, in *Dir. ind.*, 2020, p. 284 ss.

Esiste un obbligo di filtraggio special-preventivo quando il provider, utilizzando di funzionalità tecniche minime e senza subire un sacrificio sproporzionato, è in grado di impedire nuovi caricamenti di elementi oggetto di segnalazione e rimossi a seguito di ingiunzione del tribunale.

Quanto alle tecniche di filtraggio e *fingerprinting* idonee al raggiungimento dello scopo, tra le più utilizzate vi sono:

- il "*watermarking*", ossia l'introduzione nel file video di informazioni aggiuntive che "marchiano" ogni fotogramma come un tatuaggio digitale
- il "*video fingerprinting*", di particolare rilievo per gli scopi dell'analisi in esame.

Analogamente a quanto avviene nel caso delle impronte digitali delle persone, consiste nel rilevare alcuni elementi che caratterizzano univocamente il file (video/audio) e nel memorizzarli in una base dati, in modo che sia possibile confrontare successivamente qualsiasi video con le tracce presenti in tale archivio, al fine di identificare la presenza di sequenze riconducibili al file originario[316].

Una volta realizzato l'archivio delle "impronte", esso può essere utilizzato per confrontare le "impronte" memorizzate con le "impronte" dei nuovi contenuti.

A titolo esemplificativo nel caso Vimeo, il CTU ha accertato che la stessa Vimeo ha adottato, nel corso dell'anno 2014, il sistema "*Copyright Match*" con la collaborazione di *Audible Magic*, al fine di identificare i video che contengono musica soggetta a copyright, ma ha altresì precisato che la tecnica adottata per gli audio consentirebbe anche l'analisi dei contenuti video.

Anche Google, un provider analogo a Vimeo, ha creato un sofisticato meccanismo per controllare l'uso illegittimo di contenuti audio/video nella piattaforma *YouTube* che consente ai proprietari di contenuti di sottomettere i propri file per elaborarne il relativo fingerprint e memorizzarlo nell'archivio appositamente predisposto dalla stessa YouTube.

In tal modo, ogni nuovo video aggiunto alla piattaforma è dapprima confrontato con l'archivio centrale dei fingerprint e solo dopo esito negativo viene messo a disposizione degli utenti.

Tale sistema, attivo su YouTube dalla seconda metà del 2007 è noto con il nome di "Content ID".

Il CTU ha quindi concluso il c.d. video *fingerprinting* "costituiva all'epoca dei fatti (e continua ad esserlo tuttora), la tecnica più efficace ed efficiente per il controllo sia preventivo

[316] Lo ricorda anche Trib. Roma, 10 gennaio 2019, n. 693, cit. p. 397 ss.

(ex-ante, cioè effettuato prima della pubblicazione dei video) sia successivo (ex-post, cioè effettuabile anche dopo la pubblicazione dei video) dei contenuti da pubblicare o pubblicati, ed alle cui risultanze subordinare la stessa pubblicazione e/o la permanenza online del contenuto audiovisivo considerato[317].

Nella prospettiva descritta e fatta propria dalla Suprema Corte, sembra potersi sostenere che i prestatori di servizi Internet - in specie di hosting -, che nello svolgimento della loro attività omettano di adottare sistemi di filtraggio dei contenuti generalmente utilizzati e consentiti dallo stato attuale della tecnica, dovrebbero essere chiamati a rispondere dell'inosservanza degli obblighi di diligenza che su di loro incombono in qualità di operatori professionali.

Si può considerare sotteso alla disciplina della responsabilità civile del fornitore di servizi Internet un principio inderogabile, dettato nell'interesse della collettività in generale, che, in presenza di situazioni potenzialmente dannose per gli utenti, quali, appunto quelle che, a certe condizioni, può prospettare la rete Internet, impone a tale operatore di attivarsi per evitare e/o impedire il protrarsi dell'evento dannoso, risultando essere l'unico soggetto o comunque quello meglio in grado di provvedervi.

L'adozione di sistemi di filtraggio non implica di per sé la perdita automatica dei benefici previsti ex lege, d'altra parte ciò comporterebbe la fuga dei providers dai sistemi di filtraggio e dagli investimenti nella ricerca e nello sviluppo di sistemi sicuri, ma non può non comportare un aggravio ed un meccanismo operativo di responsabilità più rigido e più adatto all'odierna realtà digitale.

La peculiarità dell'*enforcement* algoritmico discende dal fatto che esso implica un'ampia raccolta di dati da fonti più diverse, che vengono poi analizzati tramite programmi che presentano diversi livelli di complessità, e il cui risultato viene successivamente utilizzato all'interno del processo decisionale.

In sostanza, la mole di dati che gli intermediari raccolgono rappresenta l'input che alimenta gli algoritmi che devono poi dire se un contenuto è illecito, e quindi deve essere automaticamente rimosso, o non deve proprio essere immesso in rete, o è invece lecito, e quindi può restare online e se ne può continuare il caricamento da parte dell'utente[318].

Tenuto a mente il divieto esistenziale di imporre ai provider obblighi generali di monitoraggio preventivo e ricerca attiva, nel contesto tecnologico attuale le "misure proattive" per "impedire in futuro il caricamento di specifiche opere non autorizzate"

[317] M. IASELLI, *I contorni della responsabilità dell'hosting provider attivo*, in *Dir. ind*., 2019, p. 399 ss.
[318] M.L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, cit., p. 224.

possono prendere un'unica forma: quella dei filtri automatici. Si tratta di software fondati su tecnologie *ACR* ("*automated content recognition*").

Sulla scorta di database e parametri preimpostati dai titolari dei diritti, questi strumenti sono in grado di verificare in modo automatico se un dato contenuto corrisponde a un altro già considerato illecito da un'autorità giudiziaria e, in quest'ultimo caso, metterne a conoscenza il titolare del diritto che può impedirne la pubblicazione, rimuoverlo o sfruttarlo economicamente.

In questa prospettiva, questo tipo di strumenti possono risolvere i conflitti prevenendo il loro insorgere, mitigando le conseguenze di una violazione o permettendo al titolare di sfruttare economicamente la violazione del suo diritto. Il tutto attraverso capacità computazionali immensamente più elevate rispetto a quelle umane.

I software basati su tecnologie ACR e dediti all'individuazione, blocco o valorizzazione di contenuti illeciti "sono una realtà del settore delle piattaforme di contenuti generati dagli utenti da molto tempo prima che diventasse di moda chiamarli 'intelligenza artificiale'"[319].

La sentenza della Corte di cassazione del 2019, che ha il pregio di aver individuato una linea univoca e di aver fatto chiarezza, ha introdotto anche l'obbligo di impedire altre violazioni dello stesso tipo ovvero un obbligo del prestatore di astenersi di pubblicare contenuti illeciti dello stesso tipo di quelli già riscontrati come violativi dell'altrui diritto e, di conseguenza, l'ammissibilità di una pronuncia di inibitoria in tal senso.

Ciò è possibile in presenza ormai della identificazione dei cd. url[320] o della constatata possibilità per il prestatore di identificarli mediante i propri mezzi tecnici.

Tale obbligo, invero, in nulla è parificabile a quello - insussistente ex art. 17 d.lgs. n. 70 del 2003, - di vigilanza generale e preventiva sui contenuti immessi dagli utenti: posto che la situazione di ignoranza di quei contenuti (legittima e tutelata dalla norma ora richiamata) è per definizione venuta meno, una volta reso edotto il prestatore dalla comunicazione proveniente dal soggetto leso.

---

[319] A. BELLAN, *Piattaforme, obblighi di monitoraggio e risoluzione delle controversie online*, in *Dir. ind.*, 2020, p. 187 ss.

[320] L'URL (*Uniform Resource Locator*) è una sequenza di caratteri che identifica una risorsa "*astratta o fisica*" su internet e fa parte della più ampia categoria degli URI (*Uniform Resource Identifier*).
Mentre l'URI è un identificatore univoco del contenuto virtuale che non può, in quanto tale, richiamare direttamente il documento, l'URL lo localizza e ne fornisce il "meccanismo primario" di accesso. A questo fine, il primo elemento della sequenza in un URL è il cd. protocollo (solitamente "http").
I software per la navigazione in internet (cioè i *browser*) si basano su questi standard, attingendo dai protocolli e dai relativi *link* per trasmettere le pagine richieste - e corrispondenti alle parole ricercate - agli utilizzatori.
Cfr., G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione-Corso d'informatica giuridica*, Torino, 2016, pp. 233-234.

Al riguardo, può essere utile richiamare le affermazioni della Corte UE, in particolare il noto caso *Telekabel c. Costantin*, secondo cui gli Stati membri devono prevedere l'adozione di misure che abbiano la funzione "non solo di far cessare le violazioni inferte al diritto d'autore o ai diritti connessi, ma altresì di prevenirle" e che nulla osta ad imporre ai provider un ordine inibitorio che possa avere per lo stesso un "costo notevole", imponendo di bloccare non solo l'accesso all'indirizzo su cui i contenuti illeciti risultano allo stato pubblicati, ma anche "ogni altro indirizzo futuro di cui tale società possa venire a conoscenza"[321].

Ciò, evidentemente, in ragione del fatto che essi si trovano nella migliore condizione non solo per porre fine alle violazioni già commesse dagli utenti attraverso i servizi forniti, ma anche per impedire il compimento di nuove violazioni, in chiave di tutela preventiva e anticipatoria.

La questione relativa alla possibilità per i titolari dei diritti lesi di esercitare azioni inibitorie nei confronti degli Internet service providers - in particolare di hosting - tese al blocco dei contenuti intermediati e/ o dei siti - in specie nell'àmbito della tutela del diritto d'autore nel mercato digitale- al fine non solo di rimuovere le violazioni già inferte, ma anche di impedire che ne vengano compiute di nuove, è stata, peraltro, risolta positivamente dalla Corte di giustizia a più riprese.

Al riguardo, la Corte di giustizia ha riconosciuto la legittimità, in via di principio, di un'ingiunzione (purché pronunciata da un giudice) che vieti al prestatore di concedere ai suoi abbonati l'accesso ad un sito Internet che metta in rete materiali protetti dal diritto d'autore senza il consenso dei titolari dei diritti, a condizione, però, che detta ingiunzione non specifichi le misure da adottare in concreto per impedire o, almeno, rendere difficili e scoraggiare le consultazioni non autorizzate dei materiali protetti, ma rimetta al fornitore la relativa scelta e gli consenta di sottrarsi alla propria responsabilità, dimostrando di aver adottato tutte le misure ragionevoli, che comunque non privino inutilmente gli utenti della possibilità di accedere in modo lecito alle informazioni disponibili.

In tal modo, la Corte offre al giudice nazionale -chiamato ad un notevole sforzo interpretativo nella determinazione del contenuto degli specifici provvedimenti inibitori da adottare in riferimento al singolo caso concreto - la chiave interpretativa per una corretta attuazione dei principi di proporzionalità, adeguatezza e ragionevolezza cui devono sottostare i rimedi di blocco a tutela dei diritti in ambito digitale.

[321] CGUE, 27 marzo 2014, C314/12, *Telekabel Wien c. Costantin Film,* in *De Jure.*

In più viene fissato il grado di diligenza professionale cui è chiamato il prestatore nel conformarsi all'ingiunzione ricevuta, riconoscendogli la potestà di adottare le misure che più si adattano alle risorse e alla capacità di cui dispone e che risultino rigorosamente giustificate alla luce dell'obiettivo perseguito, senza, tuttavia, imporre inutili e ingiustificati sacrifici delle altre due libertà fondamentali confliggenti: la libertà di impresa di cui il provider stesso è titolare e le libertà di espressione e di informazione dei fruitori di Internet, cui va garantita la massima espansione.

Anche la Corte di cassazione con la citata sentenza n. 7708/2019, in linea con il recente orientamento della Corte di Giustizia[322], ha ritenuto ammissibile l'imposizione in capo all'ISP di "un obbligo di astenersi di pubblicare contenuti illeciti dello stesso tipo di quelli già riscontrati come violativi dell'altrui diritto": obbligo che implica filtraggio dei contenuti digitali pubblicati successivamente all'inibitoria giudiziale.

Ancor più di recente, i principi espressi dalla Corte di Cassazione sono stati sia confermati dalle decisioni della Corte di Giustizia, sia applicati dalle nostre Corti di merito.

Proprio in tema di obbligo di prevenire la commissione di ulteriori illeciti dello stesso tipo di quelli già riscontrati e di cui l'hosting provider abbia già acquisito conoscenza, la Corte di Giustizia UE, con la già ricordata sentenza del 3 ottobre 2019 emessa nella causa C-18/2018 (*Eva Glawischnig-Piesczek c. Facebook Ireland Limited*), ha affermato che l'art. 15, par. 1, Dir. 2000/31/CE (corrispondente all'art. 17, d.lgs. n. 70/2003) "non osta a che un giudice di uno Stato membro possa:

- ordinare a un prestatore di servizi di hosting di rimuovere le informazioni da esso memorizzate e il cui contenuto sia identico a quello di un'informazione precedentemente dichiarata illecita o di bloccare l'accesso alle medesime, qualunque sia l'autore della richiesta di memorizzazione di siffatte informazioni;
- ordinare a un prestatore di servizi di hosting di rimuovere le informazioni da esso memorizzate e il cui contenuto sia equivalente a quello di un'informazione precedentemente dichiarata illecita o di bloccare l'accesso alle medesime, purché la sorveglianza e la ricerca delle informazioni oggetto di tale ingiunzione siano limitate a informazioni che veicolano un messaggio il cui contenuto rimane sostanzialmente invariato rispetto a quello che ha dato luogo all'accertamento d'illeceità...".

La stessa sentenza si è occupata, poi, di un'altra questione di forte interesse, stabilendo che un Giudice nazionale possa "ordinare a un prestatore di servizi di hosting di rimuovere le

[322] CGUE, 3 ottobre 2019, C-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland Limited,* in *Dir. ind.*, 2020, p. 281 ss.

informazioni oggetto dell'ingiunzione o di bloccare l'accesso alle medesime a livello mondiale" e, quindi, senza limitazioni territoriali legate al foro di competenza.

Il principio dell'effettività della tutela per le vittime di diffamazione su Facebook impone al provider l'obbligo di sorveglianza specifica preventiva di contenuti identici e/o equivalenti a quelli dichiarati illeciti.

Nessun contrasto con il divieto di sorveglianza generale del provider a patto che l'ingiunzione sia talmente precisa e circostanziata da non consentire una valutazione autonoma del gestore. La rapidità e l'estensione geografica degli illeciti on line nonché la voluta assenza di limitazioni anche territoriali dell'ingiunzione richiedono l'applicazione a livello globale del comando del giudice.

Nessun contrasto con il divieto di sorveglianza generale del provider a patto che l'ingiunzione sia rispettosa del diritto internazionale[323].

La scelta dogmatica della giurisprudenza della Suprema Corte di teorizzare e definire l'hosting attivo, delineando i caratteri della relativa responsabilità civile e ampliando i confini della conoscenza alla conoscibilità dell'illecito – secondo il parametro qualificato della diligenza tecnica – a ben vedere evidenzia tutta la sensibilità giuridica di chi avendo ravvisato l'orizzonte di un nuovo ed evoluto mercato elettronico teorizza nuovi e più calzanti scenari giuridici.

La scelta di campo, infatti, coglie perfettamente l'evoluzione del mercato economico elettronico e risponde alle relative nuove esigenze.

Si è passati, infatti, dagli albori del fenomeno con la legge di settore nel 2003, allorquando la normativa aveva quale preciso obiettivo la tutela e la promozione della crescita e dello sviluppo del mercato e degli operatori economici che investivano nel "nuovo mondo" di Internet e, quindi, teorizzava quasi una pionieristica irresponsabilità del gestore di quel mercato, all'odierna battuta di arresto.

La Suprema Corte "ha compreso che l'allora neonata rete è, ormai, cresciuta e può camminare con le proprie gambe! Ed allora quale sarà il futuro di internet nell'età adulta? Se cambia lo scenario allora devono cambiare le regole e, pertanto, la vera affermazione del mercato elettronico evoluto non poteva prescindere da una maggiore tutela dell'utente della rete che corrisponde, di converso, ad un aggravamento delle forme di responsabilità a carico dell'intermediario del commercio elettronico e, pertanto, l'emozione dello studioso, che ha visto nascere il mercato elettronico quando approfondiva il tema nel 2003, nel leggere queste

[323] D. BIANCHI, *Facebook: filtraggio globale e specifico dei contenuti equivalenti per il diffamato, in D&G,* 2019, p. 3 ss.

pagine della Suprema Corte, a distanza di sedici anni è quella di aver visto il bambino internet nascere, accompagnato da una tutela rilevantissima in termini di deresponsabilità per, poi, camminare da solo, quale uomo adulto e, pertanto, responsabile delle proprie condotte"[324].

Sul piano normativo, si segnala che la recente direttiva 2019/ 790/UE, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE, all'art. 17, chiama i prestatori di servizi di condivisione di contenuti on-line a cooperare con i titolari dei diritti per evitare che nei loro servizi siano disponibili opere e altri materiali protetti dal diritto d'autore caricati dagli utilizzatori dei servizi stessi, in assenza delle previste autorizzazioni, prevedendo espressamente che tale cooperazione possa condurre alla disabilitazione dell'accesso o alla rimozione dei contenuti.

Ancora, dispone altresì che essi sono ritenuti responsabili se non dimostrano di aver compiuto i massimi sforzi secondo elevati standard di diligenza professionale di settore per assicurare che non siano disponibili opere e altri materiali specifici per i quali abbiano ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti e, in ogni caso, ove non provino di aver agito tempestivamente, dopo aver ricevuto una segnalazione sufficientemente motivata dai titolari dei diritti, per disabilitare l'accesso o rimuovere dai loro siti web le opere o altri materiali oggetto di segnalazione e per impedirne il caricamento in futuro.

Peraltro, già il considerando n. 40 della direttiva sul commercio elettronico, riconosce che risponde all'interesse di tutte le parti attive nella prestazione dei servizi della società dell'informazione - e dunque, anche degli Internet Service Providers, in virtù della loro posizione tecnica ed economica - l'istituzione e applicazione di sistemi rapidi e affidabili idonei a rimuovere le informazioni illecite e disabilitare l'accesso alle medesime e all'interesse di tutti gli interessati lo sviluppo e utilizzo effettivo di "sistemi tecnici di protezione e identificazione, nonché strumenti tecnici di sorveglianza resi possibili dalla tecnologia digitale, entro i limiti fissati dalle direttive 97/46/CE e 97/66/CE", in tema di riservatezza.

Nei suoi lineamenti essenziali è previsto infatti dalla direttiva sul diritto d'autore nel mercato unico digitale che quelle piattaforme che memorizzano e danno accesso a grandi quantità di opere e altro materiale caricato dagli utenti hanno l'obbligo di munirsi di tecnologie efficaci per il riconoscimento dei contenuti, adeguate e proporzionate.

[324] R. BOCCHINI, *La responsabilità civile plurisoggettiva, successiva ed eventuale dell'ISP*, cit., p. 2615 ss.

Il cuore della riforma sposta quindi il punto di equilibrio rispetto alla direttiva sul commercio elettronico: ora infatti è l'intermediario a dover agire proattivamente per evitare le violazione dei diritti[325].

Sull'intermediario grava un obbligo di risultato alla cui violazione segue la riattivazione delle regole ordinarie di responsabilità.

L'adozione di riconoscimento automatico dei contenuti indicata nella originaria Proposta della Commissione appare un esito coerente con la qualificazione non neutra dell'attività compiuta dagli intermediari.

Ciò lascia sottintendere l'uso da parte del prestatore informatico di quelle tecnologie atte a identificare e a gestire facilmente ex ante i contenuti caricati sulla piattaforma[326].

Il prestatore definito dall'art. 2, n. 6[327], della nuova direttiva non si limita a svolgere l'attività di hosting in senso stretto, così come definita dall'art. 14 dir. 2000/31/CE, ma svolge quell'ulteriore attività che spesso ha portato la giurisprudenza a qualificare l'hosting provider come attivo e, conseguente, a sottrarlo dall'ambito di applicazione del menzionato art. 14[328].

Quindi la figura dell'hosting provider attivo inizia a trovare anche i primi riconoscimenti normativi: il legislatore aspira ad una normativa più idonea al contesto tecnologico oggi esistente[329].

Questa norma è chiaramente riferita alla tutela dei diritti d'autore nell'ambiente digitale, che si basa sugli accordi e sulla cooperazione di buona fede tra provider ed utente, ma in generale la policy che viene fuori è quanto mai comprensiva e a maggior ragione valida per la tutela dei diritti fondamentali dell'individuo.

---

[325] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., pp. 232 e 233.

[326] F. PIRAINO, *Spunti per una rilettura della disciplina giuridica degli Internet service provider*, in *AIDA*, 2017, p. 513 ss.

[327] Il prestatore di servizi di condivisione di contenuti online, per essere qualificato come tale, non deve limitarsi a memorizzare e dare accesso al pubblico alle opere protette, ma deve altresì` organizzare e promuovere le opere stesse a scopo di lucro. Letteralmente la disposizione legislativa prevede: "«prestatore di servizi di condivisione di contenuti online»: un prestatore di servizi della società dell'informazione il cui scopo principale o uno dei principali scopi è quello di memorizzare e dare accesso al pubblico a grandi quantità di opere protette dal diritto d'autore o altri materiali protetti caricati dai suoi utenti, che il servizio organizza e promuove a scopo di lucro".

[328] M. BELLI, *La responsabilità dei «prestatori di servizi di condivisione di contenuti online» ai sensi della Dir. 2019/790/UE*, in *NLCC*, 2020, p. 556 ss.

[329] F. DI CIOMMO, *Oltre la direttiva 2000/31/Cee, o forse no. La responsabilità del provider di Internet nell'incerta giurisprudenza europea*, in *Foro it.*, 2019, c. 2045 ss.; E. TOSI, *La disciplina applicabile all'hosting provider per la pubblicazione di contenuti digitali protetti dal diritto d'autore, tra speciale irresponsabilità dell'ISP passivo e comune responsabilità dell'ISP attivo, alla luce di Cassazione 7708/2019 e 7709/2019*, in *Riv. dir. ind.*, 2019, p. 201 ss.; R. BOCCHINI, *Responsabilità civile dell'hosting provider*, cit., p. 2604 ss.; M. L. GAMBINI, *La responsabilità dell'internet service provider approda al vaglio della Cassazione*, cit., p. 177 ss.

Dunque, resta ferma la responsabilità del provider a meno che questi dimostri di aver agito secondo i più elevati standard di diligenza professionale.

Ancora, in tal senso anche la recente direttiva Copyright 2019/719 ha introdotto un profilo di responsabilità in capo ai prestatori di servizi di condivisione di contenuti online, i quali, concedendo l'accesso al pubblico ad opere protette dal diritto d'autore o ad altri materiali protetti caricati dagli utenti, escono dal regime dell'irresponsabilità - compiendo un atto di comunicazione al pubblico di messa a disposizione del pubblico senza le necessarie autorizzazioni[330].

In tal senso l'art. 17, quarto comma, della direttiva afferma la responsabilità dei prestatori di servizi che non dimostrino di:

a) aver compiuto i massimi sforzi per ottenere un'autorizzazione;

b) aver compiuto, secondo elevati standard di diligenza professionale di settore, i massimi sforzi per assicurare che non siano disponibili opere e altri materiali specifici per i quali abbiano ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti; e in ogni caso;

c) aver agito tempestivamente, dopo aver ricevuto una segnalazione sufficientemente motivata dai titolari dei diritti, per disabilitare l'accesso o rimuovere dai loro siti web le opere o altri materiali oggetto di segnalazione e aver compiuto i massimi sforzi per impedirne il caricamento in futuro conformemente alla lettera b).

Si è avuto modo di riflettere anche sul fatto che, a proposito della recente normativa sul cyberbullismo, la definizione contenuta, nell'art. 1, 2º comma, L. n. 71/2017, sembra avvalorare la recente creazione dogmatica, ad opera della giurisprudenza di quella quarta figura di provider che è appunto il c.d. hosting provider attivo.

La presente legge si pone l'obiettivo di contrastare il fenomeno del cyberbullismo in tutte le sue manifestazioni, con azioni a carattere preventivo e con una strategia di attenzione, tutela ed educazione nei confronti dei minori coinvolti, sia nella posizione di vittime sia in quella di responsabili di illeciti, assicurando l'attuazione degli interventi senza distinzione di età nell'ambito delle istituzioni scolastiche.

Per "cyberbullismo" si intende qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché' la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di

[330] In tal senso, si veda anche la proposta di direttiva del Parlamento europeo e del Consiglio sul diritto d'autore nel mercato unico digitale COM/2016/0593 final-2016/0280 (COD).

isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo.

In più, la norma definisce il «gestore del sito Internet», identificandolo come un prestatore di servizi della società dell'informazione, diverso da quelli di cui agli articoli 14, 15 e 16 del decreto legislativo 9 aprile 2003, n. 70, che, sulla rete internet, cura la gestione dei contenuti di un sito in cui si possono riscontrare le condotte di cui al comma 2.

La norma, dunque, postulando l'esistenza di un ''gestore del sito Internet'', e cioè di un intermediario di Internet che non rientri nelle categorie di cui agli artt. 14, 15 e 16, d.lgs. n. 70/2003, potrebbe far riferimento a quei soggetti che, pur svolgendo un servizio della società dell'informazione, non siano meri hosting provider passivi.

Dunque, anche sul versante normativo l'orientamento verte verso una responsabilizzazione del provider.

5. I poteri inibitori esperibili in ambiente digitale. Quali i doveri dei provider?

L'esame della giurisprudenza della Corte di giustizia ha rilevato, sin dalle decisioni *L'Oréal c. eBay*[331] e *Telekabel c. Costantin*[332], la possibilità di imporre agli intermediari una grande varietà di ordini inibitori esperibili nei confronti dei provider.

Gli Stati membri devono prevedere l'adozione di misure che abbiano la funzione "non solo di far cessare le violazioni inferte al diritto d'autore o ai diritti connessi, ma altresì di prevenirle" e nulla osta ad imporre ai provider un ordine inibitorio che possa avere per lo stesso un "costo notevole", imponendo di bloccare non solo l'accesso all'indirizzo su cui i contenuti illeciti risultano allo stato pubblicati, ma anche "ogni altro indirizzo futuro di cui tale società possa venire a conoscenza"[333].

---

[331] *L'Oréal c. eBay*, cit.

[332] *Telekabel c. Costantin*, cit.

[333] Si veda sul punto anche Trib. Milano, Sez. specializzata in materia di impresa, 12 aprile 2018, *Arnoldo Mondadori Editore s.p.a. c. Fastweb s.p.a., Telecom Italia s.p.a., Tiscali Italia s.p.a., Vodafone Italia s.p.a., Wind Tre s.p.a.*, in *AIDA*, 2018, p. 1874 ss., secondo cui: "La mancanza in giudizio degli autori degli illeciti (nella specie: i titolari dei siti web ospitanti i contenuti protetti dal diritto d'autore) non esclude l'ammissibilità della domanda cautelare nei confronti dei terzi intermediari, quali sono i fornitori di servizi di connessione ad Internet, in quanto tra gli uni e gli altri non è ravvisabile un litisconsorzio necessario. Indipendentemente dalla loro responsabilità nelle violazioni l'autorità giudiziaria può disporre contro gli intermediari di servizi di connessione ad Internet i provvedimenti cautelari idonei a vietare la prosecuzione degli illeciti e prevenirne la ripetizione. È compatibile con il divieto di gravare gli ISP di oneri generali di sorveglianza irrogare ad un prestatore di servizi di connessione ad Internet l'ordine di adottare le più opportune misure tecniche per disabilitare l'accesso ai medesimi contenuti già accertati come illeciti - a prescindere dal nome di dominio del sito web, in continua mutazione per deliberata e palese volontà dell'autore della violazione - subordinando l'efficacia del comando cautelare all'invio formale (per PEC o raccomandata con avviso di ricevimento) dal ricorrente al resistente di una specifica segnalazione delle nuove violazioni. Qualora il prestatore di servizi di connessione alla rete sia destinatario dell'ordine di disabilitare l'accesso degli utenti ai siti cd. 'alias' (in quanto ospitanti i medesimi contenuti già qualificati come illeciti in via cautelare dall'autorità giudiziaria) che gli

Questo nella misura in cui tali ordini siano concretamente eseguibili, proporzionati ed efficaci, avendo "l'effetto di impedire o, almeno, di rendere difficilmente realizzabili" le violazioni.

