5/2018

IL SISTEMA DI CONTROLLO SUCCESSIVO: OBBLIGO DI RIMOZIONE DELL'ISP E MECCANISMI DI *NOTICE AND TAKE DOWN*

di Beatrice Panattoni

SOMMARIO: 1. Premessa. – 2. La responsabilità dell'ISP per mancata rimozione nella giurisprudenza italiana. – 3. La controversa definizione di "effettiva conoscenza" e il possibile rimedio dei meccanismi di *notice and take down*. – 4. Le esperienze degli ordinamenti statunitense, tedesco e italiano. – 5. La difficile armonizzazione degli interessi e delle fonti, prospettive *de jure condendo*.

1. Premessa.

La responsabilità per condotta omissiva dell'*Internet Service Provider*[1] (di seguito "ISP" per brevità) vive di una bipartizione intesa in termini temporali. Essa infatti, ripercorrendo i dettami normativi che ne regolano la disciplina – la Direttiva europea sul commercio elettronico 2000/31/CE e il D.lgs. n. 70/2003 che ne ha attuato il contenuto all'interno dell'ordinamento italiano –, può essere ricondotta a due differenti momenti dell'attività svolta dallo stesso ISP[2].

Da una parte si può parlare di una responsabilità *ex ante*, la quale deriverebbe da un mancato controllo preventivo e generale sulle informazioni ospitate, trasmesse o memorizzate dagli ISP. Tale forma di responsabilità è stata esclusa sia dalla dottrina[3] che

[1] Per ragioni di organicità e brevità non si menzioneranno le forme di responsabilità commissiva dell'ISP, anche se una prima premessa dovrebbe riguardare la distinzione che è stata fatta appunto tra le condotte attive e omissive dei *provider* e le conseguenti forme di responsabilità. Sul punto cfr. PETRINI D., *La responsabilità penale per i reati via Internet,* Napoli, 2004, p. 124.

[2] Nello stesso senso: M. BASSINI, *La rilettura giurisprudenziale della disciplina degli* internet service provider, in *Bocconi Legal Papers,* 2015, 5, p. 39 ss.

[3] Per quanto riguarda il diritto penale, gli orientamenti dottrinali concordano sull'esclusione di una responsabilità degli ISP fondata su un obbligo di controllo e attivazione *ex ante,* mentre, in merito alla configurabilità di una responsabilità penale dell'ISP a titolo di concorso omissivo nel reato commissivo dell'utente, la dottrina è contrastante; limitandosi a quella italiana, a favore: cfr. L. PICOTTI, *La responsabilità penale dei* service providers *in Italia*, in *Dir. pen. processo*, 1999, 4, p. 504 ss.; ID., *La legge contro lo sfruttamento sessuale dei minori e la pedopornografia in Internet (L. 6 febbraio 2006, n. 38) (Parte seconda)*, in *Studium Iuris*, 2007, 11, p. 1207 ss.; R. FLOR, *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet. Un'indagine comparata in prospettiva europea ed internazionale,* 2010, Padova, p. 457 ss.; V. TORRE, *Sulla responsabilità penale del* service provider *e la definizione del comportamento esigibile alla luce delle norme contro la pedopornografia*, in L. Picotti (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013, p. 183 ss.; – contro: cfr. S. SEMINARA, *La responsabilità penale degli operatori su internet*, in *Dir. inform.*, 1998, 4-5, p. 745 ss.; A. MANNA,

dalla giurisprudenza[4]. Essa infatti richiederebbe interventi tecnicamente impraticabili nonché eccessivamente onerosi agli ISP, e confliggerebbe con l'espresso divieto contenuto nell'art. 15 della Direttiva sull'*e-commerce* (recepito dall'art. 17 D.lgs. n. 70/2003), il quale proibisce agli Stati membri l'imposizione a carico degli ISP di un generale e preventivo obbligo di sorveglianza sulle informazioni che trasmettono o memorizzano.