La Corte di giustizia, nel determinare in concreto il contenuto del provvedimento che il giudice nazionale potrebbe essere chiamato ad adottare, ha suggerito alcune misure inibitorie:

a) la possibilità di ordinare al gestore di un mercato online la sospensione dell'autore della violazione, mediante ad esempio un ordine di chiusura dell'account dell'utente resosi ripetutamente autore del fatto illecito;
b) la possibilità di ingiungere ai gestori di tali spazi digitali l'adozione di misure volte a facilitare l'identificazione degli users allo scopo di garantire al danneggiato il diritto ad un ricorso effettivo contro gli autori del fatto illecito.

A ben guardare, nell'ambito del diritto d'autore digitale, si tratta degli stessi profili rimediali esperibili sulla base di puntuali disposizione legislative nel diritto statunitense: la *policy of repeat infringer* ed il *subpoena to identify infringer*[334].

Conseguentemente, i fornitori di servizi di hosting possono essere destinatari di ordini inibitori che non siano limitati alla rimozione di una data informazione illecita ma che abbia l'effetto di obbligare l'operatore a ricercare e rimuovere non solo tutti i contenuti identici a quello qualificato illecito ma anche tutti i contenuti equivalenti, che riproducano nella sostanza il contenuto qualificato illecito, qualunque sia l'autore della richiesta di memorizzazione delle medesime.

In altri termini, resta ferma la possibilità che Corti o Autorità amministrative adottino le ingiunzioni necessarie a far cessare o prevenire la commissione di illeciti, ai sensi degli artt. 12-14 della direttiva e degli ultimi commi degli artt. 14-16 del decreto attuativo.

Lo stesso considerando 48 della direttiva rafforza la possibilità per gli stati membri di richiedere agli intermediari di adempiere al dovere di diligenza che è ragionevole attendersi ai fini dell'individuazione di attività illecite.

---

siano specificamente segnalati dal ricorrente dopo l'irrogazione del comando cautelare l'assenza di responsabilità dell'ISP nelle correlative violazioni dei diritti d'autore giustifica l'attribuzione a suo beneficio resistente del diritto di richiedere al predetto ricorrente il rimborso delle spese tecniche, strettamente necessarie ed inerenti, sopportate per ottemperare alla misura giudiziale. Nel caso di irrogazione di penalità di mora a tutela dei diritti di proprietà intellettuale l'art. 614 bis c.p.c. affida alla responsabilità del creditore l'allegazione e la prova del concreto realizzarsi delle condotte inibite dall'ordinanza cautelare, per sua natura immediatamente esecutiva; mentre al debitore è assicurata la possibilità di contestare queste allegazioni circa l'intervenuta violazione dell'inibitoria in sede di incidente di esecuzione".

[334] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., pp. 194, 195 e 196.

Nel corso degli ultimi anni questo strumento è stato sempre più utilizzato a livello nazionale ed europeo dalle corti, al fine di predisporre obblighi di attivazione degli intermediari sempre più generici ed impegnativi, a tutela dei diritti reputazionali – esemplificativa è a tal proposito la tutela in materia di protezione dei dati personali – e dei diritti di proprietà intellettuale.

I profili rimediali più spesso invocati nell'ultimo decennio, specie nella tutela del diritto d'autore, sembrano indirizzarsi non più nella direzione della reazione aquiliana per mancata rimozione dei contenuti illeciti ma verso l'esperibilità di misure inibitorie che tendano a cooptare l'intermediario nel contrasto al fenomeno della pirateria digitale[335].

Le misure inibitorie esperibili nei confronti dei prestatori sono volte ad imporre condotte idonee ad evitare che dall'uso dei loro servizi derivino eventi pregiudizievoli.

Il comando inibitorio consisterà dunque non tanto nell'ordine di astenersi da una determinata azione quanto in quello più oneroso di tenere un determinato comportamento.

Occorre pertanto un "*fair balance*", un giusto equilibrio tra i diversi diritti fondamentali tutelati dall'ordinamenti giuridico comunitario.

Importante è il legame tra la concessione di un provvedimento inibitorio nei confronti di un prestatore informatico e i diritti fondamentali dei terzi.

Gli stessi titolari dei diritti devono poter avere la possibilità di richiedere un provvedimento inibitorio contro un intermediario che renda possibile le violazioni in rete da parte di un terzo, in base a quanto predisposto da ciascun ordinamento nazionale.

Specie nell'ambito del diritto d'autore, si è attribuito al provider il compito di adottare "misure sufficientemente efficaci" per garantire una tutela effettiva del diritto d'autore e quello di non privare "inutilmente gli utenti di Internet della possibilità di accedere in modo lecito alle informazioni disponibili"[336].

L'operatore tecnico della rete "dovrà trovare il modo – dal punto di vista tecnologico- di rendere difficilmente realizzabili le consultazioni non autorizzare dei materiali protetti, di scoraggiare seriamente gli utenti di Internet che ricorrono ai suoi servizi dal consultare tali materiali e di garantire il rispetto del diritto fondamentale alla libertà d'informazione"[337].

Per evitare arbitri da parte delle Autorità nazionali, occorre ricordare che già l'art. 15 della direttiva e l'art. 17 del decreto introducono una forte limitazione, affermando l'impossibilità

[335] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto,* cit., p. 189 ss.
[336] *Telekabel Wien c. Costantin Film,* cit.
[337] *Telekabel Wien c. Costantin Film,* cit.

di richiedere agli intermediari obbligazioni di sorveglianza sui dati immessi in rete che trasmettono o memorizzano e obbligazioni generali di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite[338].

Tali dettati legislativi prevedono altresì che gli Stati membri possono stabilire che i prestatori die servizi della società di informazione sono 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 sevizi con cui hanno accordi di memorizzazione dei dati.

L'ordinamento italiano, così come quello francese, si è ispirato alla fortunata esperienza inglese.

Le Corti del Regno Unito hanno indirizzato la tutela rimediale preventiva e specifica esperibile dal titolare delle opere dell'ingegno nei confronti dell'intermediario della rete verso l'adozione di *web-site blocking injunction*.

Il provider destinatario dell'ordine inibitorio è dunque, in questa esperienza giuridica, il fornitore di connessione alla rete, al quale è richiesto di disabilitare l'accesso ai siti web che ospitano senza alcuna autorizzazione esclusivamente o prevalentemente contenuti protetti da diritti di esclusiva.

La norma, "*Injunctions against service providers*", prevede che l'*High Court* possa emettere un ordine inibitorio nei confronti del prestatore intermedio, nel caso in cui questi abbia la conoscenza effettiva che un terzo si avvalga dei propri servizi per violare i diritto d'autore.

Tale forma di tutela ha assunto il carattere della generalità con riferimento alla esperibilità a vantaggio di qualsiasi diritto di proprietà intellettuale sulla base di principi di origine equitativa[339].

L'intermediario, una volta raggiunta la consapevolezza che i propri servizi siano adoperati per fini illeciti - su comunicazione del titolare dei diritti -, è obbligato ad adottare delle misure proporzionate per prevenire o per ostacolare il compimento di tali violazioni[340].

L'ordinamento italiano ammette, come si evince dal più recente ordinamento giurisprudenziale, l'esperibilità di misure inibitorie, come l'oscuramento dei siti web, anche

[338] M.L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, cit., pp. 119, 120 e 121.
[339] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. 213 ss.
[340] *Cartier International AG and others v. British Sky Broadcasting Ltd and others*, 2016, *EWCA Civ.* 658, par. 36.

avverso i fornitori di connessione alla rete (e cioè gli intermediari che prestano servizi di mero accesso alla rete).

Tuttavia, qualche profilo di contrato è emerso in ordine al contenuto del provvedimento inibitorio.

Secondo un orientamento, le misure inibitorie devono essere rigorosamente mirate alla chiusura di siti specifici ed individuati[341].

Questa linea è stata però contrastata da quella parte della giurisprudenza che invece ammissibili provvedimenti ingiuntivi configurati in modo tale da pretendere dall'intermediario "il blocco non solo di uno specifico sito web ma anche di tutti i siti speculari a prescindere dal nome di dominio indicato originariamente dal ricorrente e contenuto nell'ordine inibitorio"[342].

Come nelle *web-site blocking injunctions* inglesi, anche in questa ipotesi non è imposto al provider un generale obbligo di sorveglianza ma sarà il danneggiato ad essere onerato di inviare delle specifiche segnalazioni.

Anche il giudice francese, sulla scorta di quanto disposto dalla Corte europea di giustizia, ha disposto l'adozione di misure appropriate.

Le ragioni che giustificherebbero l'attribuzione a tali soggetti degli oneri di ottemperanza discendenti dall'ordine inibitorio sono da rinvenirsi, per le Corti francesi, nella necessità di tutela della vittima del fatto illecito e consistono, segnatamente, nella necessità di non rendere gravose le modalità di tutela previste a beneficio di chi sia già vittima di violazioni massive dei propri diritti[343].

Al di là di questa vicinanza del sistema italiano all'ordinamento inglese, i principi affermati in apertura sono stati ribaditi lo scorso marzo anche dalla Corte di cassazione.

Con la sua decisione 7708 del 19 marzo 2019, infatti, la Corte ha ritenuto legittimo l'ordine rivolto al gestore di una piattaforma di video sharing di "astenersi di pubblicare contenuti illeciti dello stesso tipo di quelli già riscontrati come violativi dell'altrui diritto".

La Cassazione n. 7708/2019 ammette l'inibitoria *pro-futuro* erroneamente negata dalla Corte d'Appello di Milano del 7 gennaio 2015 - ma concessa correttamente dal Tribunale di Milano 9 settembre 2011 relativamente a specifici programmi pubblicati in violazione del diritto d'autore - accogliendo il motivo di impugnazione relativo alla violazione e falsa

[341] Trib. Milano, 27 luglio 2016, in *De Jure.*
[342] Trib. Milano, 11 giugno 2018, e Trib. Milano, 12 aprile 2018, in *www.altalex.com.*
[343] R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto,* cit., p. 219.

applicazione degli artt. 41 Cost., artt. 78 ter, 79, 156 e 163 l. aut., artt. 4 e 5, d.lgs. 9 aprile 2003, n. 70, considerando 40, 45 e 48, dir. 2000/31/CE, art. 8 e considerando 9, dir. 2000/29/CE, artt. 9 e 11 e considerando 9, 23, 24 e 32 45 e 48, dir. 2004/48/CE, delle dir. 95/46/CE e 2002/ 58/CE, art. l, par. l, Cedu e artt. 11, 16, 17, par. 2 e 52, par. l, Carta dei diritti UE.

La decisione favorevole all'obbligo di filtraggio ex post pare corretta: non si tratta, infatti, di un obbligo generale ex ante vietato dalla dall'art. 17, d.lgs. n. 70/ 2003, quanto, invece, di un obbligo particolare - circostanziato - di prevenzione o rimozione di nuove violazioni, ormai prevedibili, relativamente allo stesso contenuto digitale illecito già in precedenza comunicato formalmente all'ISP: esigere tale condotta diligente dal prestatore di servizi al fine di prevenire la reiterazione della condotta illecita in relazione allo stesso contenuto digitale illecito in conformità alle norme che tutelano il diritto d'autore non pare in contrasto, a mente del generale principio di bilanciamento dei diritti contrapposti, con la tutela della libertà di impresa, come si desume anche dalla giurisprudenza conforme della Corte di giustizia UE[344].

Più in generale, è da qualche anno che le istituzioni europee e nazionali fanno riferimento alla possibilità di contrastare la diffusione di contenuti illeciti anche al di fuori di procedimenti di segnalazione e rimozione di singoli contenuti tramite processi di *notice and-take-down*.

A seguito degli attacchi terroristici che hanno colpito diverse città europee, ad esempio, nel giugno 2017 il Consiglio europeo ha incoraggiato i provider a sviluppare "nuove tecnologie e nuovi strumenti al fine di migliorare l'individuazione automatica e la rimozione dei contenuti" illeciti.

Un pensiero, questo, condiviso dal Parlamento e dalla Commissione Europea in diversi atti adottati nel contesto della complessa serie di riforme denominate "*Digital Single Market*" (DSM).

È il caso della Comunicazione della Commissione intitolata "Lotta ai Contenuti illeciti online" del settembre 2017 e della Raccomandazione della Commissione stessa "Sulle misure per contrastare efficacemente i contenuti illegali online" del marzo 2018, dove si ribadisce che "in aggiunta ai meccanismi di segnalazione e azione, anche l'adozione volontaria di misure proattive proporzionate e specifiche da parte dei prestatori di servizi di hosting, compreso il ricorso a strumenti automatizzati in taluni casi, può rappresentare un

[344] CGUE, 27 marzo 2014, C314/12, *Telekabel Wien c. Costantin Film,* cit., par. 35, 36, 37.

elemento essenziale nella lotta ai contenuti illegali online, fatto salvo l'articolo 15, paragrafo 1, della direttiva 2000/31/CE" - vale a dire, il divieto di imporre obblighi di monitoraggio preventivo e ricerca attiva[345].

In effetti le tecniche di tutela inibitoria hanno potenzialmente l'effetto di sovvertire il significato originario dell'esonero da responsabilità civile previsto dalla direttiva sul commercio elettronico.

In argomento è poi senz'altro il caso di menzionare il decreto cautelare del Tribunale di Milano del 24 dicembre 2019, emesso inaudita altera parte, con cui, al fine di impedire l'illecita riproduzione di una pellicola di prossima uscita nelle sale cinematografiche, è stata imposta ai principali fornitori di connettività del Paese una "*dynamic injunction*" consistente nell'obbligo di impedire immediatamente tanto l'accesso ai portali "pirata" elencati in ricorso, quanto l'accesso ai cc.dd. "alias" derivanti da modifiche al nome a dominio degli stessi, qualora rimandino ai medesimi contenuti illeciti ed "il collegamento soggettivo con i soggetti responsabili dell'attività illecita attualmente in essere sia obbiettivamente rilevabile".

L'elemento di assoluta novità del provvedimento citato è che esso è stato emesso sostanzialmente "in anticipo" rispetto all'effettivo verificarsi degli illeciti denunciati: nel caso in questione, infatti, la titolare dei diritti sulla pellicola aveva verificato come diversi siti di streaming illegale avessero iniziato, ben prima dell'uscita nelle sale, a pubblicizzare (con caricamento della locandina originale) la prossima disponibilità del film in questione sui medesimi portali.

Così, in considerazione del fatto che l'attività illecita di detti siti era già stata più volte accertata anche da AGCOM, e "tenuto conto che la violazione attuale dei diritti esclusivi sui materiali promozionali si pone in funzione strumentale rispetto alla verosimile imminente violazione dei diritti di distribuzione", il Tribunale ha ritenuto sussistente il *periculum in mora* sottolineando in particolare "la fondamentale importanza che riveste la prima visione nelle sale cinematografiche, in termini di accoglienza e riscontro da parte del pubblico e della critica, nel successivo ciclo di vitalità commerciale di un film", accogliendo quindi le istanze della ricorrente e concedendo la predetta inibitoria dinamica, "stante la necessità di intervento in tempi utili a evitare l'ulteriore protrarsi delle condotte illecite in concomitanza alla distribuzione del film nella sale cinematografiche di tutta Italia".

[345] ALBERTO BELLAN, *Piattaforme, obblighi di monitoraggio e risoluzione delle controversie online*, cit., p. 191 ss.

6. Il "Revenge Porn": i primi passi concreti del legislatore

Con la recente introduzione dell'art. 612-*ter* nel codice penale, il legislatore italiano ha inteso criminalizzare, in via specifica, il fenomeno conosciuto con il neologismo "*revenge porn*" (lett. "porno vendetta") e questo rappresenta – a parere di chi scrive- il primo vero rimedio legislativo previsto per le condotte illecite che si perpetrano in rete.

Tale formulazione è nata nel mondo angloamericano per indicare una condotta ben precisa: la divulgazione non consensuale, dettata da finalità divulgative, di immagini intime e a contenuto sessualmente esplicito raffiguranti l'ex partner.

Gli "ingredienti" essenziali per la configurazione del "*revenge porn* in senso stretto", dunque, sono:

- un contesto di coppia;
- il consenso alla produzione del materiale intimo e alla fruizione limitata alla coppia;
- la diffusione non consentita delle immagini dopo la fine del legame sentimentale;
- la finalità di vendicarsi da parte di chi pubblica le immagini.

Similmente a quanto avvenuto nei Paesi anglosassoni, però, anche nel linguaggio italiano l'espressione "*revenge porn*" ha assunto un significato più ampio, divenendo una sorta di "*catch all phrase*" utilizzata per indicare tutte le diverse forme di diffusione non consensuale di immagini aventi un contenuto sessuale.

Secondo questa accezione, pertanto, andrebbe ricondotta al "*revenge porn*" un'ampia casistica di condotte divulgatorie che non maturano nell'ambito di una relazione sentimentale o che sono prive della finalità vendicativa[346].

Tali condotte possono essere perpetrate anche da soggetti che non sono mai entrati in contatto con la persona offesa (a titolo esemplificativo si pensi: al c.d. "deep sex fakes", ovverosia la diffusione di immagini false o modificate tramite appositi software, o alla divulgazione di immagini ottenute mediante Trojan o Wireless Spy Cameras, nonché alla pubblicazione di immagini a seguito dell'"hackeraggio" di un dispositivo). Le motivazioni scatenanti l'abietto fenomeno possono essere le più disparate: per scherzo, per vanteria, per noia, per fini intimidatori o persino estorsivi.

Si è parlato di "*revenge porn*" ad esempio anche nel 2014, quando *hacker* mai individuati hanno manipolato gli account *iCloud* di numerose celebrità, perlopiù inglesi e americane, e la rete è stata invasa dalle loro immagini più intime.

[346] G. M. CALETTI, *Libertà e riservatezza sessuale all'epoca di Internet. L'art. 612-ter c.p. e l'incriminazione della pornografia non consensuale*, in *Rivista Italiana di Diritto e Procedura Penale*, 2019, p. 2044 ss.

In Italia è con l'art. 10 della legge 19 luglio 2019, n.69, che viene inserito l'art. 612-ter, il c.d. delitto di diffusione illecita di immagini o video sessualmente espliciti[347].

Tale dettato normativo è così formulato:

"Salvo che il fatto costituisca più grave reato, chiunque, dopo averli realizzati o sottratti, invia, consegna, cede, pubblica o diffonde immagini o video a contenuto sessualmente esplicito, destinati a rimanere privati, senza il consenso delle persone rappresentate, è punito con la reclusione da uno a sei anni e con la multa da euro cinquemila ad euro quindicimila.

La stessa pena si applica a chi, avendo ricevuto o comunque acquisito le immagini o i video di cui al primo comma, li invia, consegna, cede, pubblica o diffonde senza il consenso delle persone rappresentate al fine di recare loro nocumento.

La pena è aumentata se i fatti sono commessi dal coniuge, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva alla persona offesa ovvero se i fatti sono commessi attraverso strumenti informatici o telematici.

La pena è aumentata da un terzo alla metà se i fatti sono commessi in danno di persona in condizione di inferiorità fisica o psichica o in danno di una donna in stato di gravidanza.

Il delitto è punito a querela della persona offesa. Il termine per la proposizione della querela è di sei mesi. La remissione della querela può essere soltanto processuale. Si procede tuttavia d'ufficio nei casi di cui al quarto comma, nonché quando il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio".

Tale fattispecie presenta una disciplina complessa articolata in due differenti ipotesi, disciplinate rispettivamente al comma 1 e al comma 2, che prevedono il medesimo trattamento sanzionatorio per le condotte di invio, consegna, cessione, pubblicazione e diffusione di immagini o video dal contenuto sessualmente esplicito.

Il discrimine è costituito dalle modalità con le quali l'agente è entrato in possesso delle immagini che ha successivamente divulgato:

- nel caso del primo comma, è richiesto che egli abbia contribuito alla loro realizzazione o che le abbia «sottratte»,
- al secondo comma è disciplinato il caso in cui il diffusore le abbia «ricevute o acquisite in altro modo».

[347] Il 9 agosto del 2019 è entrata in vigore la legge n. 69 del 2019, recante "Modifiche al Codice penale, al codice di procedura penale e altre disposizioni in materia di tutela delle vittime di violenza domestica e di genere" (c.d. "Codice Rosso"). La novella legislativa è intervenuta sul versante sostanziale e procedurale, prevedendo quattro nuove fattispecie di reato, tra le quali figura la diffusione illecita di immagini o video sessualmente espliciti di cui all'art. 612-ter c.p.

L'elemento soggettivo richiesto in capo all'autore del reato è costituito dal dolo generico, nel caso del primo comma dell'art. 612-ter, mentre è richiesto il dolo specifico nelle ipotesi disciplinate dal secondo comma.

Attraverso l'introduzione di tale fattispecie penalmente rilevante si intende tutelare in primis la libertà di autodeterminazione della persona. Tuttavia, si tratta di una fattispecie plurioffensiva in quanto tutela altresì l'onore, il decoro, la reputazione, la dignità, la privacy nonché l'onore sessuale della singola persona e quindi attinente alla vita sessuale e alla reputazione di cui questa gode.

L'intervento legislativo italiano si colloca in una più ampia cornice di criminalizzazione a livello internazionale.

Il primo Paese ad aver preso l'iniziativa sono state le Filippine nel 2009. Più di recente, sono state introdotte nuove fattispecie incriminatrici "*ad hoc*" nelle giurisdizioni australiane del Victoria (2013), dell'Australia del Sud (2013) e del Nuovo Galles (2017), in Israele (2014), Canada (2014), Giappone (2014), in Inghilterra e Galles (2015), Spagna (2015), Nuova Zelanda (2015), Scozia (2016), Irlanda (2016), Germania (2017).

Il quadro è complesso ed in costante evoluzione negli Stati Uniti, dove, tra il 2013 ed il 2017, ben trentasei Stati (e il *District of Columbia*) si sono dotati di una norma penale di contrasto al "*revenge porn*", due stanno efficacemente applicando norme già esistenti da tempo (New Jersey e Alaska) e altri quattro hanno un disegno di legge pendente presso le rispettive assemblee legislative.

Se ad una prima impressione il reato di cui all'art.612-terc.p. sembra presentarsi come speciale rispetto all'art. 617-septiesc.p. soltanto in ragione dell'oggetto delle immagini o dei video (che devono, appunto, ritrarre organi sessuali o avere un contenuto sessualmente esplicito), dal confronto delle due fattispecie emergono ulteriori differenze.

In primo luogo, l'art.612-ter c.p. prevede un catalogo di condotte più ampio e specifico di quello dell'art.617-septies c.p., includendo ogni forma di consegna, cessione, divulgazione e diffusione effettuati dall'agente anche ad un solo individuo. Inoltre, a differenza del reato di cui all'art.617-septies c.p., il reato di "*revenge porn*" non richiede, quale elemento strutturale della realizzazione, la "fraudolenza" nella formazione del video o dell'immagine, essendo anche plausibile che si tratti di video o immagini formati col consenso della vittima: per l'incriminazione, in tal caso, è sufficiente l'assenza di consenso della persona rappresentata alla cessione o divulgazione di tali contenuti[348].

[348] Cass. pen., Sez. V, 17 dicembre 2020, n.3050, in *Ilpenalista.it*, 2021, p. 876 ss., con nota di F. BRIZZI, *Diffusione illecita di immagini o video sessualmente espliciti: tra tutela della privacy e revenge porn*.

Snodo centrale dell'applicazione dell'art. 612-*ter* c.p. sarà certamente rappresentato dall'individuazione di un significato quanto più possibile oggettivo all'espressione "immagini o video sessualmente espliciti".

Orbene, volendo traslare le considerazioni svolte in materia di pedopornografia minorile[349] alla fattispecie di cui all'art. 612-*ter* c.p., deve concludersi che l'elemento connotativo del concetto in esame è costituito dalla "sessualità" della raffigurazione - identificabile nella semplice rappresentazione dell'erotico piuttosto che nell'atto riproduttivo in sé - espressa nella sua valenza "esplicita", dovendo le immagini o i video attenere inequivocabilmente alla sfera sessuale.

In definitiva, non sembrano sorgere dubbi in merito al riconoscimento del carattere sessualmente esplicito di quei materiali che riproducono rapporti sessuali o di autoerotismo, organi genitali o zone erogene, nonché i toccamenti, gli strusciamenti o qualsiasi altro atto che "risolvendosi in un contatto corporeo, ancorché fugace ed estemporaneo, tra soggetto attivo e soggetto passivo ovvero in un coinvolgimento della corporeità sessuale di quest'ultimo", risulta espressivo della sessualità dell'offeso.

Un ambito tanto complesso e delicato come quello della pratica di diffusione illecita di immagini o video a sfondo sessuale costituisce certamente il terreno fertile per far sorgere serie perplessità e criticità in ordine alla normativa ad oggi esistente in tema di responsabilità degli Internet Service Provider (ISP).

I siti *web*, le piattaforme dedicate, i *social network* e i *forum* costituiscono lo spazio virtuale messo a disposizione dagli *ISP* per consentire agli internauti lo scambio reciproco del materiale incriminato.

Nonostante gli *ISP* avessero inizialmente la natura di "intermediari neutri" - in quanto deputati a consentire la diffusione passiva dei contenuti sul *web* - oggi essi hanno cambiato radicalmente volto assumendo un ruolo attivo che si sostanzia nell'intervenire concretamente sui contenuti pubblicati dagli utenti allo scopo di aumentarne la visibilità, incrementare le potenzialità di interazione e consentire maggiori possibilità di diffusione.

Di talché, risulta *prima facie* evidente come la lotta al fenomeno della pornografia non consensuale rischia di rimanere lettera morta se ad essa non si accompagna una strategia di contrasto che coinvolga i grandi portali, a loro volta responsabili della diffusione su larga scala delle immagini e dei video sessualmente espliciti e, dunque, della loro "viralità".

[349] V. MANES, *Metodo e limiti dell'interpretazione conforme alle fonti sovranazionali in materia penale*, in *Arch. pen.*, 2012, p. 36 ss.; G. COCCO, *Il concetto di pornografia minorile e i principi del diritto penale liberale*, nota a Cass., 22 marzo 2010, n. 10981, in *Resp. civ. prev.*, 2010, p. 2073 ss.

In un momento di intensa riflessione a livello dottrinale e giurisprudenziale sulla responsabilità degli *ISP*, ha assunto un rilievo fondamentale la già citata ordinanza del Tribunale di Napoli afferente ad un caso di "*Revenge porn*", che ha approfondito le caratteristiche della procedura cosiddetta di *notice and take down* (ossia di segnalazione da parte dei singoli al *provider* con conseguente obbligo di rimozione del materiale illecito).