La seconda forma di responsabilità riguarda invece un momento successivo a quello del controllo preventivo delle informazioni, più precisamente essa guarda alla fase in cui l'informazione illecita è stata "caricata" sulle piattaforme gestite dagli ISP. Questa ipotesi di responsabilità *ex post* dell'ISP si fonda su quanto è previsto nell'art. 14 c. 1 lett. b) della Direttiva citata, il quale stabilisce una responsabilità in particolare per i c.d. *hosting provider* nel caso in cui essi, effettivamente a conoscenza della presenza di un contenuto illecito sui propri *server*, omettano di rimuoverlo. Dal punto di vista del diritto penale, si parlerebbe in tali fattispecie, laddove non si ritengano applicabili le esenzioni previste dalla Direttiva 31/2000, di una responsabilità dell'ISP per concorso omissivo nel reato commissivo dell'utente, se detto contenuto sia penalmente illecito.

La seconda forma di responsabilità sopra descritta è stata oggetto di alcune recenti pronunce giurisprudenziali, in materia penale e civile, all'interno dell'ordinamento italiano[5], le quali hanno individuato nella previsione dell'art. 14 della Direttiva europea (cui corrisponde quella dell'art. 16 D.lgs. n. 70/2003) la fonte di un obbligo d'impedimento a carico degli ISP, legittimante un'imputazione di responsabilità degli stessi a titolo concorsuale.

Lo sviluppo giurisprudenziale sul tema, che non è stato accompagnato da modifiche del testo normativo di riferimento, dimostratosi ormai inadeguato alla materia che si prefigge di regolare[6], è avanzato parallelamente ai cambiamenti

---

*Considerazioni sulla responsabilità penale dell'*Internet provider *in tema di pedofilia*, in *Dir. inform.*, 2001, 17, 2, p. 145 ss.; F. RUGGIERO, *Individuazione nel ciberspazio del soggetto penalmente responsabile e ruolo dell'*internet provider, in *Giur. merito*, 2001, 2, p. 586 ss.; PETRINI, *La responsabilità penale*, cit., p. 178; V. SPAGNOLETTI, *La responsabilità del* provider *per i contenuti illeciti di Internet*, in *Giur. merito*, 2004, 9, p. 1922 ss.; A. INGRASSIA, *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine? Le responsabilità penali dei* provider *nell'ordinamento italiano*, in L. Luparia (a cura di), Internet provider *e giustizia penale*, Milano, 2012, p. 47 ss. Per quella tedesca basti qui il rinvio al fondamentale contributo di U. SIEBER, *Responsabilità penali per la circolazione di dati nelle reti internazionali di computer. Le nuove sfide di Internet,* in *Riv. trim. dir. pen. econ.,* 1997, 3, p. 775 ss.; la II parte in *Riv. trim. dir. pen. econ.,* 1997, 4, p. 1206 ss.

[4] Le più rilevanti pronunce della Corte di giustizia dell'Unione Europea sul tema riguardano i c.d. "casi SABAM: sentenza del 24 novembre 2011, C-70/10, *Scarlet Extended*, EU:C:2011:771 e sentenza del 16 febbraio 2012, C-360/10, *SABAM,* EU:C:2012:85. Nella giurisprudenza italiana si segnala invece il noto caso *Google c. ViviDown,* Cass. Pen., Sez. III, 17 dicembre 2013, n. 5107, in *Dir. fam.*, 2014, 2, p. 675 ss.

[5] Tribunale civile di Torino, 7 aprile 2017, n. 1928, in *Danno resp.*, 2018, 1, p. 87 ss.; Tribunale civile di Napoli Nord, 3 novembre 2016, in *Giur. it.*, 2017, 3, p. 629 ss.; Cass. Pen., Sez. V, 27 dicembre 2016, n. 54946, in *Foro it.*, 2017, p. 251 ss.