In particolare, il provvedimento testé citato ha chiarito che l'obbligo di sorveglianza dell'*ISP* è conseguente a due ipotesi: in primo luogo, al mancato adempimento alla diffida di rimozione dei contenuti illeciti proveniente dalla parte che assume di essere stata lesa (così aderendo all'orientamento giurisprudenziale secondo cui la segnalazione del soggetto danneggiato vale come effettiva conoscenza) e, in secondo luogo, al mancato rispetto dell'ordine promanante dall'autorità cui il soggetto si è rivolto per ottenere l'eliminazione del materiale. In ogni caso, la mera segnalazione da parte del danneggiato all'*ISP* fa venir meno l'obbligo di attendere un ordine dell'autorità, "il quale potrebbe intervenire quando i diritti in questione sono irrimediabilmente pregiudicati e non più suscettibili di valutazione economica".

In ambedue le ipotesi, quindi, si perfezionerà il concorso dell'*ISP* nell'illecito già commesso dall'autore del contenuto.

Occorreva accogliere la richiesta giudiziale di Tiziana Cantone finalizzata a condannare l'*hosting provider Facebook* ad adempiere ad obblighi proattivi e social-preventivi volti ad impedire la reiterazione dell'illecito.

Che un bilanciamento tra così rilevanti diritti sia affidato ad un ente privato con fine lucrativo può sorprendere e preoccupare; tuttavia, tale scelta risulta inevitabile in ragione del ruolo svolto dagli *ISP*, gli unici effettivi gestori di un sistema che, oltre a consentire agli utenti l'accesso a Internet e la fruizione di contenuti, è al tempo stesso fonte di pericoli che solo i provider possono controllare[350].

A fronte dell'impossibilità degli internauti di proteggere adeguatamente i beni di cui sono titolari (dotati di particolare rilevanza e costantemente esposti a seri rischi sul *web*), è da attribuire ai *provider* la speciale posizione di garanti dell'integrità dei predetti beni e, dunque, l'obbligo giuridico di attivarsi per impedire il verificarsi dell'evento lesivo.

In altri termini, una responsabilità omissiva dell'*ISP* sarebbe legittimamente configurabile ai sensi dell'art. 40 cpv c.p. nel caso in cui lo stesso, pur avendo la possibilità tecnica e giuridica

[350] A. BACCIN, *Responsabilità penale dell'Internet Service Provider e concorso degli algoritmi negli illeciti online: il caso Force V. Facebook*, in *Sistema Penale*, 2020, p.75 ss.

di controllare preventivamente i dati immessi dagli utenti, non si sia attivato per scongiurare la lesione di beni meritevoli di una tutela rafforzata[351].

7. Profili conclusivi

È l'evoluzione stessa della rete informatica mondiale ad aver portato ad un superamento nei fatti della figura tradizionale del prestatore di servizi di hosting e il superamento del dato normativo di partenza ha condotto ad un più che condivisibile aggravio di responsabilità dell'intermediario della rete.

Il regime di responsabilità dei prestatori informatici per contenuti illeciti caricati da terzi che va emergendo pare essere tale per cui l'intermediario è responsabile per non aver progettato la propria piattaforma in maniera tale da prevenire che certi contenuti siano resi disponibili al pubblico, non avendo a monte incorporato nel disegno della piattaforma quelle misure che, grazia ad algoritmi sempre più sofisticati, rimuovono o prevengono l'immissione in rete di contenuti illeciti.

Risulta necessario, pertanto, che le piattaforme o meglio gli algoritmi che le disciplinano siano disegnato in maniera tale da rendere possibile che gli intermediari si rendano responsabili per le operazioni che compiono sui contenuti, secondo una modalità di "enforcement algoritmico equilibrato, in grado di contemperare tutti gli interessi in gioco, in particolare quelli degli utenti"[352].

Auspicabile sarebbe a tal proposito l'intervento del legislatore e l'eventuale imposizione che le decisioni automatizzate degli intermediari siano sottoponibili ad uno scrutinio per verificare ed assicurare che siano rispettati tutti i diritti che vengono in gioco, con il conseguente obbligo del prestatore di tenere in considerazione tutti gli interessi dei soggetti coinvolti.

Se la sempre maggiore diffusione delle Intelligenze Artificiali nelle sue diverse soluzioni tecnologiche porterà, nell'ottica della Commissione europea stessa, incredibili benefici – si pensi alla diminuzione di incidenti stradali mortali, un migliore uso delle risorse naturali, dell'energia e dell'acqua et similia – allo stesso modo il progresso tecnologico potrà portare – e forse già ha portato – alla creazione di individuazione e rimozione di contenuti illeciti e di filtraggio automatico sempre più in grado di realizzare un "enforcement equilibrato".

---

[351] C. ZANNELLI, *"Revenge Porn". Pregi e aporie della nuova fattispecie di cui all'art. 612-ter c.p.*, in *Diritto di Famiglia e delle Persone*, 2021, p. 1427 ss.

[352] M.L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, cit., pp. 226 e 227.
N. HELBERGER-J. PIERSON-T. POELL, *Governing online platforms: From contested to cooperative responsability*, in *34 The Information Society*, 2018, p. 1 ss.

Si può ipotizzare che algoritmi di apprendimento automatico, sfruttando le informazioni che si accumulano nel tempo, possano imparare ad affinare le decisioni circa la lesività di un contenuto, tenendo conto del contesto all'interno del quale quel contenuto è inserito e quindi della eventuale sussistenza di interessi ulteriori[353].

D'altra parte, è la stessa direttiva sul commercio elettronico che contiene all'art. 21 i presupposti per il suo aggiornamento affinché possa essere adeguata all'evoluzione giuridica, tecnica ed economica dei servizi della società.

Se si sfogliano le pagine della comunicazione della Commissione europea del 28 settembre 2017, si può leggere che le piattaforme digitali hanno "la pesante responsabilità, nei confronti della società, di proteggere gli utenti e il pubblico in generale nonché di prevenire lo sfruttamento dei loro servizi da parte di criminali e altri soggetti coinvolti in attività illegali on line"[354].

È difatti previsto dall'organo proposto all'iniziativa legislativa dell'Unione europea che il compito dell'intermediario non si limita a reagire alle segnalazioni parte ricevute ma si sostanziano anche nell'adottare "misure proattive efficaci"[355].

Quindi anche la stessa direttiva che ha garantito il beneficio di esonero è comunque aperta alla possibilità di una responsabilizzazione al mutare del contesto tecnologico, arrivando addirittura a far presente il problema della prevedibilità.

È infatti indubbio che vi sono alcuni illeciti, specie quelli lesivi dell'altrui reputazione e dignità, che una volta perpetrati non possono essere in alcun modo recuperati.

A titolo esemplificativo, tra i molti potenziali casi verificabili, nell'ipotesi in cui siano illecitamente sottratte foto intime e postate sulla rete, la perpetrazione e la diffusione rapida creerebbero un pregiudizio irreparabile nel momento stesso del click di mouse con il quale si immette il materiale in rete.

In tali ipotesi la rimozione ex post non risarcirebbe di certo la vittima del danno subito.

Pertanto, alla luce dei progressi tecnologici, dei meccanismi di filtraggio e della specializzazione degli algoritmi si potrebbe immaginare un meccanismo di controllo preventivo, unico controllo in grado realmente di tutelare i diritti degli utenti.

Senza dubbio occorrerebbe ripensare ad un'inversione dell'onere della prova che vada a vantaggio dell'utente, proprio all'esito della vigenza di meccanismi sempre più sofisticati

---

[353] E. KOREN, *Fair Use by Design*, in *64 UCLA Law Review*, 2017, p. 1082 ss.; M.L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, cit., p. 230.

[354] COM (2017) 555, 28 settembre 2017, *final*, 3 ss.

[355] COM (2017) 555, cit., 11. Cfr., R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., p. 227.

degli algoritmi e alla luce del progresso tecnologico di cui i provider, soggetti professionalmente qualificati, sono gli stessi artefici e i conoscitori più consapevoli.

CAPITOLO QUARTO

Diritto all'oblio e rievocazione storica nell'era digitale

SOMMARIO: 1. Il diritto all'oblio e l'avvento dell'era digitale. - 2. La protezione dei dati personali alla luce del nuovo regolamento europeo. - 3. Il diritto all'oblio nella giurisprudenza comunitaria - 4. Il diritto all'oblio, il diritto di cronaca e la rievocazione storica nella giurisprudenza italiana

1. Il diritto all'oblio e l'avvento dell'era digitale

Il diritto all'oblio corrisponde alla pretesa di un individuo di essere dimenticato o, meglio, di non essere più ricordato per fatti che in passato furono oggetto di cronaca.

Esso di radica sul rilievo per cui l'interesse pubblico alla conoscenza di un fatto è racchiuso nello spazio temporale necessario a informarne la collettività, mentre con il trascorrere del tempo il fatto esce dal pubblico dominio per acquisire l'originaria natura di fatto privato.

Si tratta di una creazione dottrinale e giurisprudenziale che oscilla tra il rispetto della dignità e dell'identità della persona e il diritto alla riservatezza[356].

È possibile ritenere che il diritto all'oblio abbia il corpus del diritto all'identità personale e l'animus del diritto alla riservatezza.

Tale diritto, dunque, si sostanzia nella pretesa di un individuo di tornare padrone della propria storia personale e di recuperare il controllo anche dopo che è stata oggetto di divulgazione, eliminando ciò che appartiene alla propria identità personale.

Agisce quindi su quello che è stato il passato di un soggetto per tutelare il suo futuro.

---

[356] Come noto, pur in difetto di una chiara affermazione legislativa, la giurisprudenza italiana ha da tempo affermato che il nostro ordinamento riconosce il diritto soggettivo all'oblio.
Cfr. in particolare *ex multis*, Cass. civ., 9 aprile 1998, n. 3679, in *Foro it.*, 1998, c. 1834 ss., con nota di P. LAGHEZZA; Cass. civ., 18 ottobre 1984, n. 5259, in *Giur. it.*, 1985, c. 762 ss.; Trib. Roma, 15 maggio 1995, in *Dir. inf.*, 1996, p. 427 ss. e Trib. Roma, 27 novembre 1996, in *Dir. aut.*, 1997, p. 372 ss.
Anche Cass. pen., Sez. V, 24 novembre 2009, n. 45051, in *Studium Iuris*, 2010, p. 577 ss. e in *Resp. civ. prev.*, 2010, p. 1067 ss.

Con l'affermazione del diritto all'oblio si riconosce ad ogni consociato il potere di ottenere che, salvo eccezioni, accadimenti relativi alla sua vita passata, non più di interesse pubblico, fossero dimenticati, e cioè non fossero riproposti, a distanza di tempo, dai mass media all'attenzione generale dei fruitori dei giornali a stampa, così come dei programmi televisivi o radiofonici.

Fermo restando che, nel caso di notizie false, o in altro modo diffamanti o comunque lesive, non si pone propriamente un problema di oblio, quanto di tutela degli altri diritti della personalità, quali per l'appunto il diritto all'identità personale o alla reputazione o all'onore.

È oramai pacifico il riconoscimento del diritto a che una notizia, benché vera e confezionata in modo appropriato, ma lesiva per l'immagine del soggetto o per altri suoi interessi protetti, non sia resa oggetto di attenzione da parte dei mass media e dunque non sia riproposta all'opinione pubblica, dopo un certo lasso di tempo dalla sua prima diffusione o dall'accadimento del fatto a cui la notizia si riferisce[357].

Ciò sempre che non sussista o possa sussistere ancora nella comunità un interesse diffuso ed attuale per la notizia in questione, giacché in tal caso il diritto all'informazione, inteso nella sua complessità e dunque come diritto ad informare e ad essere informarti, prevarrebbe sul diritto individuale all'oblio.

Ciò che viene in rilievo è il bilanciamento d'interessi tra il diritto alla cronaca, il diritto di critica, il diritto alla riservatezza, la tutela della dignità umana e dell'informazione.

È compito importante dell'interprete non solo definire cosa sia il diritto all'oblio ma anche porsi come arbitro dei diritti e verificare in che modo possano essere bilanciati.

---

[357] Nella letteratura italiana, sul diritto all'oblio, tra gli altri, v. F. DI CIOMMO-R. PARDOLESI, *Dal diritto all'oblio in Internet alla tutela della identità dinamica. È la rete, bellezza!*, in *Danno e resp.*, 2012, p. 701 ss.; E. GABRIELLI (a cura di), *Il diritto all'oblio. Atti del convegno di studi del 17 maggio 1997*, Napoli, 1999, p. 1 ss.; G.B. FERRI, *Diritto all'informazione e diritto all'oblio*, in *Riv. dir. civ*., 1990, p. 801 ss.; T. AULETTA, *Diritto alla riservatezza e "droit à l'oubli"*, in G. ALPA-M. BESSONE-L. BONESCHI-G. CAIAZZA (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983, p. 127 ss.; G. FINOCCHIARO, *L'identità personale su Internet*, in *Danno e resp.*, 2012, p. 388 ss.; G.E. VIGEVANI, *Identità, oblio, informazione e memoria in viaggio da Strasburgo a Lussemburgo, passando per Milano*, in *Danno e resp.*, 2014, p. 731 ss.; G. MARCHETTI, *Diritto di cronaca on-line e tutela del diritto all'oblio*, in AA.VV., in *Da Internet ai social network, Sant'Arcangelo di Romagna*, 2013, p. 71 ss.; F. PIZZETTI, *Il caso del diritto all'oblio*, Torino, 2013; L. DE GRAZIA, *La libertà di stampa e il diritto all'oblio nei casi di diffusione di articoli attraverso Internet: argomenti comparativi*, in *Riv. dell'Assoc. Italiana dei cost.*, 2013, p. 4 ss.; G. CITARELLA, *Aggiornamento degli archivi online, tra diritto all'oblio e rettifica "atipica"*, in *Resp. civ. e prev*., 2012, p. 1155 ss.; L. FEROLA, *Dal diritto all'oblio al diritto alla memoria sul Web. L'esperienza applicativa italiana*, in *Dir. inf.*, 2012, p. 1001 ss.; F. MANGANO, *Diritto all'oblio*, in *Giur. merito*, 2012, p. 2621 ss.; M. MEZZANOTTE, *Il diritto all'oblio. Contributo allo studio della privacy storica*, Napoli, 2009; S. NIGER, *Il diritto all'oblio*, in G. FINOCCHIARO (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale*, Padova, 2007, p. 59 ss.; P. LAGHEZZA, *Il diritto all'oblio esiste (e si vede)*, in *Foro it.*, 1998, c. 1835 ss.; S. MORELLI, *Fondamento costituzionale e tecniche di tutela dei diritti della personalità di nuova emersione (a proposito del cd "diritto all'oblio")*, in *Giust. civ*., 1997 p. 515 ss.

Il diritto all'oblio è infatti un prodotto della società dell'informazione: l'immagine di un consociato è oggi il risultato di come egli appare agli altri attraverso il filtro dei mass media[358].

Le prime riflessioni sul diritto all'oblio risalgono agli anni '60 del Novecento e scaturiscono dalle considerazioni espresse da Samuel D. Warren e Louis D. Brandeis, che lo intesero come *ius excludendi alios*.

In origine, invero, il diritto all'oblio si presentava quale articolazione del diritto al rispetto della vita privata, nell'accezione di "*right to be forgotten*"[359].

L'imporsi del diritto all'oblio nella riflessione di interpreti e giudicanti non può dirsi, anche spaziando fuori dai confini nazionali, approdo recente della scienza giuridica.

Già in tempi ove decisamente meno forsennata era la produzione e il consumo di informazioni, l'argomento del rispetto della vita privata declinò in tale direzione.

Il riferimento è al noto caso Caruso del 1958: è a tale sentenza che viene fatta risalire la genesi della figura, pur difettando l'espresso sintagma "diritto all'oblio". Nell'occasione si parlò infatti di "diritto al segreto del disonore"[360].

Tuttavia, non può non farsi cenno alla sentenza dei giudici francesi del 1963, trovatasi a decidere sul ricorso di una delle amanti del serial killer Henri Landru.

La donna agì contro il produttore cinematografico e il registra del film, Landru, ove lamentava si mostrasse uno dei periodi più drammatici della sua vita privata e di cui ambiva a rimuovere le tracce.

La richiesta, pur rigettata, fornì alla dottrina tracce sufficienti a maturare una definizione del fenomeno, coniandosi in proposito proprio la formula *droit à l'oubli*, per riferire del diritto a che notizie di pubblico dominio non fossero ulteriormente diffuse una volta celate dal tempo[361].

In Italia numerosi sono stati i tentativi qualificatori.

Un'autorevole dottrina definisce il diritto all'oblio come "il diritto a che i fatti, pure pubblici, attinenti ad un soggetto, con il decorso del tempo cessino di avere tale qualità"[362].

---

[358] F. DI CIOMMO, *Quello che il diritto non dice. Internet e oblio*, in *Danno e resp.*, 2014, p. 1101 ss.

[359] F. DI CIOMMO, *Privacy in Europe After Regulation (EU) No 2016/679: What Will Remain of the Right to Be Forgotten?*, in *The Italian Law Journal*, 2017, p. 24 ss.
Per una riflessione sulla portata innovativa del GDPR in materia di oblio e deindicizzazione, si rinvia a S. ZANINI, *Il diritto all'oblio nel Regolamento europeo 679/2016: quid novi?*, in *federalismi.it*, 2018, p. 9 ss.

[360] Cass. civ., 13 maggio 1958, n. 1563, in *Foro it.*, 1958, c. 1116 ss.

[361] G. LYON CAEN, nota a Trib. gr. inst. Seine, 4 ottobre 1965, n. 14482, in *Semaine Juridique*, 1966, p. 284 ss.

[362] V. ZENO ZENCOVICH, *Una svolta giurisprudenziale nella tutela della riservatezza*, in *Dir. inf.*, 1986, p. 934 ss.

A propiziare un'organica meditazione del fenomeno sono le pagine di Giovanni Battista Ferri, il quale coglie l'appartenenza di tale diritto "alle ragioni e alle regioni del diritto alla riservatezza"[363].

Di qui dottrina e giurisprudenza si iniziano a confrontare con il problema di tutelare un tale interesse della persona, ipotizzandone un'autonoma considerazione giuridica in seno al sistema e ricercandone un'armonica sintesi con diritti *prima facie* confliggenti, quali, *in primis*, quello di informazione.

Si tratta cioè di trarre i rapporti di forza tra memoria collettiva e oblio entro una dinamica bilanciata, capace di assicurarne la concorrenza secondo i criteri dell'utilità sociale e, insieme, dell'ossequio all'identità dei consociati[364].

Il crescente imporsi del diritto all'oblio nell'orizzonte dei valori ha sempre più sensibilizzato a un suo congruo dimensionamento, fuori dal quale l'esercizio del diritto di cronaca rischia di danneggiare il percorso di vita di un consociato.

La rinnovata narrazione di fatti che investono un determinato soggetto quando oramai il tempo trascorso li ha gettati nel dimenticatoio, allontanandoli da una percezione viva e diffusa, insinua dunque progressivamente la premura ad una più ponderata valutazione delle conseguenze.

Verosimilmente, più ampio è l'intervallo tra originaria divulgazione di un evento e sua riproposizione, più lo scenario in cui s'insinuano le rievocazioni rischia d'essere mutato a tal punto da imporre una contestualizzazione ed attualizzazione oculata dell'informazione.

Senza di essa il fragore della pubblicità può tornare a danneggiare l'esistenza ed il percorso di vita di chi già ne abbia patito.

È in questo ambito che l'interessato potrà reclamare il diritto a una comunicazione in tal senso accorta, la quale, pur nello spazio dettato dall'utilità sociale della notizia, non indulga in perniciose quanto non necessarie specificazioni[365].

Con l'avvento di Internet la problematica si è imposta con un'attenzione molto più incisiva all'attenzione degli interpreti e degli operatori di diritto.

---

[363] G.B. FERRI, *Diritto all'informazione e diritto all'oblio*, in *Riv. dir. civ*., 1990, p. 801 ss.

[364] Il rapporto tra diritto di cronaca e diritti della persona risulta variamente indagato.
Cfr., *ex multis*, V. ROPPO, *Libertà di manifestazione del pensiero*, in *Enc. dir.*, Milano, 1974; P. PERLINGIERI, *Informazione, libertà di stampa e dignità della persona*, in *Rass. dir. civ*., 1986, p. 624 ss.; A. PACE-F. PETRANGELI, *Diritto di cronaca e di critica, in Enc. dir. (Agg. V)*, 2002; V. ZENO ZENCOVICH, *La libertà d'espressione: media, mercato, potere nella società dell'informazione*, Bologna, 2004.

[365] In dottrina, tra gli altri, v. AA.VV., *Il diritto all'oblio. Atti del Convegno di Studi del 17 maggio 1997*, cit., p. 3 ss.; T. AULETTA, *Diritto alla riservatezza e "droit à l'oubli*", cit., p. 127 ss.; M.R. MORELLI, *voce Oblio (diritto all')*, in *Enc. dir. Agg*., Milano, 2002, p. 851 ss.; M. MEZZANOTTE, *Il diritto all'oblio - contributo allo studio della privacy storica*, cit., *passim.*

Con l'avvento dell'era digitale è inevitabile che cibernauti e non siano immersi in un flusso di informazioni continue.

Si è modificato sostanzialmente e radicalmente il mondo dell'informazione ed il rapporto tra informazione, fatti e persone, in quanto:

1) oggi non è più realmente possibile distinguere chi fa informazione e chi fruisce di informazioni, giacché in rete chiunque può immettere, e normalmente immette, informazioni, anche di carattere personale, riguardanti sé o terzi;

2) mentre sino a ieri i consociati si informavano quotidianamente attraverso la lettura dei giornali a stampa o l'ascolto dei giornali televisivi e radiofonici, oggi la maggior parte della gente si informa realmente in tempo reale attraverso la semplice presenza on-line, la quale, di per sé sola, assicura la ricezione continua di informazioni di qualsiasi tipo e specie, attraverso i social network a cui si partecipa o, comunque, attraverso stringhe informative assicurate su molteplici siti;

3) oggi è semplicissimo per qualsiasi utente cercare, in vario modo, in rete informazioni, attuali o no, su qualsiasi circostanza, persona o curiosità, sicché le fonti informative dell'epoca pre-telematica sono sostanzialmente superate, salvo resistere come strumenti di approfondimento, soprattutto se specialistico;

4) mentre in passato l'informazione seguiva flussi standard e, dunque, veniva per lo più fornita al pubblico, tramite i mass media, da operatori qualificati, i quali sceglievano se, come e quando far conoscere, o quando riproporre, una certa notizia alla c.d. opinione pubblica, ai tempi di Internet le informazioni sono sempre sulla grande rete a disposizione di tutti (salvo le limitazioni proprietarie che riguardano alcune banche dati specialistiche), con la conseguenza che ogni utente può in qualsiasi momento entrare in contatto con una data notizia anche datata;

5) Internet non sconta distanze geografiche, confini territoriali o nazionali, barriere fisiche e quant'altro sicché ogni singolo utente può accedere con la stessa facilità, salvo gli ovvi eventuali problemi di lingua, ad informazioni pubblicate in Internet da chiunque, in qualsiasi modo ed in ogni parte del mondo.

Corollario di tali premesse è che oggi Internet costituisce un'immensa banca dati; anzi una immensa banca di banche dati, continuamente arricchite da milioni di informazioni immesse in rete ogni secondo, a carattere globale, senza soluzione di continuità, da chiunque voglia farlo.

Si tratta di informazioni di ogni genere e contenuto: da quelle pubblicate da giornalisti professionisti su siti che svolgono espressamente attività informativa, a quelle istituzionali

(ad esempio di Ministeri e Università), a quelle commerciali (diffuse principalmente sui siti Internet delle aziende), fino a quelle, e sono la stragrande maggioranza, postate da semplici utenti sui siti più disparati e soprattutto, oggi, tramite i social-network, nei quali i cyberutilizzatori inseriscono (normalmente senza porsi alcun problema di privacy) notizie, fotografie, comunicazioni e quant'altro, che riguardano loro o altri.

In questo *mare magnum* di informazioni, un documento, o più in generale un dato, una volta caricato in Internet e reso disponibile ai naviganti, esce, infatti, dalla sfera di esclusiva disponibilità dell'autore ovvero di colui che lo ha riversato on-line o, comunque, del sito sorgente, e cioè del primo sito nel quale il dato è apparso, in quanto può essere copiato e, dunque, memorizzato da altri siti e può essere raggiunto e rintracciato tramite i c.d. motori di ricerca, sostanzialmente da qualsiasi altro utente abilitato.

Questo significa che un qualsiasi contenuto, una volta pubblicato in rete, entra sostanzialmente nella più o meno libera utilizzabilità di qualunque altro utente, il quale - fatta salva la tenuta dei congegni tecnici utilizzati per proteggere in particolare le opere oggetto di diritto d'autore o i servizi a pagamento - potrà non solo fruirne, ma copiarlo e, a sua volta, riversarlo in un altro angolo della grande rete, senza che confini territoriali o nazionali possano influenzare la realizzabilità di tale (spesso semplice) operazione.

In definitiva, Internet è non solo una immensa, sconfinata banca dati di informazioni, ma anche un luogo in cui qualsiasi dato, una volta immesso, viene riprodotto tante più volte quanto più interesse, per varie ragioni, suscita tra gli utenti; sicché tale dato alla fine risulterà presente in Rete in diversi siti e in diverse forme contemporaneamente[366].

In questo contesto una posizione del tutto peculiare, e delicatissima, rivestono i motori di ricerca, i quali consentono all'utente di orientarsi nel *mare magnum* della grande rete ed accedere, peraltro in modo estremamente rapido, alle informazioni che cerca.

Più nel dettaglio, può dirsi che attraverso l'utilizzazione del motore prescelto, e dunque in ragione delle parole che utilizza per svolgere la ricerca, l'utente raggiunge la data informazione in quanto questa gli viene indicata, normalmente insieme ad altre, in risposta dal motore di ricerca, il quale a sua volta la recupera, nel mare di informazioni che costituiscono Internet, da un sito sorgente su cui la notizia è già pubblicata, oppure, nel caso in cui la risorsa originale sia irraggiungibile, dalla propria "memoria cache".

In questo modo, essi finiscono per svolgere una vera e propria attività di memorizzazione di tutti i contenuti della rete.

---

[366] F. DI CIOMMO, *Quello che il diritto non dice. Internet e oblio*, cit., p. 1107 ss.

Sulla base di quanto sin qui accennato, bisogna, dunque, ammettere che, nell'epoca in cui Internet costituisce il principale strumento informativo ed insieme il luogo che tutti frequentano quotidianamente, la diffusione di notizie anche molto datate, pur in assenza di interesse pubblico, rappresenta un fenomeno costante e questo non può che suscitare riflessioni in riferimento alla tutela e al riconoscimento del diritto all'oblio.

Sono tre le declinazioni del diritto all'oblio che vengono in rilievo:

- la pretesa di impedire che la notizia venga ripubblicata dopo il decorso di un significativo lasso temporale
- la pretesa alla corretta ed aggiornata contestualizzazione della notizia
- la pretesa alla deindicizzazione dei dati visibili nell'elenco dei risultati di ricerca disponibili online, connessa dunque alla reperibilità delle notizie in rete.

2. La protezione dei dati personali alla luce del nuovo regolamento europeo

L'unica norma che fa espresso rinvio al diritto all'oblio è l'art. 17 del Regolamento UE 2016/679.

Questo testo di legge del Parlamento europeo e del Consiglio è stato emanato il 27 aprile 2016 e pubblicato nella Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016[367].

Il provvedimento abroga e sostituisce la direttiva 95/46/CE, recante il "Regolamento generale sulla protezione dei dati" che per anni ha rappresentato la pietra angolare della normativa dell'Unione Europea in materia di protezione di dati personali.