[6] Sull'inadeguatezza rispetto ai tempi della Direttiva europea sull'*e-commerce* si vedano R. BOCCHINI, *Responsabilità dell'*hosting provider *– la responsabilità di Facebook per la mancata rimozione dei contenuti illeciti*, in *Giur. it.*, 2017, 3, p. 629 ss.; R. PETRUSO, *Responsabilità degli intermediari di Internet e nuovi obblighi di conformazione:* Robo-Takedown, Policy of Termination, notice and take steps, in *Eur. dir. priv.*, 2017, 2, p. 451 ss.; O. POLLICINO, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli* Internet service provider, in

tecnologici di Internet. L'evoluzione del Web, che fa parlare oggi di una sua versione 4.0, ha infatti segnato il presentarsi di nuove realtà nel *Cyberspace*, tra cui di particolare rilievo sono i c.d. *User generated content*[7]. Si tratta di nuove tipologie di piattaforme online, gestite da ISP aventi capacità tecniche di indicizzazione, organizzazione e categorizzazione delle informazioni fornite e caricate dagli stessi utenti, sempre più efficaci e incisive (basti pensare al *social network* Facebook). A fronte delle nuove capacità d'intervento acquisite dagli ISP, la giurisprudenza, europea e nazionale[8], ha segnato negli ultimi anni un importante adeguamento nell'applicazione del dato normativo alle nuove realtà oggetto dei suoi interventi.

In questa fase di rielaborazione delle regole fondanti l'eventuale responsabilità dei *provider* per mancata rimozione dei contenuti illeciti online, assumono importanza decisiva, da una parte, i contributi della dottrina e della giurisprudenza che definiscono presupposti e limiti degli obblighi di rimozione e della conseguente responsabilità; dall'altra, gli interventi normativi che in singoli ambiti tentano di ordinare diverse fattispecie, introducendo – come si vedrà – meccanismi e procedure formali in grado di disciplinare in modo chiaro il contrasto ai contenuti illeciti nel *Cyberspace*.

Un'ultima premessa risulta necessaria. La frammentarietà delle fonti e degli interventi in materia non rendono semplice un'analisi sistematica delle fattispecie che vedono coinvolti gli ISP[9]. Tale frammentarietà si lega in particolare alle diverse tipologie di *provider*[10] e all'atipicità delle loro attività rispetto alla normativa vigente, le quali presentano dunque dinamiche e problematiche differenti. La più evidente distinzione

---

ConsultaOnline, 2014; F. DI CIOMMO, *Programmi filtro e criteri di imputazione/esonero della responsabilità online. A proposito della sentenza Google/ViviDown*, in *Dir. inform.*, 2010, 6, p. 837 ss.

[7] Per una esposizione più puntuale delle nuove tipologie di ISP e delle relative attività si rimanda a: M. MONTANARI, *La responsabilità delle piattaforme online (il caso Rosanna Cantone)*, in *Dir. inf.*, 2017, 2, p. 254 ss.; R. BOCCHINI, *La responsabilità dell'*hosting provider, cit., p. 629 ss.; 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, 4, p. 1261 ss.; E. TOSI, *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 *Dir. ind.*, 2017, 1, p. 56 ss.

[8] Di particolare rilevanza è l'elaborazione giurisprudenziale di una nuova figura di *provider,* il c.d. *hosting* attivo. A partire dalla giurisprudenza europea – Corte di giustizia dell'Unione Europea, sentenza del 23 marzo 2010, cause riunite da C-236/08 a C-238/08, *Google France* e *Google,* EU:C:2010:159 –, la quale è stata poi recepita con qualche incertezza da quella italiana – a favore: Tribunale di Torino, 23 giugno 2014, in AIDA, 2915, p. 1684 ss.; contro: Corte di Appello di Milano, 7 gennaio 2015, n. 29, in *Dir. ind.*, 2015, 5, p. 455 ss. –, è emersa una nuova tipologia di ISP, non più caratterizzato dai connotati di automaticità, tecnicità e passività che avevano legittimato il regime d'esenzione da responsabilità delineato dalla Direttiva europea sull'*e-commerce,* che non risulta quindi più applicabile a queste nuove figure.

[9] Un'efficacia prospettiva sistematica è stata proposta da BASSINI, *La rilettura giurisprudenziale,* cit., p. 41 ss. dove si distingue tra attività di interpretazione diretta della disciplina degli *Internet Service Provider* e tra rilettura del regime giuridico dei fornitori di servizi in modo "indiretto", «soffermandosi su comparti normativi non necessariamente afferenti a Internet».