Proprio l'utilizzo di un regolamento, in luogo della direttiva, è significativo del mutamento di approccio da parte del legislatore europeo, il quale ha avvertito la necessità di sostituire l'obiettivo originario dell'armonizzazione con quello assai più pervasivo e ambizioso dell'uniformazione, sebbene non manchino incisivi rinvii ai legislatori nazionali, i quali, stando al considerando n. 10, dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione del presente regolamento , anche al fine di determinare con maggiore precisione le condizioni alle quali il trattamento dei dati personali è lecito[368].

[367] M.G. STANZIONE, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Europa e Diritto Privato*, 2016, p. 1259 ss.

[368] Così G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.*, 2017, p. 6 ss.

Cfr., sul punto, F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm.*, 2017, p. 372 ss.

Il nuovo regolamento si articola in 11 capi per un totale di 99 articoli e la parte dispositiva è preceduta da ben 177 considerando che contribuiscono a chiarire il contesto e le ragioni della nuova normativa[369].

L'esigenza di una riforma della materia è sorta anche e forse soprattutto per la continua evoluzione degli stessi concetti di privacy e di *data protection*, dovuta principalmente all'incessante progresso dei servizi online.

La precedente direttiva 95/46/CE era stata adottata nel 1995 con due principali obiettivi:

1) salvaguardare il diritto fondamentale dei soggetti alla protezione dei dati;
2) garantire la libera circolazione dei dati personali tra gli Stati membri.

Le tecnologie attuali consentono agli operatori economici di impiegare moli imponenti di dati personali come mai in precedenza era stato fatto e con finalità che qualche decennio fa non erano neppure immaginabili.

È divenuto dunque più necessario instaurare un quadro giuridico più solido e coerente, adeguato allo sviluppo dell'economia digitale nel mercato interno, e la normativa del 1995 ha mostrato in questo tutta la sua inadeguatezza.

Il regolamento del 2016, generale in materia do protezione dei dati personali, si presenta come una cornice normativa unitaria, una sorta di *Magna Charta* della circolazione dei dati personali e della protezione della persona, che funge, per un verso, da fondamento della disciplina europea e, per altro verso, da quadro di riferimento e di contenimento del particolarismo giuridico in materia[370].

Ciò che maggiormente colpisce è che ci si trova difronte ad un atto normativo di unificazione e che lascia ampio margine di regolazione autonoma agli Stati membri.

In particolare, ai sensi dell'art. 6 spetta ai diritti nazionali individuare:

- le ipotesi di trattamenti fondati sulla necessità di adempiere ad un obbligo legale al quale è assoggettato il titolare;
- le ipotesi di trattamenti necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;
- rispetto al trattamento delle categorie particolari di dati personali, c.d. dati sensibili, è riservata ai singoli Stati la scelta se rendere sufficiente a tal fine il consenso esplicito dell'interessato, con riferimento a finalità specifiche, l'autorizzazione al

[369] A. IULIANI, *Note minime in tema di trattamento dei dati personali*, in *Europa e Diritto Privato*, 2018, p. 293 ss.; R. GIOVAGNOLI, *Il nuovo regolamento europeo sulla protezione dei dati personali*, in ID., *Manuale di Diritto civile*, p. 55 ss.

[370] F. PIRAINO, *Sulla nozione di bene giuridico in diritto privato*, in *Riv. crit. dir. priv.*, 2013, p. 459 ss.

trattamento di tali dati per l'assolvimento di obblighi e per l'esercizio di diritto del titolare o dell'interessato in materia di diritto del lavoro della sicurezza e protezione sociale e l'individuazione dei motivi di interesse pubblico che giustificano il trattamento di tali categorie particolari in assenza di consenso.

Si assiste dunque ad un ridimensionamento della dimensione personalistica, formalizzata nel diritto alla privacy, sul presupposto che l'esposizione dell'individuo all'attenzione della società è un percorso inarrestabile.

Rispetto alla Direttiva 95/46, il Regolamento si concentra in maniera accentuata sulla disciplina della circolazione dei dati personali, piuttosto che sul riconoscimento giuridico della centralità della persona e sulla conseguente predisposizione di strumenti di realizzazione della personalità umana e di salvaguardia contro le interferenze esterne.

Il regolamento muove dalla premessa secondo cui nell'attuale contesto digitale è del tutto complicato e a tratti illusorio l'obiettivo di impedire l'acquisizione e l'impiego di dati personali da parte di soggetti terzi.

Il progresso tecnologico ha reso facilmente intelligibili le informazioni personali[371].

La situazione giuridica riconosciuta al titolare dei dati si identifica più che nel diritto alla riservatezza, nel diritto di mantenere il controllo sulle informazioni che lo riguardano, sul presupposto che il trattamento e la circolazione dei dati sono essenziali per lo svolgimento di qualsivoglia attività.

L'essenza normativa del Regolamento risiede nel predisporre una disciplina dell'attività consistente nel trattamento di dati personali, la quale presuppone ed incoraggia l'attitudine alla circolazione esibita dai dati personali.

Dunque, mentre l'impianto della direttiva 95/46 era basato su una concezione sostanzialmente statica del trattamento dei dati personali e, soprattutto, per lo più binaria (in cui le informazioni procedono prevalentemente dall'interessato al titolare), il Regolamento 2016/679 ha una struttura più dinamica ed include anche la comunicazione dei dati a soggetti terzi dal titolare e dall'interessato (i c.d. destinatari) mediante la trasmissione, diffusione o qualsiasi forma di messa a disposizione[372].

[371] F. PIRAINO, *Sulla nozione di bene giuridico in diritto privato*, cit., p. 467 ss. e F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, cit., p. 393 ss.

[372] D. BARBIERATO, *Osservazioni sul diritto all'oblio e la (mancata) novità del Regolamento Ue 2016/679 sulla protezione dei dati personali*, in *Resp. civ. prev.*, 2017, p. 2100 ss.

In una società dominata dall'interconnessione e dalla condivisione, sollecitata da social network, motori di ricerca e smartphone, le informazioni personali si presentano sin dall'origine destinate alla circolazione globale.

Il diverso bilanciamento degli interessi, che opera in favore della circolazione, come emerge dalla finalità dichiarata di favorire un clima di fiducia per lo sviluppo dell'economia digitale in tutto il mercato interno, è radicato in diversi punti della normativa e anzi, da questo punto di vista acquista un significato ben determinato l'affermazione contenuta nel considerando n. 4 secondo cui il diritto alla protezione dei dati personali non è un diritto assoluto e deve essere considerato alla luce della sua funzione sociale[373].

Ai fini del superamento del divieto generale di trattamenti delle categorie particolari di dati è sufficiente il consenso dell'interessato: si garantisce così a quest'ultimo un ampio potere di controllo e di gestione dei dati trattati senza che sia in alcun modo gravato lo scambio dei dati in ambiente informatico[374].

L'art. 6 del Regolamento ancora la liceità dei trattamento a due requisiti alterativi: la necessità del trattamento e il consenso dell'interessato[375].

---

[373] G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati*, cit., p. 8 ss.; F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, cit., p. 389 ss.; A. THIENE, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo Regolamento europeo*, in *Nuove leggi civ. comm.*, 2015, p. 412 ss.

[374] Tra questi, oltre all'ipotesi in cui il trattamento sia necessario per la prestazione del servizio, particolare discussione ha sollevato la previsione dell'art. 24 lett. d) a norma della quale non è richiesto il consenso per il trattamento dei "dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segretezza aziendale ed industriale", al punto che la dottrina più accorta ne ha parlato come una norma contenente una interpretazione duplex.

L'ambivalenza riguarda l'interpretazione del significato di attività economica, il quale può infatti riferirsi sia al soggetto che tratta i dati personali, così da fare rientrare nell'esclusione tutte quelle informazioni personali acquisite nell'ambito di un attività, ad esempio, di marketing, sia, invece, all'interessato, o meglio alla sua attività, così da escludere dalla prestazione del consenso tutte quelle informazioni concernenti, ad esempio, la ragione sociale, il numero di partita Iva.

A militare verso questa seconda interpretazione, oltre all'esigenza avvertita dagli interpreti di non svuotare di senso il ruolo del consenso, starebbe l'inciso contenuto nella norma circa la necessità di rispettare la normativa in tema di segreto aziendale ed industriale, da intendersi chiaramente come riferito all'attività di chi divulga l'informazione non certo di quella di chi l'informazione la raccoglie e la tratta.

Dello stesso tenore, al punto da porre un problema di coordinamento con la disposizione appena richiamata, è la previsione dell'art. 24 lett. g) che esclude la necessità del consenso, ma solamente quanto alla raccolta, nei casi - individuati dal Garante - in cui il trattamento è necessario "per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, anche con riferimento all'attività di gruppi bancari e di società controllate o collegate".

La disposizione, sebbene paia fare riferimento, laddove esemplificando allude all'attività dei gruppi bancari, all'interesse a conoscere informazioni patrimoniali dell'interessato ai fini dell'erogazione di un servizio, quale potrebbe essere, ad esempio l'erogazione di un mutuo, sembra piuttosto riferirsi a quell'attività di sorveglianza e di vigilanza che necessariamente implica il trattamento di dati personali e ciò dal momento che l'interesse a conoscere la situazione patrimoniale dell'interessato rientra nella fattispecie di esclusione di cui alla lett. b) al punto da trovare puntuale riscontro nella disciplina in materia bancaria.

[375] C. CASTRONOVO, *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, in *Eur. dir. priv.*, 1998, p. 653 ss.; F. D. BUSNELLI, *Spunti per un inquadramento sistematico*, in AA.VV., *Tutela della privacy. Commentario alla L. 31 dicembre 1996, n. 675*, a cura di C. M. Bianca e F. Busnelli, in *Nuove leggi*

Più precisamente il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Il legislatore europeo, oltre ad aver individuato una gamma di basi giuridiche dalle quali dipende la liceità del trattamento, ha fissato una serie di canoni, principi e criteri ai quali quest'ultimo va improntato, pena, nonostante la sussistenza della base giuridica, l'illiceità del trattamento.

In particolare, sulla base dell'art. 5 del Regolamento, i dati personali devono essere:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

civ. comm., 1999, p. 229 ss.; S. RODOTÀ, *Tra diritti fondamentali ed elasticità della normativa: il nuovo Codice sulla privacy*, in *Eur. dir. priv.*, 2004, p. 2 ss.

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).
Chiunque subisca un danno materiale o immateriale causato da una violazione del regolamento ha diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.
Nel caso di concorso di responsabilità, si applica il regime della solidarietà passiva, secondo la regola generale di cui all’art. 2055 c.c.
La disciplina europea consente all’interessato di seguire, controllare e indirizzare la circolazione delle proprie informazioni di carattere personale.
Sono funzionali all'esercizio dei diritti dell'interessato gli obblighi di informazione di cui all'articolo 14 Reg. 2016/679 imposti al titolare quando i dati personali non sono stati ottenuti presso l'interessato e chiaramente preordinati a creare in capo all'interessato quella condizione di piena consapevolezza in ordine alla circolazione di informazioni sul proprio conto che si rileva imprescindibile per consentirgli di avvalersi degli strumenti giuridici di controllo e di indirizzo.
In attuazione del principio dell'esattezza, l'articolo 16 Reg. 2016/679 attribuisce all'interessato il diritto a ottenere, senza ritardo dal titolare, la rettifica dei propri dati personali inesatti ma anche l'integrazione di quelli incompleti alla luce della finalità del trattamento, anche mediante rilascio di una dichiarazione integrativa.
Grande risalto è stato riservato dal Regolamento al diritto alla cancellazione in quanto mezzo per l'esercizio del diritto all'oblio dell'interessato, ossia del potere di riappropriarsi delle informazioni di carattere personale virgola non soltanto come strumento di reazioni a un

trattamento illecito scorretto ma anche come potere sostanziale di autodeterminazione informativa.

La cancellazione dei dati personali può essere richiesta infatti anche in presenza di un trattamento lecito e corretto in conseguenza della scelta libera e consapevole dell'interessato di interrompere il trattamento dei propri dati personali in ordine a una o più finalità determinate, in quanto l'impiego e la circolazione di tali informazioni non vengono più reputati opportuni o comunque non risultano più graditi o ancora confliggono con gli obiettivi e le strategie dell'interessato in ordine alla costruzione o all'evoluzione della propria identità personale o anche soltanto con più limitati fini specifici.

Formale manifestazione del diritto all'oblio si è avuta con il Regolamento (UE) Generale sulla Protezione dei Dati 2016/679, che esplicitamente ha riallacciato la figura ad un testo legislativo.

Infatti, l'articolo 17 - da leggersi insieme ai Considerando 65, 66 e 67 - è rubricato “Diritto alla cancellazione dati (diritto all'oblio)” e sembrerebbe aver positivizzato il diritto all'oblio.

Più precisamente, ai sensi di tale ultima disposizione legislativo, l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

Occorre altresì precisare che il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione, deve adottare le misure ragionevoli, anche tecniche, per informare i titolari del trattamento

che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

Le summentovate regole non si applicano nella misura in cui il trattamento sia necessario:

a) per l'esercizio del diritto alla libertà di espressione e di informazione;

b) per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;

d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;

e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

A ben vedere, il legislatore nell'individuare il diritto alla cancellazione, non ha fatto cenno nel corpus del dettato normativo al più controverso diritto all'oblio: l'inciso, relegato tra parentesi e tra virgolette, non trova una sostanziale e puntuale estrinsecazione.

La disposizione potrebbe ritenersi finalizzata a garantire una tutela piena ed effettiva agli interessati, ai quali dovrà essere quindi fornita una informazione consapevole.

Depone in tal senso il Considerando 66, nel quale il legislatore europeo torna a menzionare il diritto all'oblio allorché afferma che per rafforzare tale diritto nell'ambiente online, è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento, che ha pubblicato dati personali, a informare i titolari del trattamento, che trattano tali dati personali, di cancellare qualsiasi link verso tali dati personali o copia o riproduzione di detti dati personali.

Menziona il diritto all'oblio anche il Considerando 65 che esordisce affermando che un interessato dovrebbe avere il diritto di ottenere la rettifica dei dati personali che lo riguardano e il diritto all'oblio, se la conservazione di tali dati violi il presente Regolamento o il diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento.

La disposizione specifica inoltre che l'interessato dovrebbe avere il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia revocato il proprio consenso o si sia opposto al trattamento dei dati personali che lo

riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al presente regolamento.

Quanto alle modalità per limitare il trattamento dei dati, il Considerando 67 precisa che esse potrebbero consistere, tra l'altro, nel trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati da un sito web.

Negli archivi automatizzati la limitazione del trattamento dei dati personali dovrebbe in linea di massima essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati.

Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato.

In sintesi, dunque, la cancellazione ex art. 17 GDPR - la quale si concretizza tramite un'operazione sui dati che esclude ogni ulteriore conservazione degli stessi - si pone in un rapporto di conseguenza rispetto alla pretesa di oblio che può ben definirsi come un interesse giuridicamente protetto che attinge a profili propri del diritto all'onore e di quello alla riservatezza.

3. Il diritto all'oblio nella giurisprudenza comunitaria

Il rapporto tra Internet e diritto all'oblio è stato al centro di una importante sentenza della Corte di giustizia dell'Unione Europea, emessa il 13 maggio 2014, il noto caso *Google Spain*[376].

Si trattava di una vicenda che aveva ad oggetto il problema dell'accesso ai dati esistenti sulla rete Internet.

In particolare, il caso esaminato dalla Corte di giustizia riguardava il diritto dell'interessato ad ottenere che il motore di ricerca sopprimesse determinati dati dall'elenco dei risultati reperibili sulla rete.

[376] CGUE, 13 maggio 2014**,** C-131/12, *Google Spain SL/Google Inc., Agencia Española de Protección de Datos, Mario Costeja Gonzàlez,* in *https://eur-lex.europa.eu.*
Tra gli innumerevoli commenti della pronuncia in parola, v. i contributi di G.M. RICCIO, *Diritto all'oblio e responsabilità dei motori di ricerca,* in *Dir. inf*., 2014, p. 753 ss.; S. SICA-V. D'ANTONIO, *La procedura di de-indicizzazione*, *ivi*, 2014, p. 703 ss.; G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, *ivi*, p. 591 ss.; G. GIANNONE CODIGLIONE, *Motori di ricerca, trattamento di dati personali ed obbligo di rimozione: diritto all'oblio o all'autodeterminazione informativa*, in *Nuova giur. civ. comm*., 2014, p. 1054 ss. *Ex ceteris*, v. A. PALMIERI-R. PARDOLESI, *Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google*, in *Nuovi Quaderni del Foro Italiano*, 2014, in *http://www.foroitaliano.it*.

Il problema del bilanciamento tra libertà di espressione e diritto alla protezione dei dati personali è affrontato per la prima volta dalla Corte di Giustizia dell'UE nel 2003 nel caso *Bodil Lindqvist*, che concerneva la libertà di diffondere notizie riguardanti terzi soggetti[377].
In particolare, la domanda pregiudiziale interveniva in un procedimento penale a carico della signora Lindqvist, accusata di aver violato la normativa svedese in tema di protezione dei dati personali per aver pubblicato sul proprio sito Internet dati quali nomi, numeri di telefono, informazioni sulla salute e l'attività lavorativa di persone che lavoravano insieme a lei, come volontari in una parrocchia della Chiesa protestante svedese, senza aver informato gli interessati né averne richiesto il consenso.
La questione, sollevata dinanzi ai giudici di Lussemburgo, verteva sulla possibilità di configurare l'inserimento di tali informazioni come trattamento di dati personali ai sensi della Direttiva 95/46 allora vigente.
Le operazioni svolte dalla signora Lindqvist, infatti, non si collocavano né nell'ambito dell'esercizio di attività a carattere meramente personale e domestico, escluse dall'ambito di applicazione della disciplina europea ex art. 3, n. 2, della direttiva, né potevano essere inquadrate come trattamento effettuato esclusivamente a scopi giornalistici o di espressione artistica e letteraria, per i quali erano previste deroghe e sanzioni al fine di tutelare l'esercizio della libertà di espressione.
Risulta, pertanto, assai significativa la risposta affermativa circa la violazione della Corte di giustizia che precisa che la pubblicazione su un sito Internet costituisce un trattamento di dati personali interamente o parzialmente automatizzato, sottolineando la natura peculiare del mezzo Internet, idoneo a diffondere le informazioni ad un numero indeterminato di destinatari[378].
Quanto al bilanciamento con la libertà di espressione, la Corte sancisce che non vi è incompatibilità tra la disciplina europea e il principio generale di libertà di espressione o con i diritti e le libertà che trovano corrispondenza, tra l'altro, nell'art. 10 della CEDU, rimettendo alle autorità e ai giudici nazionali il compito di garantire il contemperamento tra i diritti e gli interessi in gioco, ivi compresi i diritti fondamentali tutelati dall'ordinamento giuridico comunitario.
Dieci anni più tardi la Corte di Lussemburgo decide l'ormai notissimo e assai dibattuto caso *Google Spain*, ampliando ulteriormente la nozione di trattamento dei dati personali, nella

[377] CGUE, 6 novembre 2003, C-101/01, caso *Bodil Lindqvist*, in *https://eur-lex.europa.eu/legal.*
[378] M.G. STANZIONE, *Libertà di espressione e diritto alla privacy nel dialogo delle Corti. Il caso del Diritto all'oblio*, in *Europa e Diritto Privato*, 2020, p. 991 ss.

quale fa ricadere l'attività dei motori di ricerca e riconoscendo il diritto dell'interessato di richiedere al titolare del trattamento la deindicizzazione delle informazioni, vale a dire l'eliminazione dei dati dalla lista dei risultati della ricerca.

Tale diritto è stato qualificato quale "diritto all'oblio", dicitura adottata nel medesimo Regolamento 2016/679data la natura stessa web 2.0, dove le informazioni - anche se non rilanciate o ripubblicate nel corso del tempo - sono perennemente disponibili alla generalità dei destinatari fintantoché sono indicizzate dai motori di ricerca.

Ciò, se da un lato ha sensibilmente esteso la portata della libertà di espressione, in particolare quando è declinata come diritto di informare e di essere informati, dall'altro lato porta con sé il costante rischio della violazione della privacy e dell'identità delle persone.

Sul punto risulta utile ricordare la lettura del considerando n. 66 del Regolamento 2016/679/UE, ove si sancisce che per rafforzare il "diritto all'oblio" nell'ambiente online, è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento, che ha pubblicato dati personali, a informare i titolari del trattamento, che trattano tali dati personali, di cancellare qualsiasi link verso tali dati personali o copia o riproduzione di detti dati.

Nel fare ciò, è opportuno che il titolare del trattamento adotti misure ragionevoli, tenendo conto della tecnologia disponibile e dei mezzi a disposizione del titolare del trattamento, comprese misure tecniche, per informare della richiesta dell'interessato i titolari del trattamento che trattano i dati personali.

In tale prospettiva va interpretata la norma dell'art. 17 del Reg., che disciplina il diritto alla cancellazione e gli obblighi che ne derivano in capo al titolare del trattamento.

La previsione al n. 3, lett. a), esclude l'obbligo del titolare di accogliere la richiesta di cancellazione allorché il trattamento sia necessario per l'esercizio della libertà di espressione e di informazione.

Tali norme vanno lette congiuntamente all'art. 85 Reg., in virtù del quale gli Stati membri devono conciliare la protezione dei dati personali con il diritto alla libertà d'espressione e di informazione.

In particolare, esenzioni e deroghe rispetto a capi specifici del regolamento generale sulla protezione dei dati sono previste a scopi giornalistici o di espressione accademica, artistica o letteraria, a condizione che siano necessarie per conciliare il diritto alla protezione dei dati personali e la libertà d'espressione e di informazione[379].

[379] M.G. STANZIONE, *Libertà di espressione e diritto alla privacy nel dialogo delle Corti*, cit., p. 1010 ss.

Con la sentenza del 2014 sul cosiddetto caso *Google Spain*, la Corte di giustizia ha affermato che il gestore del motore di ricerca è titolare di un trattamento autonomo rispetto all'archivio sorgente e dunque il trattamento del dato da parte del motore di ricerca può essere illecito, anche se non lo è il trattamento originario e cioè l'inserimento della notizia nel *database* sorgente (si pensi all'archivio del giornale che l'ha pubblicata)[380].

In questo modo si delinea un'illiceità a geometria variabile dove la notizia sgradita all'interessato campeggia a pieno titolo nel *database* sorgente ma si ammanta di negatività non appena venga catturata dal *crawler* di Google e, per questa via, messa a disposizione degli utilizzatori del motore di ricerca.

La tutela del diritto all'oblio prescinde dalla natura pregiudizievole dell'informazione che l'interessato vuole deindicizzare.

Il trattamento dei dati personali può infatti risultare incompatibile con l'art. 12 lettera b) della direttiva non soltanto se i dati sono inesatti ma anche se essi sono inadeguati, non pertinenti o eccessivi in rapporto alla finalità del trattamento, oppure non aggiornati o conservati per un arco superiore a quello necessario, a meno che la loro conservazione non si imponga per motivi storici, di cronaca, statistici o scientifici.

Il diritto dell'interessato, a chiedere che l'informazione in questione non venga più messa a disposizione del grande pubblico mediante la sua inclusione in un elenco accessibile tramite Internet, prevale in linea di massima sull'interesse economico del gestore del motore di ricerca ed anche su quello del pubblico a reperire tale informazione in rete, a meno che non risultino ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, tali da rendere preponderante e giustificato l'interesse del pubblico ad avere accesso a tale informazione.

La Corte europea di giustizia ha posto l'accento sui rischi peculiari derivanti dalla prestazione di un servizio di motore di ricerca, vale a dire l'amplificazione della diffusione dei dati del singolo e la "gravità potenziale" dell'ingerenza nel diritto alla riservatezza ed alla protezione dei dati personali consistente nel fornire a chiunque "una visione complessiva strutturata delle informazioni relative a questa persona reperibili in Internet e quindi nel rendere pubblico un profilo più o meno dettagliato di quest'ultima"[381].

---

[380] A. SALARELLI, *Ancora sul diritto all'oblio: cosa cambia dopo la sentenza della Corte di Giustizia Europea contro Google*, in *Italian Journal of Library and Information Science*, 2015, p. 149 ss.; R. GIOVAGNOLI, *Il diritto all'oblio*, in ID., in *Manuale di Diritto civile*, p. 37 ss.

[381] CGUE, 13 maggio 2014, C-131/12, *Google Spain*, cit., par. 80.

R. PETRUSO, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, cit., pp. 243 e 244.

Il ragionamento condotto dai giudici nella pronuncia Google Spain ha rinvenuto il parametro per risolvere il conflitto con la libertà di espressione nell'attualità dell'interesse pubblico alla notizia e nella natura di personaggio pubblico della persona interessata.

Ne deriva che, come si afferma nella sentenza, in tutte le altre ipotesi il diritto della persona interessata alla protezione dei dati personali e all'identità prevalgono su ogni altra considerazione, in particolare sugli interessi economici dei gestori del motore di ricerca.

Risolvendo il caso specifico, nel quale l'attore aveva chiesto l'eliminazione del dato che collegava la sua persona ad un pignoramento, effettuato per la riscossione coattiva dei crediti previdenziali, la Corte ha affermato che sussisteva il diritto alla soppressione dei link corrispondenti esistenti nella rete in quanto, anche in considerazione del lungo lasso di tempo trascorso (16 anni dalla pubblicazione della notizia originaria), l'interessato aveva diritto a che quelle informazioni non fossero più collegate alla sua persona.

Da queste brevi considerazioni si evince che la disciplina dettata dal caso *Google Spain* sul diritto all'oblio non è proprio completamente esaustiva come si auspicava, essendo rimasti ancora aperti diversi interrogativi che preannunciavano nuovi sviluppi.

In tale cornice, dunque, si inserisce la sentenza *Google France*.[382]

Infatti, di recente la Grande Camera della Corte di giustizia è tornata sul rapporto tra il diritto all'oblio e obblighi del gestore del motore di ricerca con due sentenze, rese entrambe il 25 settembre 2019, in risposta a ordinanze di rinvio pregiudiziale del Consiglio di Stato francese, relativi a *Google France*[383].

L'arresto *Google Spain* segna un momento di svolta lungo il percorso che ha portato al riconoscimento, prima pretorio, poi normativo, del diritto all'oblio nello spazio comunitario.

Le sentenze del 2019 si pongono in rapporto di continuazione rispetto alla pronuncia *Google Spain*, che costituisce un antecedente giurisprudenziale imprescindibile.

Nell'ambito di queste sentenze vi è stata la ridefinizione della relazione intercorrente tra privato, dati personali e Internet Service Provider (ISP), che è stato investito di una responsabilità strumentale alla pretesa, al diritto di far rimuovere il link contenente informazioni non più attuali e non più preordinati a soddisfare un concreto interesse pubblico[384].

---

[382] L. GRIMALDI, *Diritto alla deindicizzazione: dati sensibili, potere e responsabilità-Google France*, in *Dir. inf.*, 2020, p. 265 ss.

[383] CGUE, Grande Camera, 24 settembre 2019, in C-136/201 e C-112/2017, caso *Google France*, in *Dir. inf.*, 2020, p. 254 ss.

[384] In assenza di una normativa che disciplinasse la procedura di deindicizzazione, i motori di ricerca hanno predisposto un iter finalizzato alla deindicizzazione dei link associati al nome del soggetto istante. Quella offerta da Google richiede che siano indicati gli URL dei link da occultare, che sia giustificata la pertinenza di

In seguito alla *Google Spain* e alle sentenze *Google France* il ruolo assunto dal gestore del motore di ricerca è stato considerato ancora maggiore rispetto a quello degli editori sotto il profilo della responsabilità, per due ordini di ragioni: anzitutto, con riguardo alla visibilità del dato presente nell'elenco di risultati del *search engine*, che diventa accessibile universalmente a chiunque effettui una ricerca a partire dal nome della persona interessata; secondariamente, a causa dell'attività svolta dal motore di ricerca e consistente nel procedimento di aggregazione dei dati e di visualizzazione dei risultati.