[10] La Direttiva europea 31/2000 ha distinto gli ISP, sulla scorta dell'antecedente preso a modello del *Digital Millennium Copyright Act* (DMCA), in tre categorie: *mere conduit, caching* e *hosting provider* in base alle attività che essi svolgono. A queste categorie anderebbero aggiunte le nuove realtà che si sono sviluppate negli anni, in particolare i c.d. *hosting* attivi e i SERP.

può essere riscontrata tra i c.d. SERP (*Serch Engine Results Page*) – i motori di ricerca come ad esempio *Google, Bing* o *Qwant* – e i gestori dei siti sorgente – piattaforme online, come ad esempio *Facebook* o *YouTube*, che ospitano o trasmettono i contenuti organizzati e messi a disposizione dal motore di ricerca.

Ma prima di approfondire la problematica legata all'eterogeneità delle fonti, occorre delineare quali siano allo stato gli obblighi di rimozione a carico degli ISP e le soluzioni che sono emerse per regolarne l'applicazione.

2. La responsabilità dell'ISP per mancata rimozione nella giurisprudenza italiana.

L'elaborazione di una responsabilità penale dell'*hosting provider* a titolo di concorso omissivo nel reato commissivo dell'utente si fonderebbe sull'obbligo di rimozione previsto dall'art. 16 D.lgs. n. 70/2003. Questa responsabilità è stata affermata in particolare dalla Cassazione penale, in una sentenza del 27 dicembre 2016[11], con riferimento ad una vicenda che vedeva contrapposti, da un lato, il legale rappresentante di una società gerente il sito *agenziacalcio.it*, dall'altro lato il presidente della Lega Nazionale Dilettanti della Federazione Italiana Gioco Calcio, il quale lamentava l'avvenuta pubblicazione sul sito in questione di un articolo da parte di un soggetto terzo avente carattere diffamatorio nei suoi confronti. La Corte di Cassazione, confermando quanto deciso in sede di appello, ha ritenuto nella fattispecie sussistente la responsabilità dell'imputato a titolo di concorso nel reato di diffamazione, fondando il proprio giudizio sulla circostanza che il *provider* aveva consapevolmente mantenuto il contenuto diffamatorio sul proprio sito e consentito «che lo stesso esercitasse l'efficacia diffamatoria», pur avendone avuto conoscenza in un momento anteriore all'ordine di sequestro del sito (attraverso l'invio di un'e-mail).

Secondo la costruzione giurisprudenziale, «il giudizio di responsabilità veniva […] formulato per l'aspetto […] dell'aver l'imputato mantenuto consapevolmente l'articolo sul sito»[12]. La condotta di mantenimento del contenuto illecito posta in essere dal *provider*, successiva all'avverarsi della sua effettiva conoscenza, porta quindi, come è stato rilevato in dottrina, alla conseguenza che il gestore del sito Internet «di fatto fa proprio (quello stesso contenuto) e si rende anch'egli colpevole del reato di diffamazione»[13].

Tale pronuncia ha suscitato diverse critiche in dottrina. Secondo alcuni, per paura delle sanzioni in cui i *provider* potrebbero incorrere, una tale impostazione porterebbe a una disincentivazione della creazione di spazi di discussione e scambio di opinione online a scopi non lucrativi[14]; secondo altri la fattispecie non sarebbe

---

[11] Cass., Sez. V, 27 dicembre 2016, n. 54946, cit., con nota di F. DI CIOMMO, *Responsabilità dell'*Internet hosting provider, *diffamazione a mezzo Facebook e principio di tassatività della norma penale: troppa polvere sotto il tappeto*.

[12] Cass. Pen., Sez. V, 27 dicembre 2016, n. 54946, cit.

[13] V. PEZZELLA, *Diffamazione sui* social network*: il gestore del sito deve rimuovere i contenuti?*, in *Web & Tech*, 15 marzo 2017.

[14] R. CARBONE, *Responsabilità del* blogger*: parziale* revirement *della Cassazione?*, in *Cass. Pen.*, 2017, 7-8, p. 2782

riconducibile all'ipotesi del concorso omissivo nel reato, non sussistendo un obbligo giuridico di impedimento, per cui configurerebbe un caso di semplice connivenza[15].