Esso comporta, in particolare, la creazione di un profilo più o meno dettagliato della persona oggetto di ricerca, che si ripercuote sulla sua immagine sociale, sfuggendo a qualsiasi forma di controllo da parte dell'interessato e risultando permanentemente attualizzata.

Ciò ha giustificato il riconoscimento del diritto di richiedere in via diretta e immediata ai motori di ricerca l'eliminazione dei link in questione dall'elenco dei risultati, generando una sostanziale asimmetria tra il ruolo svolto dal gestore dei motori di ricerca e quello dei responsabili delle pagine web che vengono indicizzate.

Da tale discrasia deriva che la responsabilità del gestore, essendo limitata all'attività di indicizzazione, prescinde totalmente dalla permanenza del dato sulla rete.

Invero, la richiesta rivolta al gestore è del tutto autonoma rispetto all'istanza presentata eventualmente al titolare del sito sorgente, finalizzata alla cancellazione dell'informazione.

Su questo punto le sentenze convergono nel circoscrivere la responsabilità di Google all'indicizzazione dei risultati di ricerca[385].

In particolare, la prima pronuncia della Grande Camera del 2019 sembra riconoscere al gestore del motore di ricerca la facoltà di verificare in autonomia e decidere di conseguenza, prima di operare una deindicizzazione, se l'inserimento del link contestato nell'elenco dei risultati si riveli strettamente necessario per proteggere la libertà di informazione degli utenti di Internet potenzialmente interessati ad avere accesso a tale pagina[386].

In sintesi la Corte di giustizia ha affermato che, sebbene i diritti della persona prevalgano, di norma, sulla libertà di informazione degli utenti di Internet, tale equilibrio può nondimeno

---

tali link al soggetto richiedente e che sia argomentata la rilevanza dei collegamenti inappropriati o non aggiornati.

Si interrogano sulle carenze di tali procedure, S. SICA-V. D'ANTONIO, *La procedura di de-indicizzazione*, in G. RESTA-V. ZENO ZENCOVICH (a cura di), *Il Diritto All'Oblio Su Internet Dopo La Sentenza Google Spain*, Roma, 2015, p. 162 ss.

Trattasi di un diritto che, per come configurato dalla Corte di Giustizia, incontra dei limiti solo in un preminente interesse pubblico dipendente dal ruolo rivestito dal soggetto nella vita pubblica, dalla natura dell'informazione e dal tempo trascorso rispetto a quando la notizia è stata pubblicata.

[385] L. GRIMALDI, *Diritto alla deindicizzazione: dati sensibili, potere e responsabilità- Google France*, cit., p. 277 ss.

[386]CGUE, Grande Camera, 24 settembre 2019, in C-136/201, cit.

essere rimesso in discussione a seconda della natura delle informazioni di cui trattasi e del suo carattere sensibile per la vita privata della persona interessata, nonché dell'interesse del pubblico a disporre di tale informazione, il quale può variare in base al ruolo che tale persona riveste nella vita pubblica.

La Corte ha concluso quindi nel senso che il gestore di un motore di ricerca, quando riceve una richiesta di deindicizzazione riguardante un link verso una pagina Internet nella quale sono pubblicati dati sensibili del genere, deve, sulla base di tutte le circostanze pertinenti della fattispecie e tenuto conto della gravità dell'ingerenza nei diritti fondamentali della persona interessata al rispetto della vita privata e alla protezione dei dati personali, verificare se l'inserimento di detto link nell'elenco dei risultati, visualizzato in esito ad una ricerca effettuata a partire dal nome della persona in questione, si riveli strettamente necessario per proteggere la libertà di informazione degli utenti di Internet potenzialmente interessati ad avere accesso a tale pagina Internet mediante una ricerca siffatta.

La Corte ha precisato altresì che, quand' anche il gestore di un motore di ricerca dovesse constatare che la persona interessata non ha diritto alla deindicizzazione di simili link per il fatto che l'inserimento considerato si rivela strettamente necessario per conciliare i diritti della persona interessata rispetto alla vita privata e alla protezione dei dati con la libertà di informazione degli utenti di Internet potenzialmente interessati, tale gestore è in ogni caso tenuto, al più tardi al momento della richiesta di deindicizzazione, a sistemare l'elenco dei risultati in modo tale che l'immagine globale che ne risulta per l'utente di Internet rifletta la situazione giudiziaria attuale, il che necessita in particolare che compaiano per primi nel suddetto elenco i link verso pagine Internet contenenti informazioni a tal proposito.

Con la seconda sentenza la Corte ha ulteriormente precisato che il gestore di un motore di ricerca non è tenuto ad effettuare la deindicizzazione in tutte le versioni del suo motore di ricerca ma è tenuto ad effettuarla nelle versioni corrispondenti a tutti gli Stati membri e ad attuare misure che scoraggino gli utenti di Internet dall'avere accesso, a partire da uno degli Stati membri, ai link di cui trattasi contenuti nelle versioni extra UE di detto motore[387].

In altri termini, il motore di ricerca chiamato alla deindicizzazione deve procedere a tale operazione non più con riguardo a tutte le estensioni territoriali del c.d. "dominio", quindi non più a livello globale, bensì con riguardo alle estensioni territoriali riconducibili agli Stati

[387] CGUE, Grande Camera, 24 settembre 2019, in C-112/2017, cit.

membri (es. motorediricerca.it; motorediricerca.fr, ecc.), non dovendo quindi intervenire sulle estensioni relative a continenti diversi da quello europeo[388].

La Corte sottolinea che, in un mondo globalizzato, l'accesso da parte degli utenti di Internet, in particolare quelli localizzati al di fuori dell'Unione, all'indicizzazione di un link, che rinvia a informazioni concernenti una persona il cui centro di interessi si trova nell'Unione, può produrre effetti immediati e sostanziali sulla persona in questione all'interno dell'Unione stessa, ragion per cui una deindicizzazione mondiale sarebbe idonea a conseguire pienamente l'obiettivo di protezione perseguito dal diritto dell'Unione.

Essa precisa tuttavia che molti Stati terzi non riconoscono il diritto alla deindicizzazione o comunque adottano un approccio diverso per tale diritto.

Con l'avvento di Internet, che annulla la percezione dello scorrere del tempo, si è posta l'esigenza di tutelare il soggetto da una esposizione permanente e costante alle informazioni, derivante dal loro inserimento nelle banche dati dei motori di ricerca.

Misure idonee a perseguire tale obiettivo sono quelle tese a contestualizzare e ad aggiornare la notizia meritevole di attenzione.

In tal modo, difatti, è possibile salvaguardare l'identità personale del soggetto cui la notizia si riferisce e, al contempo, garantire il diritto della collettività ad essere informati in maniera corretta e completa.

Al contempo, la Corte ammette il gestore a verificare se la presenza del *link* sul motore di ricerca sia strettamente necessaria per tutelare la libertà di informazione degli utenti di Internet, i quali hanno un potenziale interesse a conoscere tali dati, accedendo alla pagina web mediante i *link* dei quali si chiede la rimozione.

Sotto questo profilo, viene posto l'accento sull'importanza del bilanciamento tra i valori antagonisti, annoverati entrambi tra i diritti fondamentali della persona in numerosi *Bill of Rights*, tra i quali si richiamano gli artt. 7,8 e 11 della Carta dei diritti fondamentali dell'Unione europea (CDFUE).

La Corte aggiunge che il diritto alla protezione dei dati personali non è una prerogativa assoluta ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali in ossequio al principio di proporzionalità.

Inoltre, l'equilibrio tra il diritto al rispetto della vita privata alla protezione dei dati personali e la libertà di informazione degli utenti di Internet può variare notevolmente nel mondo.

---

[388] R. PARDOLESI, *Oltre ''Google Spain'' e il diritto all'oblio*, in *Foro it.*, 2017, c. 219 ss.
C. SCARPELLINO, *Un oblio tutto europeo*, in *Danno e resp.*, 2020, p. 209 ss.

Dalla normativa non emerge che il legislatore dell'unione europea abbia proceduto a tale bilanciamento per quanto riguarda la portata di una deindicizzazione al di fuori dell'Unione né che abbia scelto di attribuire ai diritti dei singoli una portata che vada oltre il territorio degli Stati membri.

Non risulta neppure che esso abbia inteso imporre a un operatore, come Google, un obbligo di deindicizzazione riguardante anche le versioni nazionali del suo motore di ricerca che non corrispondono agli Stati membri.

Il diritto dell'Unione non prevede per giunta strumenti e meccanismi di cooperazione per quanto riguarda la portata di una deindicizzazione al di fuori dell'Unione.

La Corte conclude quindi che allo stato attuale non sussiste per il gestore di un motore di ricerca che accoglie una richiesta di deindicizzazione presentata dall'interessato, eventualmente a seguito di un'ingiunzione di un'autorità di controllo, di un'autorità giudiziaria di uno Stato membro, un obbligo derivante dal diritto dell'Unione di fare tale dell'intento tutte le versioni del suo motore di ricerca.

Il diritto dell'Unione obbliga tuttavia il gestore di un motore di ricerca ad effettuare tale deindicizzazione nelle versioni del suo motore di ricerca corrispondente a tutti gli Stati membri e ad adottare misure sufficientemente efficaci per garantire una tutela effettiva dei diritti fondamentali della persona interessata.

In tal senso una simile idea di indicizzazione deve, se necessario, accompagnarsi a misure che permettano effettivamente impedire, o quantomeno di scoraggiarli seriamente dal farlo, agli utenti di Internet che effettuano la ricerca sulla base del nome dell'interessato a partire da uno degli Stati membri di accedere, attraverso l'elenco dei risultati visualizzati in seguito a tale ricerca mediante una versione extra Ue del suddetto motore, ai link oggetto della domanda di deindicizzazione.

Il giudice nazionale dovrà verificare che le misure attuate dalla *Google Inc*. soddisfino tali esigenze.

Infine, la Corte osserva che il diritto dell'Unione europea, pur non imponendo allo stato attuale che la deindicizzazione verta su tutte le versioni del motore di ricerca, neppure lo vieta.

Pertanto le autorità degli Stati membri restano competenti ad effettuare, conformemente agli standard nazionali di protezione dei diritti fondamentali, un bilanciamento tra, da un lato, il diritto dell'interessato alla tutela della sua vita privata e alla protezione dei suoi dati personali e, dall’altro, il diritto alla libertà dell'informazione e, al termine di tale bilanciamento, a

richiedere, se del caso, che il gestore del motore di ricerca effetti una deindicizzazione su tutte le versioni del suddetto motore.

Ai sensi dell'art. 17, 2º comma, il destinatario della richiesta di cancellazione, che già abbia reso pubblici i dati personali dell'interessato, è obbligato, tenendo conto della tecnologia disponibile e dei relativi costi, ad informare eventuali altri titolari del trattamento, che stanno trattando i dati personali oggetto della richiesta di cancellazione, al fine di permettere l'eliminazione di qualsiasi link, copia o riproduzione degli stessi.

Da ciò deriva che se il destinatario della richiesta è il gestore del sito fonte, questi dovrà informare i motori di ricerca, che dovranno a loro volta cancellare i dati di cui si tratta.

Se, invece, il destinatario della richiesta è il motore di ricerca, questi dovrà informare gli altri titolari del trattamento, quindi in primo luogo il sito fonte, ma anche tutti gli altri soggetti che stiano effettuando un trattamento sui dati che il motore di ricerca ha deciso di cancellare, dando seguito alla richiesta dell'interessato; ciò, tuttavia, senza poter pretendere dal motore di ricerca sforzi da ritenersi spropositati, o meglio sproporzionati in termini di costi e tecnologie applicabili.

A partire dalla sentenza pronunciata dalla Grande Sezione della Corte di giustizia, definita un *landmark case*, i giudici europei hanno qualificato per la prima volta l'attività del motore di ricerca, consistente nella raccolta, registrazione, organizzazione, conservazione e comunicazione di dati, come trattamento di dati personali, riconoscendo, di conseguenza, il gestore del motore di ricerca quale responsabile del trattamento.

Pertanto, la normativa in materia di protezione dei dati si applica anche al motore di ricerca, implicando per l'Internet Service Provider (ISP) l'obbligo di eliminare dall'elenco dei risultati di ricerca quei link che rinviano a pagine web pubblicati da terzi, qualora il trattamento non sia più conforme alla direttiva e su istanza dell'interessato.

Il diritto alla deindicizzazione, dunque, mira a conseguire un effetto diverso dalla cancellazione della notizia *tout court*; invero, essa non scompare della rete, essendo ancora presente sul sito sorgente.

Piuttosto, viene reso più difficile il reperimento del dato *online*, conferendo un ulteriore volto al diritto all'oblio inteso come *right not to be found easily*[389].

La decisione assunta dai giudici di Lussemburgo spinge a riflettere sulla rilevanza del bilanciamento in tema di oblio e sul ruolo assegnato agli operatori economici privati.

[389] M.G. STANZIONE, *Libertà di espressione e diritto alla privacy nel dialogo delle Corti*, cit., p. 1108 ss.

Giova considerare le posizioni giuridiche che si contrappongono nel caso in esame, ciascuna corrispondente a un soggetto coinvolto nel trattamento: la prima concerne l'interessato alla rimozione, il quale, presentando istanza di *delisting*, vanta il diritto alla riservatezza e alla protezione dei dati personali; la seconda, al contrario, coinvolge gli utenti del web, potenzialmente interessati ad accedere al link per conoscere l'informazione ivi contenuta. Essa si configura quale declinazione del diritto all'informazione.

I diritti coinvolti vanno ascritti, nelle argomentazioni della Corte (punto 59), al catalogo di diritti fondamentali, trovando una importante guarentigia negli artt. 7,8 e 11 dalla Carta di Nizza.

Come sostenuto dalla Corte nel negare la natura assoluta del diritto all'oblio, la normativa comunitaria prevede il loro necessario contemperamento.

Sotto questo profilo, peraltro, il giudice dell'Unione richiama l'art. 52 della Carta con riferimento ai criteri che legittimano le limitazioni dei diritti ivi sanciti.

Contestualmente, si afferma la generale prevalenza del diritto all'oblio, ancora maggiore quando coinvolge dati sensibili, sul contrapposto diritto all'informazione, che si riflette in termini di stretta necessità della deroga all'obbligo di rimozione automatica dei link, gravante in capo al gestore.

Inoltre, occorre tenere a mente che la posizione assunta dai giudici comunitari circa la generale soccombenza del diritto ad accedere all'informazione sul diritto all'oblio non trova riscontro nella giurisprudenza offerta dalla Corte europea dei diritti dell'uomo, in particolare nella pronuncia *Węgrzynowski and Smolczewski v. Poland*.

Difatti, la Corte di Strasburgo fa prevalere la libertà di espressione, interpretando in maniera restrittiva le limitazioni a tale libertà anche nell'ipotesi di notizie diffamatorie presenti sul sito web, optando, dunque, per l'obbligo di aggiornamento e di rettifica della notizia in luogo della sua rimozione, misura considerata sproporzionata ed eccessivamente lesiva libertà di espressione e conoscenza.

La sentenza della CEDU del 16 luglio 2013, *nel caso Węgrzynowski and Smolczewski v. Poland* [390], è intervenuta sul tema del bilanciamento tra libertà di espressione, interessi individuali incisi dall'esercizio di tale libertà e interesse pubblico a conoscere la data informazione.

Nel caso in questione, in realtà, non veniva realmente in rilievo il diritto all'oblio in quanto il giudice nazionale aveva già accertato il carattere diffamatorio della notizia, la quale

[390] Corte EDU, 16 luglio 2013, *caso Węgrzynowski and Smolczewski v. Poland,* Ric. n. 33846/07, in *dirittocomparati.it*

dunque, nella tesi del ricorrente, andava rimossa da Internet in quanto, per l'appunto, diffamatoria e non in quanto lesiva del diritto all'oblio.

Tuttavia, la sentenza risulta particolarmente significativa giacché disconosce all'interessato il diritto ad ottenere la rimozione del materiale informativo pubblicato online, in considerazione del fatto che, secondo la Corte, il punto di equilibrio tra conservazione della notizia (pur non corretta) nel patrimonio informativo dei giornali in rete e la pretesa della persona coinvolta alla conservazione dell'identità personale può essere individuato nell'eventuale obbligo, posto a carico dell'*editor,* di pubblicare un'aggiunta o una nota ad una fonte disponibile in un archivio Internet, che specifici la circostanza che lo stesso sia stato reputato diffamatorio dall'Autorità giudiziaria.

Per scartare la diversa ipotesi, costituita dall'ordinare la rimozione del contenuto illecito da Internet, la Corte rileva come la totale eliminazione di un articolo giornalistico pubblicato on-line non rientri affatto nelle prerogative giurisdizionali.

Sul punto, i Giudici di Strasburgo entrano nel merito della questione, osservando che "*it is not the role of judicial authorities to engage in rewriting history by ordering the removal from the public domain of all traces of publications which have in the past been found, by final judicial decisions, to amount to unjustified attacks on individual reputations"*.

Il principio risulta corroborato dalla protezione offerta dall'art. 10 della Convenzione Europea dei Diritti dell'Uomo nei confronti dell'interesse pubblico all'accesso agli archivi Internet della stampa.

Conseguentemente, il rimedio della rimozione integrale di un articolo giornalistico diffamatorio, pubblicato nella versione online di un quotidiano, finalizzata alla tutela della reputazione degli individui ex art. 8 della Convenzione, risulta sproporzionato.

Il punto di incontro tra le esigenze poste dai due articoli di legge appena citati, viceversa e come già accennato, dovrebbe individuarsi - secondo la Corte - nell'obbligo, a carico dell'*editor*, di pubblicare aggiunte o precisazioni all'articolo in questione, che consentano al pubblico un'immediata contestualizzazione dello stesso alla luce degli avvenimenti storici successivi alla pubblicazione quale, ad esempio, l'emissione di una sentenza che ne accerti il carattere diffamatorio[391].

[391] P. GIANNITI, *La "comunitarizzazione" della "Carta" a seguito del Trattato di Lisbona*, in ID. (a cura di), *I diritti fondamentali nell'Unione europea. La Carta di Nizza dopo il Trattato di Lisbona*, Bologna, 2013, p. 357 ss.; K. STERN, *La Carta dei diritti fondamentali dell'Unione europea. Riflessioni sulla forza vincolante e l'ambito di applicazione dei diritti codificati nella Carta*, in *Rivista italiana di diritto pubblico comunitario*, 2014, p. 184 ss.; C. CHIARIELLO, *Il valore costituzionale della Carta di Nizza: un problema ancora aperto anche alla luce della sentenza n. 269/2017 della Corte costituzionale*, in *Consulta Online*, 2018, p. 381 ss.

Le differenti soluzioni cui sono pervenuti i due organi giudicanti testimoniano l'estrema complessità di tracciare il ragionevole punto di equilibrio tra i diritti coinvolti, che costituiscono, nella immagine dell'Avvocato Generale Jääskinen, una "costellazione di posizioni giuridiche particolarmente complessa".

In ogni caso secondo la Corte di giustizia, come si è già tentato di mettere in rilievo, l'attività di bilanciamento, dunque, grava preliminarmente sulla figura del gestore, subentrando solo in secondo momento e in via eventuale l'intervento dell'autorità nazionale di controllo in materia di privacy o in alternativa del giudice comune.

In tal guisa, si conferma la scelta di rimettere il primo vaglio di fondatezza dell'istanza di *delisting* in capo al prestatore di servizi, il quale si trasforma in arbitro discrezionale del diritto all'oblio, con potenziali rischi a danno dell'informazione e della cd. memoria collettiva digitale.

Una tale visione da parte della Corte degli intermediari informatici conferma, in linea con il progresso tecnologico che li vede sempre più protagonisti attivi delle attività sul web, la possibilità di una responsabilizzazione maggiore, in vista di una tutela effettiva dei diritti fondamentali della persona.

4. Il diritto all'oblio, il diritto di cronaca e la rievocazione storica nella giurisprudenza italiana

Nel diritto nazionale una delle più recenti e significative pronunce sul diritto all'oblio è la sentenza della Corte di cassazione del 2018, sul cosiddetto caso Venditti[392].

In tale sentenza i giudici di legittimità hanno tentato di tracciare un bilanciamento tra oblio e cronaca, il cui rapporto è molto delicato ed è l'interprete a dover operare una sapiente opera di coordinamento.

Le Sezioni unite già anni prima si erano già pronunciate in merito ad un argomento simile, indicando che la lesione dell'onore e della reputazione può essere giustificata in base al diritto di cronaca solo al ricorrere di tre condizioni:

1) la verità oggettiva della notizia pubblicata;
2) l'interesse pubblico alla conoscenza della notizia (pertinenza);
3) la correttezza formale dell'esposizione (continenza)[393].

[392] Cass. civ., Sez. I, 20 marzo 2018, n. 6919, in *Giuricivile.it*, 2019, con nota di G. DEL VECCHIO, *Il diritto all'oblio e i limiti al suo esercizio: il caso Venditti.*

[393] Cass. civ., Sez. un., 18 ottobre 1984, n. 5259, in *www.altalex.com*

Con il caso Venditti la Corte ha affermato che il diritto fondamentale all'oblio può subire una compressione a favore dell'ugualmente fondamentale diritto di cronaca solo in presenza di specifici e determinati presupposti:

- il contributo arrecato dalla diffusione dell'immagine o della notizia a un dibattito di interesse pubblico;
- l'interesse effettivo e attuale alla diffusione dell'immagine o della notizia per ragioni di giustizia, di polizia o di tutela dei diritti e delle libertà altrui, ovvero per scopi scientifici, didattici o culturali;
- l'elevato grado di notorietà del soggetto rappresentato, per la peculiare posizione rivestita nella vita pubblica del Paese;
- le modalità impiegate per ottenere e nel dare l'informazione, che deve essere veritiera, diffusa con modalità non eccedenti lo scopo informativo, nell'interesse del pubblico e scevra da insinuazioni o considerazioni personali, sì da evidenziare un esclusivo interesse oggettivo alla nuova diffusione;
- la preventiva informazione circa la pubblicazione o trasmissione della notizia o dell'immagine distanza di tempo, in modo da consentire all'interessato il diritto di replica prima della sua divulgazione al pubblico.

Come emerge dalla giurisprudenza esaminata, solo impropriamente e a costo di un'eccessiva semplificazione, il tema dell'oblio può essere ricondotto a un mero bilanciamento tra il diritto alla privacy, da un lato, e il diritto di cronaca, dall'altro.

Le situazioni giuridiche che innervano il diritto all'oblio sono più diverse, coinvolgendo non solo altri diritti della personalità, come il diritto all'identità personale, all'immagine, alla riservatezza, all'onore e alla reputazione etc., ma anche delicate situazioni costituzionalmente rilevanti, legate alla funzione rieducativa della sanzione penale e al diritto del reo a reinserirsi nella società e a rifarsi una vita, senza che gli eventi del passato continuino a condizionarne l'esistenza.

Per converso, mette conto osservare come non ogni rievocazione dei fatti del passato effettuato dalle testate giornalistiche sia sempre supportata dal diritto di cronaca.

Spesso l'evocazione avviene per mere finalità commerciali e di sfruttamento economico (come nel caso Venditti), per il solo fatto che un certo argomento incontra l'interesse del pubblico[394].

[394] P. STANZIONE, *Informazione: potere, contropotere e libertà del cittadino?*, in *Riv. dir. priv*., 1992, p. 339 ss.

La questione del bilanciamento tra il diritto all'oblio e il diritto di cronaca è stata recentemente rimessa alle Sezioni unite da parte della Sezione III.

L'ordinanza interlocutoria (20084/2018) ha osservato che il diritto all'oblio è stato oggetto di alcune recenti pronunce della I Sezione civile, le quali hanno riconosciuto a determinate condizioni la prevalenza del medesimo sul diritto all'informazione.

In particolare, l'ordinanza interlocutoria si sofferma sui principi enunciati dalla sentenza 20 marzo 2018, n. 6919.

La Suprema Corte nel marzo 2018 ha individuato alcuni specifici presupposti in presenza dei quali il diritto all'oblio può arretrare in favore del diritto di cronaca, quali, per esempio, la sussistenza di un contributo ad un dibattito di interesse pubblico (riprendendo il concetto di attualità già delineato in passato); l'interesse effettivo ed attuale alla diffusione della notizia; la notorietà del soggetto rappresentato; le modalità con le quali la notizia è stata diffusa e , infine, la preventiva informazione all'interessato, al fine di rendere effettivo il diritto di replica prima della divulgazione.

L'attenzione della giurisprudenza è stata richiamata anche sull'attività di elaborazione e conservazione degli archivi, attività precipua del mondo del giornalismo e aspetto delicato, in special modo avendo a riguardo la tutela dei dati personali.

D'altra parte, la materia è stata oggetto anche di un recente intervento della legislazione europea, con il Regolamento Ue n. 2016/679, il cui articolo 17 prevede che, a determinate condizioni, l'interessato abbia diritto a chiedere la rimozione dei dati personali che lo riguardano e che siano stati resi pubblici.

Rileva l'ordinanza, in conclusione, come appaia oramai indifferibile l'individuazione di univoci criteri di riferimento che consentano agli operatori del diritto e ai consociati di conoscere preventivamente i presupposti in presenza dei quali un soggetto ha diritto di chiedere che una notizia a sé relativa, pur legittimamente diffuse in passato, non resti esposta a tempo indeterminato alla possibilità di una nuova divulgazione.

In particolare, ad avviso della Corte, non è ancora dato evincere con certezza se i presupposti individuati dalla giurisprudenza siano richiesti in via concorrente o in via alternativa.

Sulla questione rimessa dalla III Sezione, le Sezioni unite si sono pronunciate con la sentenza del 22 luglio 2019, n. 19681.

Le summentovate Sezioni unite hanno individuato tre possibili declinazioni del diritto all'oblio:

i) quella di chi desidera non vedere nuovamente pubblicate notizie relative a vicende, in passato legittimamente diffuse, quando è trascorso un certo lasso di tempo tra la prima e la seconda pubblicazione'';

ii) quella, connessa all'uso di internet ed alla reperibilità delle notizie nella rete, consistente nell'esigenza di collocare la pubblicazione, avvenuta legittimamente molti anni prima, nel contesto attuale;

iii) quella, infine, trattata nella sentenza *Google Spain* della Corte di giustizia dell'Unione Europea, nella quale l'interessato fa valere il diritto alla cancellazione dei dati[395].

Il focus della decisione delle Sezioni unite è incentrato nell'ambito della prima delle tre alternative su indicate, trattandosi di una vicenda relativa alla ripubblicazione su quotidiani di una notizia di circa ventisette anni prima, relativa ad un omicidio.

Nell'ambito di una rubrica settimanale, che rievocava i delitti più efferati rimasti impressi nella comunità locale, era stata ripubblicata infatti anche la storia di un marito che aveva ucciso la moglie, senza omettere le generalità del reo.

L'uomo, già espiata la pena, agiva in giudizio contro la cronista ed il giornale. Questi lamentava un profondo senso di angoscia e prostrazione cagionato dalla pubblicazione, tale da incidere sulle sue già precarie condizioni di salute. Segnalava altresì il notevole danno all'immagine e alla reputazione in quanto nuovamente esposto ad una "gogna mediatica" quando era ormai riuscito a reinserirsi nella società grazie a una nuova vita ed allo svolgimento di un'apprezzata attività.