La critica più importante tuttavia sta nella constatazione che l'obbligo d'impedimento, sul quale si fonda il giudizio di responsabilità concorsuale, verrebbe in essere in un momento successivo a quello della consumazione del reato che è diretto ad impedire, scardinando in questo modo l'intera costruzione della fattispecie omissiva impropria risultante dal combinato disposto degli artt. 40 e 110 c.p.[16].

Il reato di diffamazione integra, infatti, un reato istantaneo, che si consuma nella sua realizzazione online nel momento della pubblicazione in rete del contenuto offensivo, per cui un obbligo di rimozione di quello stesso contenuto sarebbe possibile solo post-consumazione. Non conoscendo il nostro ordinamento la complicità successiva, in dottrina è stato proposto il ricorso alla figura della pluralità di reati, «integrati dalla ripetuta trasmissione del dato e riuniti in continuazione»[17]. La criticità di tale costruzione risiede però nell'elemento fattuale, poiché risulta difficile configurare un'azione umana ripetuta nel tempo, quando è il sistema informatico a determinare questi effetti di permanenza e continuazione[18].

Non potendo qui approfondire, per esigenze di brevità, la possibilità di configurare un concorso omissivo del *provider* nel reato commesso dall'utente per mezzo delle strutture dal primo gestite, emerge in ogni caso come l'elemento dato dall'obbligo di rimozione del contenuto illecito da parte dell'ISP abbia assunto un'importante rilevanza. Circostanza che trova conferma in altre pronunce giurisprudenziali, che hanno contribuito all'elaborazione di una definizione più precisa dell'obbligo giuridico di rimozione.

Il Tribunale civile di Napoli Nord, in una sentenza del 2016, ha espressamente dichiarato che «pur in assenza di un generale obbligo di sorveglianza […] deve tuttavia ritenersi sussistente una responsabilità per le informazioni oggetto di memorizzazione durevole o "*hosting*" laddove […] il *provider* sia effettivamente venuto a conoscenza del fatto che l'informazione è illecita (art. 16 c. 1 lett. b) D.lgs. n. 70/2003) e non si sia attivato per impedire l'ulteriore diffusione della stessa»[19]. La previsione di un *sistema di controllo e attivazione successivi* è stata ritenuta il punto di equilibrio tra i diversi interessi coinvolti: tutela dell'indipendenza di Internet, della libertà d'impresa e di manifestazione del pensiero da una parte; tutela dei diritti facenti capo ai singoli utenti ed ai terzi dall'altra. La medesima posizione è stata adottata anche dal Tribunale civile di Torino, nella sentenza del 7 aprile 2017, che ha ulteriormente ampliato il significato dell'obbligo di rimozione, il quale – in virtù delle capacità e degli strumenti tecnici di cui erano in

---

ss.

[15] C. CURRELI, *La controversa responsabilità del gestore di un sito web, in caso di diffamazione commessa da terzi*, in *Resp. civ. prev.*, 2017, 5, p. 1648 ss.

[16] Ibidem; nonché A. INGRASSIA, *Responsabilità penale degli* internet service provider*: attualità e prospettive,* in *Dir. pen. processo*, 2017, 12, p. 1621 ss.

[17] CURRELI, *La controversa responsabilità,* cit.

[18] Ibidem.

[19] Tribunale di Napoli Nord, 3 novembre 2016, cit., con nota di R: BOCCHINI, *La responsabilità di Facebook per la mancata rimozione di contenuti illeciti.*

possesso gli ISP coinvolti[20] – riguarderebbe, sulla base dello stesso dato normativo, anche l'impedimento di nuovi caricamenti aventi ad oggetto informazioni già segnalate come violazioni a quello stesso *provider*[21].