L'attore denunciava a suo danno la palese violazione del diritto all'oblio, discendendone gravi danni, patrimoniali e non patrimoniali, vista anche la cessazione dell'attività.

Esigeva pertanto adeguato risarcimento.

I convenuti contestavano la pretesa precisando come l'articolo s'iscrivesse entro una rubrica del giornale, con cadenza settimanale, tesa a rievocare taluni fatti di cronaca nera consumatisi nella città, i quali avevano profondamente colpito e turbato la collettività del piccolo centro.

La rievocazione dell'episodio, dopo considerevole tempo, non poteva vulnerare il diritto all'oblio in quanto parte di una rievocazione settimanale di avvenimenti accaduti negli ultimi quarant'anni.

---

[395] A. SPANGARO, *Notizie sul web e oblio: il conflitto tra cronaca, reputazione, riservatezza*, in *Giur. it.*, 2021, p. 1331 ss.

Il giudice di prime cure e la Corte d'Appello non accoglievano la domanda. Difettava, a loro giudizio, ogni gratuita e strumentale rievocazione del delitto oltre che ogni volontaria spettacolarizzazione idonea a provocare la pretesa offesa triviale o irridente del sentimento umano.

Secondo la Corte d'appello, in particolare, scopo della pubblicazione era offrire una sponda di riflessione per i lettori su temi delicati quali emarginazione, la gelosia, la depressione, la prostituzione, con tutti i risvolti e le implicazioni che queste realtà possono determinare nella vita quotidiana.

D'altronde sui diciannove omicidi rievocati v'era stato lungo confronto da parte dell'opinione pubblica locale.

Vieppiù, secondo la Corte, la descrizione dell'omicidio era avvenuta senza accostamenti suggestionanti e/o fuorvianti sottintesi.

Il nome del colpevole, per giunta, risultava solo nel corpo dell'articolo e non nel titolo in grassetto, mentre in testa all'articolo, e con caratteri più piccoli, era scritto il riferimento.

Anzi, la figura del protagonista della vicenda veniva tratteggiata come vittima di un contesto di disagio psicologico, scorgendosi un corretto bilanciamento tra il diritto di cronaca e diritto all'oblio, ovvero tra gli artt. 2 e 21 Cost.

Nel caso di specie, dunque, il Giudice di merito non ravvisava alcuna gratuita e strumentale rievocazione del passato né volontarie spettacolarizzazioni.

Neppure emergeva alcun desiderio di nuova condanna mediatica e sociale in danno dell'attore.

Piuttosto si riportava il progetto editoriale in questione al costituzionale diritto di cronaca, di libertà di stampa e di espressione.

Avverso la sentenza di appello l'attore ricorreva in Cassazione.

Di qui, la Terza Sezione Civile della Suprema Corte, con ordinanza interlocutoria del 5 novembre 2018 n. 28084, trasmetteva gli atti al Primo Presidente per valutare l'assegnazione della questione alle Sezioni unite, evidenziando la particolare importanza di stabilire precisi confini tra diritto all'oblio e diritto di cronaca[396].

L'elaborazione giurisprudenziale, in particolare della Suprema Corte, ha nel tempo ricondotto il diritto alla riservatezza nell'alveo dell'art. 2 Cost. e ha delineato i criteri del bilanciamento tra quest'ultimo e la libertà di stampa, in virtù dei quali, in primo luogo, la pubblicazione deve essere giustificata dalla funzione dell'informazione e conforme ai canoni

[396] A. SPATUZZI, *Diritto all'oblio e rievocazione storica. Il bilanciamento delle Sezioni Unite*, in *Diritto di Famiglia e delle Persone*, 2020, p. 1260 ss., nota a Cass. civ., Sez. un., 22 luglio 2019, n.19681.

della correttezza professionale e, in secondo luogo, deve sussistere un apprezzabile interesse del pubblico alla conoscenza dei fatti privati, in considerazione di finalità culturali o didattiche e di una rilevanza sociale dei fatti stessi.

In questa prospettiva, la questione del c.d. diritto all'oblio introduce il profilo dinamico della tutela della riservatezza e dell'identità della persona, imperniato sull'elemento temporale[397]. È proprio il trascorrere del tempo, infatti, che, incidendo sul configurarsi dell'interesse pubblico alla notizia, modifica l'equilibrio tra gli interessi in gioco.

Su questi presupposti si fonda il ragionamento condotto dalle Sezioni unite della Cassazione italiana nella recente sentenza del 22 luglio 2019 che - con una puntuale ricostruzione dell'elaborazione giurisprudenziale nazionale e sovranazionale - tenta di mettere ordine nella materia magmatica del conflitto tra libertà di espressione e diritto alla privacy, rinvenendo un punto di equilibrio nel principio per cui il diritto ad informare non equivale in automatico al diritto alla nuova e ripetuta diffusione dei dati personali[398].

Le Sezioni unite 2019 hanno delimitato anzitutto il campo d'indagine, precisando che, fra le varie situazioni che possono interessare il tema dell'oblio, quella oggetto della vicenda concreta riguarda esclusivamente la legittimità della ripubblicazione di quanto a suo tempo è stato pubblicato senza contestazioni.

A tal proposito, le Sezioni unite hanno chiarito che quando un giornalista pubblica di nuovo, a distanza di un lungo periodo di tempo, una notizia già pubblicata - la quale all'epoca

---

[397] L'elaborazione giurisprudenziale italiana sul problema del bilanciamento tra libertà di espressione e privacy risente fortemente dell'influenza delle pronunce della Corte EDU, cui non manca di far riferimento la sentenza della Cassazione in analisi. I giudici di Strasburgo elaborano i criteri generali di tale bilanciamento, rinvenendone il fondamento nel rapporto tra la libertà di informare e di essere informati sancita dall'art. 10 CEDU e la protezione della vita privata ai sensi dell'art. 8 della Convenzione.

Il discrimen utilizzato dalla Corte è, in primo luogo, la sussistenza dell'interesse generale nei confronti delle vicende oggetto di pubblicazione. Ad esso, tuttavia, deve aggiungersi il rispetto di altre condizioni, quali il fatto che l'interessato sia un personaggio pubblico e, infine, che la notizia sia ritenuta affidabile, anche in base alle modalità con cui è stata acquisita.

In tale prospettiva, è di rilievo la pronuncia della Corte EDU del 19 ottobre 2017, riguardante la richiesta di rimozione da parte di un uomo d'affari ucraino residente in Germania di un articolo on line in cui si rendeva noto il suo presunto coinvolgimento in vicende di corruzione volte a ottenere licenze televisive in Ucraina. Secondo il ragionamento della Corte, la violazione del diritto alla vita privata e familiare è esclusa in virtù della natura di personaggio pubblico dell'interessato nonché della sussistenza di un interesse pubblico all'apprendimento di quelle informazioni, per cui il diritto della generalità dei consociati alla conoscenza dei fatti prevale su quello individuale all'oblio sui medesimi.

[398] Cass. civ., Sez. un., 22 luglio 2019, n. 19681, in *Giust. civ.*, 2019, p. 1 ss., con nota di G. FINOCCHIARO, *Le S.U: sul diritto all'oblio*; in *Corriere giur*., 2019, p. 1195 ss., con nota di V. CUFFARO, *Una decisione assennata sul diritto all'oblio*; in *Foro it.*, 2019, c. 3071 ss. e in *Danno e resp.*, 2019, p. 604 ss., con nota di R. PARDOLESI, *Oblio e anonimato storiografico: usque tandem...?*.

Cfr. anche la relativa ordinanza di rimessione: Cass. civ., 5 novembre 2018, n. 28084, in *Giustiziacivile.com*, 2019, con nota di G. FINOCCHIARO, *Diritto all'oblio e dovere di cronaca: una nuova luce su un problema antico*; in *Corriere giur.*, 2019, p. 5 ss. e con nota di F. DI CIOMMO, *Oblio e cronaca: rimessa alle Sezioni Unite la definizione dei criteri di bilanciamento*, in *Foro it.*, 2019, c. 235 ss.

rivestiva un interesse pubblico - egli non sta esercitando il diritto di cronaca quanto il diritto alla rievocazione storica e storiografica di quei fatti.

Lo stesso termine diritto di cronaca infatti, traendo la propria etimologia dalla parola greca *chronos*, non può che indicare un diritto avente ad oggetto il racconto, con la stampa o altri mezzi di diffusione, di qualcosa che attiene a quel tempo ed è perciò collegato con un determinato contesto.

Ciò non esclude naturalmente che, in relazione a un evento del passato, possano intervenire elementi nuovi tali per cui la notizia ritorni di attualità, di modo che diffonderla, nel momento presente, rappresenti ancora una manifestazione del diritto di cronaca.

In assenza di questi elementi, però, tornare a diffondere la notizia del passato, anche se di sicura importanza, costituisce un'esplicazione di un'attività storiografica che non può godere della stessa garanzia costituzionale che è prevista per il diritto in cronaca.

Hanno precisato ancora le Sezioni unite che l'attività storiografica, intesa appunto quale rievocazione di fatti ed eventi che hanno segnato la vita di una collettività, fa parte della storia di un popolo, ne rappresenta l'anima ed è perciò attività preziosa.

Ma proprio perché essa storia non può essere considerata cronaca.

Ne deriva che una simile rievocazione, a meno che non riguardi personaggi che hanno rivestito e rivestono tuttora un ruolo pubblico, ovvero fatti che per il loro stesso concreto svolgersi implicano il richiamo necessario a nomi dei protagonisti, deve avvenire in forma anonima, perché nessuna particolare utilità può trarre chi fruisce di quelle informazioni dalla circostanza che siano individuati in modo preciso coloro i quali tali atti hanno compiuto[399].

Il *discrimen* storia - cronaca reca con sé la pregnante conseguenza che l'attività rievocativa debba svolgersi in forma anonima, non restando legata alla precisa individuazione di chi si rese autore gli atti rievocati, salvo che questi non ricoprisse ruoli pubblici (nel passato o nel presente).

Una simile attività, cioè, secondo il piano argomentare della Corte, pur restando preziosa per la vita della collettività, occorre si svolga preservando i protagonisti da una nuova attenzione mediatica, dunque evitando di svelarne l'identità.

In altre parole, l'interesse alla conoscenza di un fatto, che costituisce manifestazione del diritto a informare e ad essere informati e che rappresenta la spinta ideale che muove ogni ricostruzione storica, non necessariamente implica la sussistenza di un analogo interesse alla conoscenza dell'identità della singola persona che quel fatto ha compiuto.

---

[399] R. GIOVAGNOLI, *Il diritto all'oblio*, in ID., in *Manuale di Diritto civile*, p. 49 ss.

Le Sezioni unite hanno ulteriormente evidenziato che la decisione di un quotidiano, di un settimanale o comunque di una testata giornalistica di procedere alla rievocazione storica di fatti ritenuti importanti in un determinato contesto sociale e territoriale non può essere sindacata in termini di opportunità.

La scelta di una linea editoriale o piuttosto di un'altra rappresenta infatti una delle forme in cui si manifesta la libertà di stampa e di informazione tutelata dalla Costituzione; per cui non può essere sindacata la decisione di pubblicare con cadenza settimanale, nell'arco di un certo periodo di tempo, la ricostruzione storica della serie di fatti criminosi che hanno coinvolto e impressionato in modo particolare la vita di una collettività in determinato periodo.

Ciò che al contrario può e deve essere verificato dal giudice di merito è se, essendo pacifico il diritto alla ripubblicazione di una certa notizia, sussista o meno l' interesse qualificato a che essa venga diffusa con riferimenti precisi alla persona che di quella vicenda fu protagonista in un passato più o meno remoto; perché l'identificazione personale, che rivestiva un sicuro interesse pubblico nel momento in cui il fatto avvenne, potrebbe divenire irrilevante per i destinatari dell'informazione una volta che il tempo sia trascorso e che i fatti, anche se gravi, si siano sbiaditi nella memoria collettiva.

Il che significa che il diritto a informare, che sussiste anche rispetto a fatti molto lontani, non equivale in automatico al diritto alla nuova e ripetuta diffusione dei dati personali.

Secondo la sentenza è questo il costante *file rouge* che tiene unita la giurisprudenza nazionale ed europea richiamata in precedenza.

D'altra parte, è questo il senso dell'affermazione, più volte rintracciabile nella citata giurisprudenza, secondo cui il trascorrere del tempo modifica l'esito del bilanciamento tra i contrapposti diritti e porta il protagonista di un fatto come quello di cui oggi si discute - che nessun diritto alla riservatezza avrebbe potuto opporre nel momento in cui il fatto avvenne - a riappropriarsi della propria storia personale.

In conclusione, le Sezioni unite, ribadita la rilevanza costituzionale sia del diritto di cronaca che del diritto all'oblio, hanno però chiarito che quando una notizia del passato, a suo tempo diffusa nel legittimo esercizio del diritto di cronaca, venga ad essere nuovamente diffusa a distanza di un lasso di tempo significativo, sulla base di una libera scelta editoriale, l'attività svolta dal giornalista riveste un carattere storiografico.

Pertanto, il diritto dell'interessato al mantenimento dell'anonimato sulla sua identità personale è prevalente, a meno che non sussista un rinnovato interesse pubblico ai fatti ovvero il protagonista abbia ricoperto o ricopra una funzione che lo renda pubblicamente noto.

Giova non da ultimo evidenziare, come accade nella sentenza, che tali principi si trovino predicati nell'art. 3, Testo Unico dei doveri del giornalista, approvato il 27 gennaio 2016.
Nel primo comma si legge infatti che "il giornalista rispetta il diritto all'identità personale ed evita di fare riferimento a particolari relativi al passato, salvo quando essi risultino essenziali per la completezza dell'informazione".
Nei successivi commi (2° e 3°) si afferma ancora che il giornalista "nel diffondere a distanza di tempo identificativi del condannato, valuta anche l'incidenza della pubblicazione sul percorso di reinserimento sociale dell'interessato e sulla famiglia".
Tali asserzioni rappresentano ulteriore riscontro di una tutela che pur assicurata al diritto all'informazione, non trascura di mediarne l'esercizio con gli interessi personali di chi può patirne pregiudizi più o meno gravi.
La prima Sezione della Corte di Cassazione nel marzo 2020 ha ribadito alcuni principi, tornando a pronunciarsi sul diritto all'oblio e analizzandolo in rapporto al coordinamento tra storiografica on line e cronaca giudiziaria[400].
Più nel dettaglio, la presenza nell'archivio storico on line di un quotidiano, di articoli di cronaca giudiziaria pubblicati anni prima nell'edizione cartacea dello stesso giornale, riguardanti fatti penalmente rilevanti riferiti all'attività imprenditoriale di un primario centro di imputazione di interessi economici rilevanti per la collettività, facente capo ad una persona nelle more deceduta, è giustificata dalla permanenza dell'interesse della collettività, ed in particolare del mondo economico, di "fare memoria" di tali vicende, se l'editore ha provveduto alla "deindicizzazione" ed allo spontaneo aggiornamento degli articoli in questione, trattandosi di una soluzione idonea a bilanciare i contrapposti interessi in gioco, che pur consentendo la conservazione del dato personale pubblicato, lo rende però accessibile non più tramite gli usuali motori di ricerca presenti nella Rete, bensì, esclusivamente dall'archivio storico dello stesso quotidiano, in tale modo, garantendo altresì la totale sovrapponibilità, altrimenti irrimediabilmente compromessa, fra l'archivio cartaceo e quello informatico del medesimo giornale, funzionale al diritto della collettività ad essere informata correttamente sulle relative vicende.
Nel maggio 2020 la Corte di cassazione con un importante arresto torna ancora sul tema dell'oblio, riferendosi alla permanenza in rete di una notizia appartenente al passato *sine die*, anche in considerazione dell'eventuale passaggio all'archivio on line della testata giornalistica[401].

[400] Cass. civ., Sez. I, 27 marzo 2020, n. 7559, in *Giustiziacivile.com*, 2020, con nota di A. VITO.
[401] Cass. civ., Sez. I, 19 maggio 2020, n. 9147, in *Giur. it*., 2021, p. 1329 ss.

Il diritto all'oblio consiste nel non rimanere esposti senza limiti di tempo ad una rappresentazione non più attuale della propria persona con pregiudizio alla reputazione ed alla riservatezza, a causa della ripubblicazione, a distanza di un importante intervallo temporale, di una notizia relativa a fatti del passato.

Tuttavia, la tutela del menzionato diritto va posta in bilanciamento con l'interesse pubblico alla conoscenza del fatto, espressione del diritto di manifestazione del pensiero e quindi di cronaca e di conservazione della notizia per finalità storico-sociale e documentaristica, sicché nel caso di notizia pubblicata sul web, il medesimo può trovare soddisfazione anche nella sola deindicizzazione dell'articolo dai motori di ricerca.

Proprio in tema di obbligo di deindicizzazione dei motori di ricerca si è recentissimamente espressa la Corte di cassazione, con ordinanza del 21 luglio 2021, n. 20861[402].

Ai fini della determinazione del *petitum* mediato, la domanda di deindicizzazione esige la precisa individuazione dei risultati della ricerca che l'attore intende rimuovere, e quindi, normalmente, l'indicazione degli indirizzi telematici, o URL, dei contenuti rilevanti a tal fine, anche se non è escluso che una puntuale rappresentazione delle singole informazioni che sono associate alle parole chiave possa rivelarsi, secondo le circostanze, idonea a dare precisa contezza della cosa oggetto della domanda, in modo da consentire al convenuto, gestore del motore di ricerca, di apprestare adeguate e puntuali difese sul punto

Pur non arrivando a pronunciandosi sul primo mezzo di ricorso con cui la ricorrente denunciava la

violazione e falsa applicazione dell'art. 15, Dir. 2000/31/CE e del corrispondente art. 17, D.lgs. n. 70 del 2003 per avere il giudice del merito disposto un'inibitoria generica che comporta in capo a Google, quale Internet service provider, un obbligo di ricerca attiva o di monitoraggio dei contenuti, con tale pronuncia la Suprema Corte ha cassato una sentenza del Tribunale di Spoleto che aveva accertato il diritto all'oblio per i fatti oggetto di causa e per l'effetto ordinava a Google la rimozione e cancellazione dal motore di ricerca di tutti i risultati che apparivano digitando il nome dell'attore.

Richiamata la sentenza n. 7708/2019 in tema di violazione di diritti autorali, e partendo dall'assunto che l'obbligo di intervento dell'Internet service provider presuppone, comunque, in entrambe le ipotesi (sia nel caso di violazione dei diritti di privativa che nel caso in cui venga in questione il trattamento dei dati personali), la precisa conoscenza, da parte dello stesso prestatore di servizi, dei contenuti passibili di rimozione", la Cassazione

[402] R. SETTIMIO, *Nota a Cassazione civile 21 luglio 2021, n.20861,* in *Giustiziacivile.com*, 2021, p. 876 ss.

ha ritenuto non sufficientemente determinata la domanda attorea spiegata nell'atto di citazione, limitata per l'appunto ad una richiesta di rimozione di "tutti i risultati che appaiono in seguito alla digitazione delle parole 'Don B.R.".

Pur ribadendo che resta affidato al giudice del merito l'accertamento in fatto se, in riferimento al profilo tecnico-informatico, l'identificazione di contenuti (nella specie fonogrammi) diffusi in violazione dell'altrui diritto, sia possibile mediante l'indicazione del solo nome o titolo (della trasmissione, in quel caso) da cui sono tratti, oppure sia indispensabile, a tal fine, la comunicazione dell'indirizzo URL, alla stregua delle condizioni esistenti all'epoca dei fatti, sul punto la Corte ha precisato che, seppure sia da ritenere che nello specifico tema della deindicizzazione gli URL rappresentino, di regola, lo strumento più idoneo ai fini dell'individuazione del *petitum* mediato della domanda.

Non può però escludersi che, perlomeno in alcune circostanze, in assenza dei detti URL, i contenuti di cui è domandata in giudizio la rimozione, siano suscettibili di identificazione attraverso il rinvio dell'atto introduttivo alle parole chiave impiegate e ai precisi contenuti cui l'utente ha accesso attraverso i link che appaiono come risultati della ricerca.

Con la citata sentenza è possibile individuare almeno due accezioni di diritto all'oblio:

- la prima è riferita al diritto nato nel mondo "offline", nell'era predigitale come aspetto del diritto alla riservatezza e all'identità personale: in questo ambito, l'oblio si sostanziava nel diritto della persona a non rimanere esposta ai danni relativi alla ripubblicazione non necessaria di una notizia risalente nel tempo, legittimamente pubblicata in passato.
- La seconda si riferisce all'avvento dell'era digitale in cui l'oblio ha trovato nuovo vigore laddove il web vive dell'inserimento costante di dati di qualsiasi natura e provenienza; in questo senso, il diritto all'oblio assume connotati specifici con riferimento ai motori di ricerca rispetto ai quali si parla di diritto alla deindicizzazione e alle questioni concernenti le informazioni presenti in rete.

In relazione alla rimozione dei risultati, la Corte ha sancito che il motore di ricerca è obbligato a eliminare dall'elenco di risultati di una ricerca effettuata, a partire dal nome di una persona, i link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi e anche quando la loro pubblicazione su tali pagine web sia di per sé lecita.

Al riguardo, nel par. 2 dell'art 17 del GDPR si configura la nuova responsabilità del titolare del trattamento che ha reso pubblici i dati personali, ponendosi la questione dell'adozione di

tutte le misure per notiziare i terzi che trattano i dati oggetto della richiesta di cancellazione[403].

La rimozione deve essere totale e definitiva, deve riguardare qualsiasi copia o riproduzione ricorrendo anche alla tecnica dell'anonimizzazione, purché eseguita correttamente. Nell'ambito del diritto all'oblio, in parallelo, si è affermato che i provider debbano intervenire per la rimozione dei risultati che appaiono a seguito di una ricerca effettuata perché tale attività del motore di ricerca presuppone un obbligo di intervento da parte del titolare del trattamento in quanto indicizzare, trovare informazioni e metterle a disposizione degli utenti secondo un certo ordine di preferenza o memorizzarle temporaneamente è a tutti gli effetti un trattamento dei dati personali regolamentato oggi dal GDPR e, pertanto, il gestore del motore di ricerca deve assicurare che le attività sopramenzionate siano svolte nel rispetto di detto Regolamento.

In tema di diritto all'oblio, per la Suprema Corte, per l'obbligo di intervento dell'Internet service provider, viene in rilievo l'art. 14.1, lett. a), della Direttiva 2000/31/CE, secondo cui il prestatore del servizio può essere esonerato da qualsiasi responsabilità per i dati di natura illecita che ha memorizzato solo a condizione di non essere stato "effettivamente al corrente del fatto che l'attività o l'informazione è illecita".

Come è evidenziato dalla Corte di cassazione, l'intervento dell'Internet service provider presuppone la conoscenza specifica dei contenuti passibili di rimozione: vi è la necessità di porre il gestore nella condizione di poter intervenire e di prendere atto della interferenza delle informazioni oggetto della richiesta con i diritti fondamentali della persona e, quindi, anche con il diritto alla riservatezza.

Per tali ragioni, è possibile configurare il diritto all'oblio come espressione peculiare del diritto alla riservatezza e del legittimo interesse di ognuno a non rimanere indeterminatamente esposto ad una rappresentazione non più attuale della propria persona derivante dalla reiterata pubblicazione di notizie, soprattutto mediante la indicizzazione sui motori di ricerca.

Ad oggi, infatti, nel mondo di Internet e dei *social media* è impossibile dimenticare.

Il web ha la capacità di richiamare, attraverso l'inserimento anche di una sola parola, fatti ed eventi verificatisi anni addietro oppure pubblicati su quotidiani che hanno digitalizzato i loro archivi.

---

[403] F. PIZZETTI, *Il prisma del diritto all'oblio*, in ID. (a cura di), *Il caso del diritto all'oblio*, Torino, 2013, p. 62 ss.; L. BOLOGNINI-E. PELINO-C. BISTOLFI, *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p 265 ss.

Essere prigionieri di informazioni del passato può essere un ostacolo per la tutela della persona umana e per la "libera costruzione della personalità" ed ecco perché l'oblio, inteso come diritto della persona, è concretamente rilevante nella società contemporanea.

Dall'analisi della giurisprudenza emerge come la Corte di giustizia e la Corte di cassazione siano intervenute, attraverso il prisma del diritto all'oblio, sul più ampio tema della *governance* della società digitale, offrendo una pronuncia alquanto ambivalente.

Le sentenze più recenti hanno infatti aggiunto un nuovo tassello alla responsabilizzazione delle piattaforme che operano *online*, prendendo atto del loro impatto incisivo e determinante sui diritti fondamentali.

Una scelta che trova nuovi riscontri in ulteriori decisioni assunte dagli stessi ISP, come quella annunciata dal celebre *social network,* Facebook, volta a istituire un organismo, di portata globale e che si autodefinisce indipendente, il quale dovrà pronunciarsi su questioni relative a *hate speech*, *fake news* e conflitto tra libertà di informazione e tutela della privacy, sebbene notevole sia la preoccupazione di alcuni nel lasciare delle mani di privati una così delicata regolamentazione di diritti.

In realtà i soggetti intermediari dovrebbero solo agire in prima battuta, fermo restando sempre il vigile controllo delle autorità giudiziarie, di controllo e garanti, il cui ruolo certamente non verrebbe in alcun modo scalfito.

Si tratta, in definitiva, di questioni di estrema rilevanza, poiché dalla loro risoluzione dipende il modo di intendere la rete come grande spazio globale in cui esercitare le libertà tradizionali e i nuovi diritti digitali della persona.

Tale dimensione di Internet sarà attuabile solo a patto che venga garantita l'effettività dei diritti fondamentali *online*, mediante l'intervento (anche pubblico) a presidio dei principi di legalità e del *due process*.

INDICE DEGLI AUTORI CITATI

AA.VV., *Il diritto all'oblio. Atti del Convegno di Studi del 17 maggio 1997*, a cura di E. Gabrielli, Napoli, 1999.

ABRIANI N., *Le utilizzazioni libere nella società dell'informazione*, in *Annali Italiani del Diritto d'Autore*, Pavia, 2001.

AKDENIZ Y., *Freedom of expression*: *Laurence Godfrey v. Demon Internet Limited*, in *4 Journal of Civil Liberties*, 1999, p. 260 ss.

ALPA G., *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in *Dir. inf.*, 1997, p. 703 ss.

AMMENDOLA M. - UBERTAZZI L. C., *Il diritto d'autore*, Torino, 1993.

ANGELOPOULOS C. - SMET S., *Notice-and-Fair Balance: How to Reach a Compromise between Fundamental Rights in European Intermediary Liability*, in *8 Journal of Media Law*, 2016, p. 266 ss.

ANGELOPOULOS C., *European Intermediary Liability in Copyright: A Tort Based Analysis*, in *Alphen aan den Rijn*, 2017, p. 74 ss.

ANGELOPOULOS C., *Filtering the Internet for Copyrighted Content in Europe*, in *Amsterdam Law School Legal Studies Research Paper No*., 2012, p. 1 ss.

ARNÒ G. - LENSI ORLANDO A., *La tutela della privacy nella rete internet*, Torino, 2002.

ARNÒ G. - Lista G., *Il commercio elettronico alla luce delle recenti iniziative comunitarie*, in *Contratti*, 2000, p. 938 ss.

ASTONE F., *L'enforcement privato in Italia*, in *23 AIDA*, 2014, p. 59 ss.

AULETTA T., *Diritto alla riservatezza e "droit à l'oubli"*, in G. Alpa - M. Bessone - L. Boneschi - G. Caiazza (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983, p. 127 ss.

AUTERI P., *Internet e il contenuto del diritto d'autore*, in *AIDA*, 2006.

BACCIN A., *Responsabilità penale dell'Internet Service Provider e concorso degli algoritmi negli illeciti online: il caso Force V. Facebook*, in *Sistema Penale*, 2020, p.75 ss.

BALKIN J. M., *The Future of Free Expression in a Digital Age*, in *36 Pepp. L. Rev.*, 2009, p. 427 ss.

BALKIN J.M., *Free Speech in a Triangle*, 2018, p. 2011 ss.

BALKIN J.M., *Free Speech in Algorithmic Society: Big Data, Private Governance, and New School Speech Regulations,* in *51 U.C.D. L. Rev.*, 2018, p. 1149 ss.

BALKIN J.M., *Old School/New School Speech Regulation*, in *Faculty Scholarship Series*, paper n. 4877, 2014, p. 2304.

BARBIERATO D., *Osservazioni sul diritto all'oblio e la (mancata) novità del Regolamento Ue 2016/679 sulla protezione dei dati personali*, in *Resp. civ. prev.*, 2017, p. 2100 ss.

BASSOLI E., *Giurisprudenza italiana e comunitaria sulla responsabilità civile del service provider e la sentenza della Corte di Appello di Milano nel caso Yahoo vs. RTI*, in *Contratto e impresa*, 2015, p. 231 ss.

BATTINI S. - PEREZ R. - FRANCHINI C. - VESPERINI G. - CASSESE S., *Manuale di diritto pubblico*, 2002.

BELLAN A., *Piattaforme, obblighi di monitoraggio e risoluzione delle controversie online*, in *Dir. ind.*, 2020, p. 187 ss.

BELLI M., *La responsabilità dei «prestatori di servizi di condivisione di contenuti online» ai sensi della Dir. 2019/790/UE*, in *NLCC*, 2020, p. 556 ss.

BENNIS A., *Realism about Remedies and the Need for a CDA Takedown: A Comparative Analysis of 230 CDA and the U. K. Defamation Act 2013*, in *27 Fla. J. Int'l L.*, 2015, p. 316.

BERTONI A. - MONTAGNANI M. L., *Il ruolo degli intermediari internet tra tutela del diritto d'autore e valorizzazione della creatività in rete*, in *Giurisprudenza commerciale*, 2013.

BIANCHI D., *Facebook: filtraggio globale e specifico dei contenuti equivalenti per il diffamato, in Diritto & Giustizia*, 2019, p. 3 ss.

BIANCHI D., *Internet e il danno alla persona: i casi e le ipotesi risarcitorie*, 2012, p. 367 ss.

BIN M., *Privacy e trattamento dei dati personali*, in *Contr. e impr. /Europa*, 1997, p. 459 ss.

BIN R., *Giudizio in astratto e delega di bilanciamento in concreto*, in *Giur. cost.*, 1991, p. 3574 ss.

BIOCCA A., *Reti digitali*, Milano, 2002.

BOCCHINI R., *Il contratto di accesso ad Internet*, in D. VALENTINO, *Manuale di diritto dell'informatica*, Napoli, 2004.

BOCCHINI R., *La responsabilità civile degli intermediari del commercio elettronico*, Napoli, 2003.

BOCCHINI R., *La responsabilità civile plurisoggettiva, successiva ed eventuale dell'ISP*, in *Giur. it.*, 2019, p. 2609 ss.

BOCCHINI R., *La responsabilità contrattuale ed extracontrattuale telematica*, in D. VALENTINO, *Manuale di diritto dell'informatica*, Napoli, 2004.

BOCCHINI R., *La responsabilità extracontrattuale del provider*, in D.VALENTINO, *Manuale di diritto dell'informatica*, 2013, p. 67 ss.

BOCCHINI R., *La responsabilità extracontrattuale del provider*, in D. VALENTINO (a cura di), *Manuale di diritto dell'informatica*, Napoli, 2016, p. 539.

BOLOGNINI L. - PELINO E. - BISTOLFI C., *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016.

BRAITHWAITE N., *The United Kingdom Defamation Act 1996*, in *15 Comm. Law.*, 1997, p. 12 ss.

BRAUN O., *Internet Publications and Defamation: Why the Single Publication Rule Should Not Apply*, in *Golden Gate U.L. Rev.*, 2002, p. 325 ss.

BRIZZI F., *Diffusione illecita di immagini o video sessualmente espliciti: tra tutela della privacy e revenge porn*, in *Ilpenalista.it*, 2021, p. 876 ss.

BRUGALETTA F., *Internet per giuristi*, 2003.

BUGIOLACCHI L., *Ascesa e declino della figura del provider attivo? Riflessioni in tema di fondamento e limiti del regime privilegiato di responsabilità dell'hosting provider*, in *Resp. civ. prev.*, 2015, p. 1261 ss.

BUGIOLACCHI L., *Evoluzione dei servizi di hosting provider, conseguenze sul regime di responsabilità e limiti all'attuale approccio case by case*, in *Resp. civ. prev.*, 2013, p. 1997 ss.

BUGIOLACCHI L., *I presupposti dell'obbligo di rimozione dei contenuti da parte dell'hosting provider tra interpretazione giurisprudenziale e dettato normativo*, in *Resp. civ. prev.*, 2017, p. 536 ss.

BUGIOLACCHI L., *La responsabilità dell'host provider alla luce del d. legisl. n. 70 del 2003: esegesi di una disciplina "dimezzata"*, in *Resp. civ. prev.*, 2005, p. 188.

BUGIOLACCHI L., *Principi e questioni aperte in materia di responsabilità extracontrattuale dell'Internet provider. Una sintesi di diritto comparato*, in *Dir. inf.*, 2000, p. 836 ss.

BUSNELLI F. D., *Il «trattamento dei dati personali» nella vicenda dei diritti della persona: la tutela risarcitoria*, in V. CUFFARO-V. RICCIUTO-V. ZENO ZENCOVICH, *Trattamento dei dati e tutela della persona*, Milano, 1998, p. 177 ss.

BUSNELLI F.D., *Nuove frontiere della responsabilità civile*, in *Jus Civile*, 1976, p. 41 ss.

BUSNELLI F.D., *Spunti per un inquadramento sistematico*, in AA.VV., *Tutela della privacy. Commentario alla L. 31 dicembre 1996, n. 675*, a cura di C. M. Bianca e F. D. Busnelli, in *Nuove leggi civ. comm.*, 1999, p. 229 ss.

BUTTARELLI G., *Banche dati e tutela della riservatezza*, Milano, 1997.

CAFAGGI F., *Profili di relazionalità della colpa. Contributo ad una teoria della responsabilità extracontrattuale*, Padova, 2006.

CAJANI F., *Alla ricerca del log (perduto)*, in *Diritto dell'Internet*, 2006.

CALETTI G. M., *Libertà e riservatezza sessuale all'epoca di Internet. L'art. 612-ter c.p. e l'incriminazione della pornografia non consensuale*, in *Rivista Italiana di Diritto e Procedura Penale*, 2019, p. 2044 ss.

CALOGERO A., *Streaming on line e tutela del diritto d'autore*, 2011.

CAMARDI C., *Inibitorie amministrative di inibitorie*, in *AIDA*, 2012, p. 874 ss.

CAMILLETTI F., *La responsabilità civile del provider*, in *Nomi di dominio, marchi e copyright*, Milano, 2005.

CAMMARATA M., *Il codice deontologico per gli Internet provider: quali obblighi e quali garanzie?*, 1996, in *www.interlex.it.*

CAMMARATA M., *Il minimo danno possibile con la maggiore utilità?*, 1994, in *www.interlex.it.*

CAMMARATA M., *Internet, diritto e politica, non c'è da stare allegri*, 1998, in *www.interlex.it.*

CAMMARATA M., *Le trappole nei contratti di hosting*, 2003, in *www.interlex.it.*

CAMMARATA M., *Passaggi impegnativi per gli internet provider*, 2002, in *www.interlex.it.*

CAMMARATA M., *Sotto torchio gli operatori della Rete*, 2003, in *www.interlex.it.*

CAMMARATA M., *Troppe norme, occorre un testo unico*, 2003, in *www.interlex.it.*

CAPITANT H., *La responsabilité du fait des choses inanimées après l'arrêt des Chambres réunies du 13 févr. 1930*, in *Dalloz Hebd*, 1930, p. 29 ss.

CAPRIOLI A., *Responsabilité du fournisseur d'hébergement*, in *Droit & Patrimoine*, 1999, p. 107 ss.

CARAPELLA M.D. - CASSANO G., *Il danno da informazione a mezzo reti telematiche*, 2000.

CARBONE P. e ZANOVELLO F., *La responsabilità dell'Internet Service Provider. Brevi note a Cass. 19 marzo 2019, nn. 7708 e 7709*, in *Studium Iuris*, 2020, p. 563 ss.

CARUSI D., *La responsabilità*, in V. CUFFARO-V. RICCIUTO, *Il trattamento dei dati personali*, Torino, 1999, p. 356 ss.

CARUSO C., *Teoria e ideologia della libertà di espressione. La giurisprudenza della Corte Suprema degli Stati Uniti sulla freedom of speech*, in *Forum di Quaderni Costituzionali Rassegna*, 2013, p. 1 ss.

CASSANO G. - CIMINO I., *Il nuovo regime di responsabilità dei providers: verso la creazione di un novello "censore telematico"*, in *Contratti*, 2004, p. 90 ss.

CASSANO G. - BUFFA F., *Responsabilità del content provider e dell'host provider*, in *Corriere giur.*, 2003, p. 987 ss.

CASSANO G. - CIMINO I., *Il nuovo regime di responsabilità del provider: verso la creazione di un novello "censore telematico"*, in *Contratti*, 2004, p. 88 ss.

CASSANO G. - VACIAGO G. - SCORZA G., *Diritto dell'internet. Manuale operativo: casi, legislazione, Giurisprudenza*, 2012.

CASSANO G., *Caso Break: confermata in appello la responsabilità del provider*, in *Il Diritto industriale*, 2018, p. 182 ss.

CASSANO G., *Competenza territoriale per la diffamazione commessa attraverso internet*, in *Dir. inf.*, 2001, p. 251 ss.

CASSANO G., *Il diritto dell'Internet*, Milano, 2005.

CASSANO G., *Vita Notarile*, 2019, p. 557 ss.

CASTRONOVO C., *La nuova responsabilità civile*, 2006, p. 271 ss.

CASTRONOVO C., *Le frontiere nobili della responsabilità civile*, in *Riv. crit. dir. priv.*,1989, p. 567 ss.

CASTRONOVO C., *Responsabilità civile*, Milano, 2018.

CASTRONOVO C., *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, in *Eur. dir. priv.*, 1998, p. 653 ss.

CHIARIELLO C., *Il valore costituzionale della Carta di Nizza: un problema ancora aperto anche alla luce della sentenza n. 269/2017 della Corte costituzionale*, in *Consulta Online*, 2018, p. 381 ss.

CIMINO P., *Il nuove regime della responsabilità dei provider: verso la creazione di un nuovo censore telematico*, in *Contratti*, 2004.

CITARELLA G., *Aggiornamento degli archivi online, tra diritto all'oblio e rettifica "atipica"*, in *Resp. civ. prev.*, 2012, p. 1155 ss.

CITRON D. K. - WITTES B., *The Internet Will not Break: Denying Bad Samaritans "Sect" 230 Immunity*, in *86 Fordham L. Rev.*, 2017, p. 401 ss.

CITRON D.K., *Extremist Speech and Compelled Conformity*, in *93 Notre Dame Law Review*, 2018, p. 1035 ss.

CLARIZIA R., *Legge 675/96 e responsabilità civile*, in *Dir. inf.*, 1998, p. 235 ss.

COCCO G., *Il concetto di pornografia minorile e i principi del diritto penale liberale*, in *Resp. civ. prev*., 2010, p. 2073 ss.

COMANDÈ G. - SICA S., *Il commercio elettronico*, Torino, 2004.

COMANDÈ G., *Al via l'attuazione della direttiva sul commercio elettronico, ma…serve un maggior coordinamento*, in *Danno e resp.*, 2003, p. 811 ss.

COMANDÈ G., *Danni cagionati per effetto del trattamento dei dati personali*, in F.D. BUSNELLI- C.M. BIANCA, *Tutela della privacy*, in *Nuove leggi civ. comm.*, 1999, p. 482 ss.

COMANDÉ G., *Persona e tutele giuridiche*, Torino, 2004.

CORTI M., *In tema di diffamazione a mezzo Internet*, in *AIDA*, 2001, p. 476 ss.

COSTANTINESCO L. J., *Il metodo comparativo*, Torino, 2000.

COSTANZO P., *Aspetti evolutivi del regime giuridico di Internet*, in *Dir. inf.*, 1996, p. 831 ss.

COSTANZO P., *I newsgroups al vaglio dell'Autorità giudiziaria (ancora a proposito della responsabilità degli attori d'Internet)*, in *Dir. inf.*, 1998, p. 807 ss.

COSTANZO P., *La governance di Internet in Italia*, in *Internet: regole e tutela dei diritti fondamentali*, a cura di O. Pollicino, E. Bertolini, V. Lubello, 2013, p. 41 ss.

COSTANZO P., *Le nuove forme di comunicazione in rete: Internet*, in *Inform. e dir*., 1997, p. 678 ss.

COSTANZO P., *Osservazioni sparse su nodi, legami e regole su Internet*, in *Nodi virtuali, legami informali: Internet alla ricerca di regole*, a cura di P. Passaglia e D. Poletti, 2017, p. 17 ss.

COSTANZO P., *Quali garanzie costituzionali per gli interventi rimediali in rete*, in *Dir. inf.*, 2013, p. 17 ss.

CUFFARO V., *Una decisione assennata sul diritto all'oblio*, in *Foro it.*, 2019, c. 3071 ss.

CUOMO L. - RAZZANTE R., *"La disciplina dei reati informatici"*, Torino, 2009.

CUOMO L., *La Cassazione affonda la Baia dei Pirati*, in *Cass. Pen.*, 2011, p. 395 ss.

D'ARRIGO R., *La responsabilità degli intermediari nella nuova disciplina del commercio elettronico*, in *Danno e resp.*, 2004, p. 912 ss.

DALIA G., *I reati informatici: dalla legge n. 547 del 1993 alla legge n.48 del 2008*, in D. VALENTINO, *Manuel di diritto dell'informatica*, 2015, p. 65 ss.

DE ANGELIS D., *La tutela giuridica delle opere musicali digitali*, Milano, 2005.

DE BEER J.-CLEMMER D.C., *Global Trends in Online Copyright Enforcement: a Non-Neutral Role for Network Intermediaries?*, in *49 Jurimetrics*, 2009, p. 396 ss.

DE CATA M., *La responsabilità civile dell'internet service provider*, Milano, 2010.

DE GRAZIA L., *La libertà di stampa e il diritto all'oblio nei casi di diffusione di articoli attraverso Internet: argomenti comparativi*, in *Riv. dell'Assoc. Italiana dei cost.*, 2013, p. 4 ss.

DE LUCA N. - TUCCI E., *Il caso Google/Vivi Down e la responsabilità dell'Internet Service Provider. Una materia che esige chiarezza*, in *Giur. comm*., 2011, p. 1215.

DE LUCIA L. E GUZZI F.F., *L'incerta natura giuridica dei procedimento amministrativi a tutela del diritto d'autore online (Regolamento AGCOM n. 680/13/CONS)*, in *AIDA*, 2014, p. 136 ss.

DELFINI F., *La responsabilità dei prestatori intermediari nella Direttiva 2000/31/CE e nel D.lgs. 70/03*, in *Riv. dir. priv.*, 2004, p. 84 ss.

DI CIOMMO F. - PARDOLESI R., *Dal diritto all'oblio in Internet alla tutela della identità dinamica. È la rete, bellezza!*, in *Danno e resp.*, 2012, p. 701 ss.

DI CIOMMO F., *Diritti della personalità tra media tradizionali e avvento di internet*, in *Persone e tutele giuridiche*, Torino, 2003.

DI CIOMMO F., *Internet, diritti della personalità e responsabilità aquiliana del provider*, in *Danno e resp*., 1999, p. 756 ss.

DI CIOMMO F., *La responsabilità civile nell'era di Internet*, in G. PONZANELLI, *La responsabilità civile*, Padova, 2002, p. 179 ss.

DI CIOMMO F., *Oblio e cronaca: rimessa alle Sezioni Unite la definizione dei criteri di bilanciamento*, in *Foro it.*, 2019, c. 235 ss.

DI CIOMMO F., *Oltre la direttiva 2000/31/Cee, o forse no. La responsabilità del provider di Internet nell'incerta giurisprudenza europea*, in *Foro it*., 2019, c. 2045 ss.

DI CIOMMO F., *Privacy in Europe After Regulation (EU) No 2016/679: What Will Remain of the Right to Be Forgotten?*, in *The Italian Law Journal*, 2017, p. 24 ss.

DI CIOMMO F., *Quello che il diritto non dice. Internet e oblio*, in *Danno e resp*., 2014, p. 1101 ss.

DI CIOMMO F., voce *Internet (responsabilità civile)*, in *Enc. Giur. Treccani*, 2002, p. 340 ss.

DI GIOVANNI F., *Gli intermediari dell'e-commerce*, in *Commercio elettronico e categorie civilistiche*, Milano, 2002.

DI MAJO A., *La responsabilità del provider tra prevenzione e rimozione*, in *Corriere giur*., 2012, p. 553 ss.

DI MAJO A., *La tutela civile dei diritti*, Milano, 2003.

DÖRR D. - JANICH S., *The Criminal Responsability of Interbet service Providers in Germany, 80 Miss. L. J.*, 2011, p. 1247 ss.

ENGSTROM E.-FEAMSTER N., *The Limits of Filtering: A Look at the Functionality & Shortcomings of Content Detection Tools*, 2017, p. 13, in *https://www.engine.is/the-limits-of-filtering.*

FABIANO P.-GORGONI S., *Disintermediazione e nuovi media. Come cambia la comunicazione*, Roma, 2017.

FACCI G., *La responsabilità dei Providers*, in C. ROSSELLO, *Il Commercio elettronico*, Torino, 2002.

FACCI G., *La responsabilità del provider*, in C. ROSSELLO, G. FINOCCHIARO, G. TOSI (a cura di), *Commercio elettronico. Documento informatico, Firma digitale. La nuova disciplina*, 2003, p. 131 ss.

FACCI G., *La responsabilità extracontrattuale dell'internet provider*, in *Resp. civ. prev*., 2002, p. 265 ss.

FALLETTA P., *La responsabilità degli internet service provider*, in *Il diritto del web. Casi e materiali*, 2015.

FEROLA L., *Dal diritto all'oblio al diritto alla memoria sul Web. L'esperienza applicativa italiana*, in *Dir. inf.*, 2012, p. 1001 ss.

FERRETTI A., *Diritto d'autore*, Napoli, 201.

FERRI G.B., *Diritto all'informazione e diritto all'oblio*, in *Riv. dir. civ*., 1990, p. 801 ss.

FINOCCHIARO G., *Diritto all'oblio e dovere di cronaca: una nuova luce su un problema antico*, in *Corriere giur*., 2019, p. 5 ss.

FINOCCHIARO G., *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Corriere giur*., 2020, p. 591 ss.

FINOCCHIARO G., *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm*., 2017, p. 6 ss.

FINOCCHIARO G., *L'identità personale su Internet*, in *Danno e resp.*, 2012, p. 388 ss.

FINOCCHIARO G., *Le S.U: sul diritto all'oblio*, in *Corriere giur*., 2019, p. 1195 ss.

FLETCHER G.P., *Fairness and Utility in Tort Theory*, in *84 Harv. L. Rev*., 1972, p. 537 ss.

FRANCESCHELLI V., *Convergenza*, in *Diritto delle nuove tecnologie*, Milano, 2009.

FRANCESCHELLI V., *La tutela della privacy informatica*, Milano, 1998.

FRANZONI M., *Colpa presunta e responsabilità del debitore*, Padova, 1988, p. 172 ss.

FRANZONI M., *Dati personali e responsabilità civile*, in *Resp. civ. prev.*,1998, p. 902 ss.

FRANZONI M., *Gli illeciti in Internet*, in *Resp. civ. prev*., 2002, p. 23 ss.

FRANZONI M., *Il danno da attività pericolose nella giurisprudenza*, in *Contr. e impr.*, 1985, p. 155 ss.

FRANZONI M., *La responsabilità del provider*, in *Ann.it. dir. autore*, 1997, p. 250 ss.

FREIWALD S., *Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for defamation*, 2001.

FRIED F., *Perfect freedom or perfect control*, in *Harvard Law Review*, 2002.

FROSINI T.E., *Costituzionalismo 2.0*, in *Rassegna Parlamentare*, 2016, p. 691 ss.

FROSINI T.E., *L'accesso a Internet come diritto fondamentale*, in *Internet: regole e tutela dei diritti fondamentali*, a cura di O. Pollicino, E. Bertolini, V. Lubello, 2013, p. 69 ss.

GABRIELLI E. (a cura di), *Il diritto all'oblio. Atti del convegno di studi del 17 maggio 1997*, Napoli, 1999.

GALGANO F., *Le mobili frontiere del danno ingiusto*, in *Contr. e impr*., 1985, p. 198 ss.

GAMBARO A., *Falsa luce agli occhi del pubblico, False Lights in the Public Eyes*, in *Riv. dir. civ.*, 1981, p. 84 ss.

GAMBARO A., *Falsa luce agli occhi del pubblico*, in *Quadr*., 1998, p. 301 ss.

GAMBINI M.L., *La responsabilità civile dell'Internet service provider*, Napoli, 2006.

GAMBINI M.L., *La responsabilità dell'Internet service provider approda al vaglio della Cassazione*, in *Corriere giur.*, 2020, p. 195 ss.

GAMBINI M. L., *La responsabilità civile telematica*, in C. PERLINGIERI e L. RUGGIERI (a cura di), *Internet e diritto civile*, 2015 p. 313 ss.

GATTEI C., *Considerazioni sulla responsabilità dell'Internet provider*, 1998, in *www.interlex.it.*

GATTEI C., *La responsabilità dell'Internet provider. Analisi di diritto comparato*, in CASSANO G., *Il diritto delle nuove tecnologie informatiche e dell'Internet*, Milano, 2002.

GHIDINI G., *Della concorrenza sleale*, in *Il Codice civile. Commentario*, diretto da P. SCHLESINGER, Milano, 1991, p. 186 ss.

GIACOBBE G., *La responsabilità civile per l'uso di internet*, in *Il contratto telematico, Trattato di diritto pubblico dell'economia*, Padova, 2002.

GIANNANTONIO E., *Responsabilità civile e trattamento dei dati personali*, in *Dir. inf*., 1999, p. 1035 ss.

GIANNITI P., *La "comunitarizzazione" della "Carta" a seguito del Trattato di Lisbona*, *in* ID. (a cura di), *I diritti fondamentali nell'Unione europea. La Carta di Nizza dopo il Trattato di Lisbona*, Bologna, 2013, p. 357 ss.

GIANNONE CODIGLIONE G., *Indirizzo IP, reti wi-fi e responsabilità per illeciti commessi da terzi*, in *Dir. inf*., 2013 p. 107 ss.

GIANNONE CODIGLIONE G., *La nuova legge tedesca per l'enforcement dei diritti sui social media*, in *Dir. inf.*, 2017, p. 728 ss.

GIANNONE CODIGLIONE G., *Motori di ricerca, trattamento di dati personali ed obbligo di rimozione: diritto all'oblio o all'autodeterminazione informativa*, in *Nuova giur. civ. comm.*, 2014, p. 1054 ss.

GIOVAGNOLI R., *Il diritto all'oblio*, in ID., in *Manuale di Diritto civile*, 2019, p. 37 ss.

GIOVAGNOLI R., *Il nuovo regolamento europeo sulla protezione dei dati personali*, in ID., *Manuale di Diritto civile*, 2019, p. 55 ss.

GIULIANI F. M., *Tecniche di commercio elettronico e nozione stabile di organizzazione*, in *Contr. impres.*, 2003, p. 985 ss.

GODWIN G., *Internet libel: is the provider responsible?*, in *www.eff.or.*

GOLDBERG E., *Free Speech consequentialism*, in *116 Colum. L. Rev.*, 2016, p. 687.

GOLDMAN E., *Online User Account Termination and 47 U.S.C.*, in *2 U.C. Irvine L. Rev.*, 2012, p. 659 ss.

GOUNALAKIS G. - RHODE L., *Haftung des Host-Providers: ein neues Fehlurteil aus München?*, in *NJW*, 2000, p. 2168 ss.

GRIMALDI L., *Diritto alla deindicizzazione: dati sensibili, potere e responsabilità - Google France*, in *Dir. inf.*, 2020, p. 265 ss.

HARDOUIN R., *L'hébergeur et la publicité: la neutralité comme condition d'une coexistence*, *RLDI* 2010/62, p. 47 ss.

HARDOUIN R., *La jurisprudence, les textes, et la responsabilité des hébergeurs*, 2008.

HELBERGER N.-PIERSON J.-POELL T., *Governing online platforms: From contested to cooperative responsability*, in *34 The Information Society*, 2018, p. 1 ss.

HELMAN L.-PARCHOMOVSKY G., *The Best Available Technology Standard*, in *111 Colum. L. Rev.*, 2011, p. 1194 ss.

HOEREN T.-PICHLER R., *Zivilrechtliche Haftungim Online-Bereich*, in U. LOEWENHEI-F.A. KOCH, *Praxis des Online-Rechts*, Weinheim,1997, p. 107 ss.

HOEREN T., *Ist Somm ein Krimineller?*, in *NJW*, 1998, p. 2792 ss.

HOEREN T., *Liability in the internet and the new German multimedia regulations*, in *Autern & Media*, 2008.

HUSOVEC M., *Injuctions Against Intermediaries in the European Union. Accountable But Not Liable*, Cambridge University Press, 2017.

IASELLI M., *I contorni della responsabilità dell'hosting provider attivo*, in *Dir. ind.*, 2019, p. 399 ss.

IRTI N., *Norma e luoghi. Problemi di geo-diritto*, Bari, 2002.

IULIANI A., *Note minime in tema di trattamento dei dati personali*, in *Europa e Diritto Privato*, 2018, p. 293 ss.

JESSERAND C., *Régime français de la responsabilité des intermédiaires technique*, in *25 Les Cahiers de propriété intellectuelle*, 2013, p. 1135 ss.

JOSSERAND L., *La responsabilité du fait des automobiles devant les Chambres réunies de la Cour de Cassation*, in *Dalloz Hebd.*, 1930, *Chron.*, p. 25 ss.

KAMDAR A., *CDA 230: The Most Important Law Protecting Internet Speech*, in *Electronic Frontier Found*, 2012, in *www.eff.org*.

KATYAL S.K.-SCHULTZ J. M, *The Unending Search for the Optimal Infringement Filter*, in *112 Colum. L. Rev. Sidebar*, 2012, p. 83 ss.

KIDNER R., *Casebook on Torts*, Oxford, 2012, p. 352 ss.

KLEINDSCHMIDT B., *An International Comparison of ISP's Liabilities for Unlawful Third Party Content*, in *18 Int'l J.L. & Info.Tech*, 2010, p. 332 ss.

KLONICK K., *The New Governors: The People, Rules and Processes Governing Online Speech*, in *131 Harv. L. Rev.*, 2018, p. 1598 ss.

KOCH F.A., *Zivilrechtliche Anbienterhaftung fùr Inhalte in Komminikationetzen*, in *Computer und Recht*, 1997, p. 193 ss.

KOREN E., *Fair Use by Design*, in *64 UCLA Law Review*, 2017, p. 1082 ss.

KÜHNE H., *Strafbarkeit der Zugangsvermittlung von pornographischen Informationen im Internet*, in *NJW*, 1999, p. 188 ss.

LAGHEZZA P., *Il diritto all'oblio esiste (e si vede)*, in *Foro it.*, 1998, c. 1835 ss.

LAVI M., *Content Providers' Secondary liability: A Social Network Perspective*, in *26 Fordham Intell. Prop. Media&Ent. L.J.*, 2016, p. 855 ss.

LIBERTINI M., *Le nuove frontiere del danno risarcibile*, in *Contr. e impr.*, 1987, p. 85 ss.

LONGHINI L., *Internet nella giurisprudenza*, Milano, 2003.

LUPARIA L., *Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, 2012.

LYON CAEN G., *Nota a Trib. gr. inst. Seine, 4 ottobre 1965, n. 14482*, in *Semaine Juridique*, 1966, p. 284 ss.

MAESKE B., *Ermittlungen im Internet. Positionen und Dissonanzen: Rechtliche Konfliktpunkte bei der Bekämpfung von Kriminalität im Internet*, in *Kriminalistik*, 2000, p. 245 ss.

MAGGI M., *Gli illeciti per violazione dei diritti d'autore e connessi in internet*, in *Il regolamento AGCOM sul diritto d'autore*, Torino, 2014.

MANES V., *Metodo e limiti dell'interpretazione conforme alle fonti sovranazionali in materia penale*, in *Arch. Pen.*, 2012, p. 36 ss.

MANGANO F., *Diritto all'oblio*, in *Giur. merito*, 2012, p. 2621 ss.

MANNA A., *Considerazioni in tema di responsabilità penale dell'internet provider in tema di pedofilia*, in *Dir. inf.*, 2001, p. 2 ss.

MARCHETTI G., *Diritto di cronaca on-line e tutela del diritto all'oblio*, in AA.VV., *Da Internet ai social network, Sant'Arcangelo di Romagna*, 2013, p. 71 ss.

MARINI L., *Profili giuridici del commercio elettronico*, in *Dir. comm. Int.*, 2000, p. 329 ss.

MARTIN J. A.-FARGO A.L., *Anonymity as a Legal Right: Where and Why It Matters*, in *16 N.C. J. L. & Tech.*, 2015, p. 311 ss.

MAZZAMUTO S., *L'autonomia negoziale e le situazioni giuridiche soggettive*, in *Manuale di Diritto privato*, a cura di S. Mazzamuto, Torino, 2017, p. 108 ss.

MENSI M. - FALLETTA P., *Il diritto del web. Casi e materiali*, 2015.

MERHA S. K.-TRIMBLE M., S*econdary Liability, ISP Immunity, and Incumbent Entrenchment*, in *62 Am. J. Comp. L.*, 2014, p. 685 ss.

MEZZANOTTE M., *Il diritto all'oblio. Contributo allo studio della privacy storica*, Napoli, 2009.

MINOTTI D., *Responsabilità penale: il provider è tenuto ad "attivarsi"?*, 2003, in *www.interlex.it.*

MONATERI P.G., *La responsabilità civile*, in *Tratt. dir. civ.* diretto da R. Sacco, Torino, 1998, p. 1012.

MONTAGNANI M. L., *Internet, contenuti illeciti e responsabilità degli intermediari*, Milano, 2018.

MONTI A., *Uno spettro si aggira per l'Europa: la responsabilità del provider*, 2000, in *www.interlex.it.*

MORELLI M.R., *voce Oblio (diritto all')*, in *Enc. dir. Agg.*, Milano, 2002, p. 851 ss.

MORELLI S., *Fondamento costituzionale e tecniche di tutela dei diritti della personalità di nuova emersione (a proposito del cd "diritto all'oblio")*, in *Giust. civ.*, 1997 p. 515 ss.

NATHRATH D., *Criminal Liability of Internet Providers in Germany: Convinction of a CompuServe Executive*, in *Jour. of Internet Law*, 1998, p. 1 ss.

NATOLI R., *La tutela dell'onore e della reputazione in Internet: il caso della diffamazione anonima*, in *Eur. dir. priv.*, 2001, p. 450 ss.

NIGER S., *Il diritto all'oblio*, in G. Finocchiaro (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale*, Padova, 2007, p. 59 ss.

NIMMER B.- NIMMER D., *On Copyright*, New York, 2002.

NIVARRA L.- RICCIUTO V., *Internet e diritto dei privati, persone e proprietà intellettuale nelle reti telematiche*, Torino, 2010.

NIVARRA L., *Internet e responsabilità extracontrattuale*, in A. PALAZZO-U. RUFFOLO, *La tutela del navigatore in Internet*, Milano, 2002, p. 204 ss.

NIVARRA L., *L'enforcement dei diritti di proprietà intellettuale dopo la Direttiva 2004/48/CE*, in *Rivista di diritto industriale*, 2005.

NIVARRA L., *La responsabilità degli intermediari*, in *AIDA*, 2002, p. 307 ss.

NIVARRA L., *Le opere multimediali in internet*, in *AIDA*, 1996, p. 49 ss.

NIVARRA L., *Responsabilità del provider*, in *Dig. Disc. priv*., 2003, p. 1996 ss.

OBERDORFF H., *Le Conseil costitutionelle et l'ordre juridique communautaire: coopération et controle (à propos de la décision du Conseil costitutionelle n. 2004-496 du 10 juin 2004 relative à la loi pour la confiance dand l'économie numérique)*, in *Revue dr. Publ. Sc. Pol.*, 2004, p. 869 ss.

ONOFRIO T., *L'impresa di content, host e access providing*, in *AIDA*, 2007, p. 355 ss.

PACE A.-PETRANGELI F., *Diritto di cronaca e di critica, in Enc. dir. (Agg. V)*, 2002.

PAGALLO U., *Sul principio di responsabilità giuridica in rete*, in *Dir. inf*., 2009, p. 714 ss.

PALMIERI A.-PARDOLESI R., *Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google*, in *Nuovi Quaderni del Foro Italiano*, 2014, p. 1 ss.

PALMIERI A., *I contratti di accesso*, Milano, 2012.

PANETTA R.-ROVATI A.M., *Diritto di Internet*, 2019.

PARDOLESI R., *Oblio e anonimato storiografico: usque tandem...?*, in *Danno e resp.*, 2019, p. 604 ss.

PARDOLESI R., *Oltre ''Google Spain'' e il diritto all'oblio*, in *Foro it*., 2017, c. 219 ss.

PARISI A.G., *Il commercio elettronico*, in S. SICA-V. ZENO ZENCOVICH, *Manuale di diritto dell'informazione*, 2012, p. 231 ss.

PASCUZZI G.-GIOVANELLA F., *Dal diritto alla riservatezza alla compute privacy*, in *Il diritto dell'era digitale*, a cura di G. Pascuzzi, Bologna, 2016, p. 43 ss.

PASCUZZI G., *Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche*, 2003.

PASCUZZI G., *Il diritto nell'era digitale*, Bologna, 2016.

PASCUZZI G., *Internet*, in *Dig. Disc. priv.*, Torino, 2000, p. 121 ss.

PASQUALE F., *Platform Neutrality: Enchancing Freedom of Expression in Spheres of Private Power*, in *17 Theoretical Inquiries L.*, 2016, p. 494.

PASQUINI T., *Servizi telematici e criteri di responsabilità*, Milano, 2003.

PASSAGLIA P., *Privacy e nuove tecnologie, un rapporto difficile. Il caso emblematico dei social media, tra regole generali e ricerca di una specificità*, in *Consulta Online*, 2016, in *www.giurcost.org*

PELZ C., *Die strafrechtliche Verantwortlichkeit von Internet-Providern*, in *ZUM*, 1998, p. 534 ss.

PERLINGIERI P., *Informazione, libertà di stampa e dignità della persona*, in *Rass. dir. civ.*, 1986, p. 624 ss.

PERON S., *Responsabilità extracontrattuale: problematiche giuridiche connesse alla Rete Internet*, in *Resp. civ. prev.*, 2000, p. 56 ss.

PETRUSO R., *Fatto illecito degli intermediari tecnico della rete e diritto d'autore: un'indagine di diritto comparato*, in *Europa e Diritto Privato*, 2012, p. 1175 ss.

PETRUSO R., *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, Palermo, 2019.

PETRUSO R., *Responsabilità degli intermediari di Internet e nuovi obblighi di conformazione: robo-takedown, policy of termination, notice and take steps*, in *Europa e Diritto Privato*, 2017, p. 451 ss.

PICOTTI L., *Studi di diritto penale dell'informatica*, 1992.

PICOTTI L., *Il diritto penale dell'informatica nell'epoca di internet*, 2004.

PIERUCCI A., *La responsabilità del provider per i contenuti illeciti della Rete*, in *Riv. crit. dir. priv.*, 2003, p. 144 ss.

PIRAINO F., *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm.*, 2017, p. 372 ss.

PIRAINO F., *Spunti per una rilettura della disciplina giuridica degli Internet service provider*, in *AIDA*, 2017, p. 513 ss.

PIRAINO F., *Sulla nozione di bene giuridico in diritto privato*, in *Riv. crit. dir. priv.*, 2013, p. 459 ss.

PITRUZZELLA G., *La libertà di informazione nell'era di Internet*, in *Media Laws, Rivista di diritto dei media*, 2018, p. 12 ss.

PIZZETTI F., *Il caso del diritto all'oblio*, Torino, 2013.

PIZZETTI F., *Il prisma del diritto all'oblio*, in ID. (a cura di), *Il caso del diritto all'oblio*, Torino, 2013, p. 62 ss.

POGGIO G., *La responsabilità dell'internet provider*, in A. PALAZZO- U. RUFFOLO, *La tutela del navigatore in Internet*, 2011.

PONZANELLI G., *Verso un diritto uniforme per la responsabilità degli internet service provider*, in P. STANZIONE- S. SICA, *Commercio elettronico e categorie civilistiche*, Milano, 2002, p. 371 ss.

PONZANELLI G., *Verso un diritto uniforme per la responsabilità degli Internet Service providers?*, in *Danno e resp*., 2002, p. 5 ss.

PROCIDA MIRABELLI DI LAURO A., *Intelligenze artificiali e responsabilità civile*, in A. PROCIDA MIRABELLI DI LAURO-M. FEOLA, *Diritto delle obbligazioni*, Napoli, 2020, p. 507 ss.

PROCIDA MIRABELLI DI LAURO A.- FEOLA M., *Diritto delle obbligazioni*, Napoli, 2020.

PROSPERETTI E., *La circolazione delle opere digitali*, in *Diritto dell'internet. Manuale operativo: casi, legislazione, giurisprudenza*, 2012.

PULIGHEDDU C., *Trattamento dei dati personali e responsabilità da esercizio di attività pericolose*, in *Resp. com. impr.*, 1998, p. 445 ss.

RAZZANTE R., *Manuale di diritto dell'informazione e della comunicazione*, Padova 2002.

RESTA G., *Diritti esclusivi e nuovi beni immateriali*, Torino, 2010.

RICCIO G.M.-PERON S., *Responsabilità extracontrattuale: problematiche connesse all'utilizzo della Rete Internet*, in *Resp. civ. prev*., 2000, p. 820 ss.

RICCIO G.M., *Alla ricerca della responsabilità dei motori di ricerca*, in *Danno e resp.*, 2011, p. 753 ss.

RICCIO G.M., *Anonimato e responsabilità in Internet*, in *Dir. inf*., 2000, p. 20 ss.

RICCIO G.M., *Diritto all'anonimato e responsabilità civile del provider*, Torino, 2009.

RICCIO G.M., *Diritto all'oblio e responsabilità dei motori di ricerca*, in *Dir. inf*., 2014, p. 753 ss.

RICCIO G.M., *La responsabilità civile degli Internet providers*, Torino, 2002.

RICCIO G.M., L*a responsabilità degli internet providers nel d. legisl. n. 70 del 2003,* in *Danno e resp*., 2003, p. 1157.

RICCIO G.M., *La responsabilità degli Internet Service Provider. Situazione legislativa e problemi aperti,* in *Studi di diritto della comunicazione, Persone, Società e Tecnologie dell'Informazione*, a cura di V. D'Antonio e S. Vigilar, Padova, 2009, p. 154 ss.

RICCIO G.M., *La responsabilità del provider nell'esperienza francese: il caso Hallyday*, in *Dir. inf.*, 1999, p. 929.

RICCIO G.M., *La tutela della riservatezza*, in *Manuale di diritto dell'informazione e della comunicazione*, a cura di S. Sica e V. Zeno Zencovich, Padova, 2015, p. 335 ss.

RICCIO G.M., *Profili di responsabilità civile dell'Internet Provider*, in *Quaderni del Dipartimento di Diritto dei rapporti civili ed economici nei sistemi giuridici contemporane*i, diretti da P. Stanzione, Salerno, 2000, p. 19 ss.

RICCIUTO V.- ZORZI N., *Il contratto telematico, Trattato di diritto pubblico dell'economia*, Padova, 2002.

RISTUCCIA R.-TUFARELLI L., *La natura giuridica di Internet e le responsabilità del provider*, 1997, in *www.interlex.it.*

RODOTÀ S., *Libertà, opportunità, democrazia, informazione, in Internet e privacy: quali regole?*, in *Supp. n.1 Bollett. n. 5 Garante*, 1998, p. 15 ss.

RODOTÀ S., *Tra diritti fondamentali ed elasticità della normativa: il nuovo Codice sulla privacy*, in *Eur. dir. priv*., 2004, p. 2 ss.

ROPPO V., *La responsabilità civile per trattamento di dati personali*, in *Danno e resp.*, 1997, p. 660 ss.

ROPPO V., *Libertà di manifestazione del pensiero*, in *Enc. dir.*, 1974, p. 361 ss.

ROSSELLO C. - FINOCCHIARO G. -TOSI E., *Commercio elettronico, documento informatico e firma digitale. La nuova disciplina*, Torino, 2003.

ROSSELLO C., *Commercio elettronico*, Milano, 2006.

ROSSELLO C., *La governance di internet tra diritto statuale, autodisciplina, soft law e lex mercatoria*, in *20 Diritto del commercio internazionale*, 2006, p. 45 ss.

ROSSELLO C., *Riflessioni de jure in materia di responsabilità del provider*, in *Dir. inf.*, 2010.

ROVATI A.M., *Commentario breve alle leggi su proprietà intellettuale e concorrenza*, 2012.

ROVATI A.M., *Il dibattito sulla legittimità del regolamento AGCOM: le opinioni in campo*, in *Il regolamento AGCOM sul diritto d'autore*, Torino, 2014.

RUFFOLO U., *La tutela del navigatore in Internet*, Milano, 2002, p. 183 ss.

RUGGIERO F., *Individuazione nel cyberspazio del soggetto responsabile e ruolo dell'Internet provider*, in *Giur. it*., 2001, p. 601 ss.

SALARELLI A., *Ancora sul diritto all'oblio: cosa cambia dopo la sentenza della Corte di Giustizia Europea contro Google*, in *Italian Journal of Library and Information Science*, 2015, p. 149 ss.

SAMMARCO P., *Atti di concorrenza sleale attraverso Internet e responsabilità del "provider"*, in *Dir. inf.*, 2002, p. 100 ss.

SAMMARCO P., *Brevi note critiche sul fondamento del potere normativo dell'AGCOM nel procedimento di notice and take down*, in *Dir. inf.*, 2017 p. 346 ss.

SAMMARCO P., *La posizione dell'intermediario tra l'estraneità ai contenuti trasmessi e l'effettiva conoscenza dell'illecito: un'analisi comparata tra Spagna, Francia e regolamentazione comunitaria*, in *Dir. Inf.*, 2017, p. 285 ss.

SANNA E., *Il regime di responsabilità dei provider intermediari di servizi della società dell'informazione*, in *Resp. civ. prev*., 2004, p. 279 ss.

SARTOR G., *L'informatica giuridica e le tecnologie dell'informazione-Corso d'informatica giuridica*, Torino, 2016, p. 233 ss.

SCARPELLINO C., *Un oblio tutto europeo*, in *Danno e resp*., 2020, p. 209 ss.

SCIALDONE M., *Il rapporto tra informatica e diritto: passato, presente e futuro*, in *Cyberspazio e diritto*, 2010, p. 8 ss.

SCOPINARO L., *Internet e delitti contro l'onore*, 2000.

SERIO M., *La tutela della parte adempiente: il principio di effettività del rimedio risarcitorio e la sua attenzione negli ordinamenti nazionali*, in *Eur. dir. priv*., 2010, p. 1108 ss.

SERIO M., *Studi comparatistici sulla responsabilità civile*, Torino, 2007.

SETTIMIO R., *Nota a Cassazione civile 21 luglio 2021, n.20861*, in *Giustiziacivile.com*, 2021, p. 876 ss.

SHEDD J.A., *Salt from my Attic*, in F.R. SHAPIRO (a cura di), *The Yale Book of Quotation*, in *Yale University Press*, 2006, p. 75 ss.

SICA S.-D'ANTONIO V., *La procedura di de-indicizzazione*, in G. RESTA-V. ZENO ZENCOVICH (a cura di), *Il Diritto All'Oblio Su Internet Dopo La Sentenza Google Spain*, Roma, 2015, p. 162 ss.

SICA S.-ZENO ZENCOVICH V., *Manuale di diritto dell'informazione e della comunicazione*, Padova, 2012.

SICA S.-D'ANTONIO V., *La procedura di de-indicizzazione*, in *Dir. inf*., 2014, p. 708 ss.

SICA S.-ZENO ZENCOVICH V., *Legislazione, giurisprudenza e dottrina nel diritto dell'Internet*, in *Dir. inf.*, 2010, p. 377 ss.

SICA S., *Commento* sub *art. 18*, in E. GIANNANTONIO-M. G. LOSANO -V. ZENO-ZENCOVICH, *La tutela dei dati personali. Commentario alla l. 675/96*, Padova,1997, p. 176 ss.

SICA S., *Il sistema di responsabilità*, in S. SICA-G. COMANDÈ, *Il commercio elettronico*, Torino, 2001, p. 221 ss.

SICA S., *Le responsabilità civili*, in *Commercio elettronico e servizi della società dell'informazione*., Milano, 2005.

SICA S., *Recepita la direttiva sul commercio elettronico*, in *Corriere giur.*, 2003, p. 1247 ss.
SICA S., *Responsabilità del* provider*: per una soluzione "equilibrata" del problema*, in *Corriere giur.*, 2013, p. 506 ss.
SIGNORELLI F., *Profili di responsabilità del provider nell'E-Commerce*, in V. FRANCESCHELLI (a cura di), *Commercio elettronico*, Milano, 2001, p. 555 ss.
SMITH G., *Internet Law and Regulation*, London, 2007.
SOCHA M., *Double Standard: a comparison of British and American defamation law*, in *Penn. St. Int'l L. Rev.*, 2004 p. 471 ss.
SOLOVE D.J., *The future of Reputation: Gossip, Rumor, and Privacy on the Internet*, Yale University Press, 2007.
SPANGARO A., *Notizie sul web e oblio: il conflitto tra cronaca, reputazione, riservatezza*, in *Giur. it.*, 2021, p. 1331 ss.
SPATUZZI A., *Diritto all'oblio e rievocazione storica. Il bilanciamento delle Sezioni Unite*, in *Diritto di Famiglia e delle Persone*, 2020, p. 1260 ss.
SPLINDER G.-SCHUSTER F., *Recht der elektronischen Medien: Kommentar*, in *GRUR*, 2011, p. 7 ss.
STALLA-BOURDILLON S., *The flip side of ISP's liability regimes: The ambiguous protection of fundamental rights and liberties in private digital spaces*, in *26 Computer Law & Security Review*, 2010, p. 492 ss.
STANZIONE M.G., *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Europa e Diritto Privato*, 2016, p. 1259 ss.
STANZIONE M.G., *Libertà di espressione e diritto alla privacy nel dialogo delle Corti. Il caso del Diritto all'oblio*, in *Europa e Diritto Privato*, 2020, p. 991 ss.
STANZIONE P., *Commercio elettronico e altre categorie civilistiche*, in S. SICA-P. STANZIONE, *Commercio elettronico e categorie civilistiche*, 2002, p. 37 ss.
STANZIONE P., *Commercio elettronico, contratto ed altre categorie civilistiche*, in *Dir. inf.*, 2001, p. 652 ss.
STANZIONE P., *Informazione, potere, contropotere: e le libertà del cittadino?*, in S. SICA- P. STANZIONE, *Informazione, verità e tutela della persona*, in *Quaderni del Dipartimento dei rapporti civili ed economici nei sistemi giuridici contemporanei dell'Università degli studi di Salern*o, 1997, p. 55 ss.
STANZIONE P., *Informazione: potere, contropotere e libertà del cittadino?*, in *Riv. dir. priv.*, 1992, p. 339 ss.

STERN K., *La Carta dei diritti fondamentali dell'Unione europea. Riflessioni sulla forza vincolante e l'ambito di applicazione dei diritti codificati nella Carta*, in *Rivista italiana di diritto pubblico comunitario*, 2014, p. 184 ss.

STOMER T.H., *Online-recht: Rechtfragen im Internet*, Heidelberg, 1999, p. 216 ss.

TAVELLA M.-BONAVITA S., *La Corte di Giustizia sul caso "Adwords": tra normativa marchi e commercio elettronico*, in *Dir. ind.*, 2010, p. 429 ss.

TESCARO M., *La responsabilità dell'internet provider nel d.lgs n. 70/2003*, in *Resp. civ. prev., 2010*, p. 175 ss.

TEUBNER G., *Soggetti giuridici digitali? Sullo* status *privatistico degli agenti* software *autonomi*, a cura di P. Femia, Napoli, 2019, p. 19 ss.

THIENE A., *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo Regolamento europeo*, in *Nuove leggi civ. comm*., 2015, p. 412 ss.

THOMPSON M., *Beyond Gatekeeping: The Normative Responsability of Internet Intermediaries*, in *18 Vand. J. Ent. & Tech*., 2016, p. 783 ss.

TONOLETTI B., *La tutela dei diritti di proprietà intellettuale tra giurisdizione e amministrazione*, in *AIDA*, 2013.

TORRIANI S. - PARISE O., *Internet e diritto*, Milano, 1998.

TOSI E., *Contrasti giurisprudenziali in materia di responsabilità civile degli hosting provider- passivi e attivi- tra tipizzazione normativa e interpretazione evolutiva applicata alle nuove figure soggettive dei motori di ricerca, social network e aggregatori di contenuti*, in *Riv. dir. priv.*, 2017, p. 100 ss.

TOSI E., *I problemi giuridici di Internet*, Milano, 2001.

TOSI E., *I problemi giuridici di Internet. Dall'E-Commerce all'E-Business*, Milano, 2003, p. 570 ss.

TOSI E., *La disciplina applicabile all'hosting provider per la pubblicazione di contenuti digitali protetti dal diritto d'autore, tra speciale irresponsabilità dell'ISP passivo e comune responsabilità dell'ISP attivo, alla luce di Cassazione 7708/2019 e 7709/2019*, in *Riv. dir. ind*., 2019, p. 201 ss.

TOSI E., *Obblighi di filtraggio ex post di contenuti illegali illeciti equivalenti e responsabilità civile degli hosting provider*, in *Dir. ind.*, 2020, p. 284 ss.

TRAINA CHIARINI R., *L'evoluzione della responsabilità degli Internet Service Provider,* in *Corriere giur.*, 2021, p. 1435 ss.

TRIMARCHI P., *Rischio e responsabilità oggettiva*, Milano, 1961.

TRIPODI E.M.- SANTORO F.- MISSINEO S., *Manuela dell'E-Commerce*, Milano, 2000.

TROIANO O., *L'impresa di content, host e access providing*, in *AIDA*, 2011, p. 201 ss.

TURNER M., *Libel on line: the U. K. Perspective*, in *Comp. L. Ass. Bull.*, 1995, p. 12 ss.

URBAN M.-KARAGANIS J., *Notice and Takedown in Everyday Practice*, BerkleyLaw, 2016, p. 60 ss.

VAN EIJK N.-VAN ENGERS T.-ABEL W.-WIERSMA C.-JESSERAND C., *Moving Towards Balance: a Study into Duties of Care on the Internet*, in *Amsterdam Law School Legal Studies Research Paper Series*, 2012, p. 58 ss.

VICK D.W. - MACPHERSON L., *An Opportunity Lost: The United Kingdom's Failed Reform of Defamation Law*, in *Fed. Comm. L.J*., 1996, p. 621 ss.

VIGEVANI G.E., *Identità, oblio, informazione e memoria in viaggio da Strasburgo a Lussemburgo, passando per Milano*, in *Danno e resp.*, 2014, p. 731 ss.

VIGORITI V., *E-Commerce e tutela giurisdizionale*, in *Dir. inf.*, 2001, p. 669 ss.

VOITURIEZ A., *Problématique de la responsabilité du fournisseur d'accès sur internet,* in *Gaz. Pal.*, 1999, p. 22 ss.

VON BAR C., *Gemeineuropäisches Deliktsrecht*, I, München, 1996, p. 137 ss.

VOZZA V., *La responsabilità civile degli Internet Service Provider tra interpretazione giurisprudenziale e dettato normativo*, in *Danno e resp*., 2018, p. 95 ss.

WIMMER N., *Die Verantwortlichkeit des Online-Providers nach dem neuren Multimediarecht – zugleich ein Überblick über die Entwicklung der Rechtsprechung seit dem 1.8.1997,* in *Zeitschrift für Urheber-und Medienrecht*, 1999, p. 439 ss.

YEN A. C., *Internet Service Provider Liability for Subscriber Copyright Infringement Enterprise Liability and the First Amendment*, in *Georgetown Law Journal*, 2002, p. 1 ss.

YEN A., *A preliminary economic analysis of Napster: Internet Technology, Copyright liability and the possibility of Coasen Bargaining,* in *Dayton*, 2000, p. 248 ss.

YOO C.S., *Free Speech and the Myth of the Internet as an Unintermediated Experience*, in *78 Geo. Wash. L. Rev*., 2010, p. 697 ss.

ZAGREBELSKY G., *Manuale di diritto costituzionale*, 1987.

ZANINI S., *Il diritto all'oblio nel Regolamento europeo 679/2016: quid novi?*, in *www.federalismi.it*, 2018, p. 9 ss.

ZANNELLI C., *"Revenge Porn". Pregi e aporie della nuova fattispecie di cui all'art. 612-ter c.p.*, in *Diritto di Famiglia e delle Persone*, 2021, p. 1427 ss.

ZENO ZENCOVICH V., *I rapporti tra responsabilità civile e responsabilità penale nelle comunicazioni su Internet (riflessioni preliminari)*, in *Dir. inf*., 1999, p. 37 ss.

ZENO ZENCOVICH V., *La pretesa estensione alla telematica del regime sulla stampa: note critiche*, 1998.

ZENO ZENCOVICH V., *La pubblicità nei mezzi di comunicazione*, in *AIDA*, 1996, p. 256 ss.

ZENO ZENCOVICH V., *Note critiche sulla nuova disciplina del commercio elettronico dettata dal d. legisl. n. 70 del 2003*, in *Dir. inf.*, 2003, p. 505 ss.

ZENO-ZENCOVICH V., *Appunti sulla disciplina costituzionale delle telecomunicazioni*, in *Dir. inf.*, 1996, p. 400 ss.

ZENO-ZENCOVICH V., *La libertà d'espressione: media, mercato, potere nella società dell'informazione*, Bologna, 2004.

ZENO-ZENCOVICH V., *Profili attivi e passivi della responsabilità dell'utente in Internet*, in A. PALAZZO e U. RUFFOLO (a cura di), *La tutela del navigatore in Internet*, 2002, p. 137 ss.

ZENO-ZENCOVICH V., *Una svolta giurisprudenziale nella tutela della riservatezza*, in *Dir. inf.*, 1986, p. 934 ss.