L'esigibilità di un intervento dell'ISP in termini di rimozione del contenuto illecito presente sulle piattaforme dallo stesso gestite trova riscontro anche a livello europeo nella Comunicazione della Commissione in merito alla Strategia per il mercato unico digitale[22]. La Commissione, infatti, dopo aver ribadito il principio «che i prestatori intermediari di servizi via internet non sono responsabili dei contenuti che trasmettono, conservano o ospitano purché mantengano al riguardo un comportamento di rigorosa passività», ha sottolineato che «allo stesso tempo, gli intermediari sono tenuti ad intervenire efficacemente per rimuovere i contenuti illeciti individuati, siano essi informazioni inerenti ad attività illegali quali il terrorismo o la pedopornografia oppure informazioni che violano i diritti di proprietà intellettuale altrui (ad es. il diritto d'autore)»[23].

Se dunque una bilanciata regolamentazione delle dinamiche nel *Cyberspace* passa inevitabilmente attraverso un sistema di controllo e attivazione successivi, una sua formalizzazione si rende quanto mai necessaria, soprattutto per la risoluzione delle problematiche che dottrina e giurisprudenza riconducono all'attivazione dell'obbligo di rimozione da parte dei *provider*, prima fra tutte la definizione della c.d. "effettiva conoscenza", che rappresenta il presupposto applicativo per l'esigibilità dello stesso obbligo.

3. La controversa definizione di "effettiva conoscenza" e il possibile rimedio dei meccanismi di *notice and take down*.

La delimitazione del concetto di "effettiva conoscenza" rappresenta una problematica tuttora aperta all'interno dell'ordinamento italiano, in virtù di un inciso che il legislatore ha inserito all'interno dell'art. 16 c. 1 lett. b) D.lgs. n. 70/2003. Nella lettera del primo comma, che regola l'ipotesi per la quale l'*hosting provider* può andare esente da responsabilità se, una volta a conoscenza del contenuto illecito, provvede a rimuoverlo, è stato infatti aggiunto – rispetto alla previsione corrispondente dell'art. 14

[20] In particolare si tratta dell'utilizzo del c.d. *software* Content ID, tramite il quale si opererebbe un'esclusione dell'informazione per occorrenza attraverso l'utilizzo dei contenuti lesivi oggetto di controversia come *reference file*.

[21] Tribunale di Torino, 7 aprile 2017, n. 1928, cit., con nota di V. VOZZA.

[22] Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, *Strategia per il mercato unico digitale in Europa*; COM(2015) 192 *final* del 6 maggio 2015.

[23] La stessa comunicazione prosegue con il rilevare che «attualmente la disattivazione dell'accesso a contenuti illeciti e la rimozione di questi da parte dei prestatori di servizi di *hosting* può rivelarsi un processo lungo e complicato, con il rischio che siano rimossi per errore anche contenuti che sono invece leciti», elemento che sottolinea la necessaria adozione di meccanismi comuni di *notice and take down*, di cui si dirà meglio in seguito.

Direttiva europea 31/2000 – l'inciso: «*su comunicazione delle autorità competenti*». Da un punto di vista letterale sembrerebbe quindi che presupposto per l'attivazione dell'obbligo di rimozione da parte dell'ISP sia soltanto l'avvenuta comunicazione da parte dell'Autorità della presenza di un contenuto illecito ospitato sui propri *server*.

Il quesito che è allora stato sollevato in dottrina è se l'obbligo di rimozione si configuri a carico del *provider* solamente a seguito di una comunicazione da parte dell'autorità, presupposto per una conoscenza qualificata, o se invece il *provider* debba rispondere di tale obbligo autonomamente, non appena venga a conoscenza del contenuto illecito ospitato, anche ad esempio attraverso una notifica effettuata dalla parte offesa. La giurisprudenza più recente sembra orientata nel ritenere sufficiente una notifica della parte offesa, come tutte e tre le pronunce sopra menzionate, di concerto con altre[24], dimostrano sposando questa tesi.

In particolare la sentenza del Tribunale di Napoli Nord argomenta in modo articolato e completo la scelta di non ritenere quale presupposto necessario la comunicazione dell'Autorità, basandosi sul tenore dell'art. 17, il quale perderebbe altrimenti di significato[25]; sul considerando n. 46 della Direttiva europea sull'*e-commerce*[26] e sull'esigenza di effettività della forma di tutela data dalla tempestiva rimozione del contenuto, la quale non condurrebbe a risultati efficaci laddove vi fosse invece un eccessivo prolungamento dei tempi di reazione.

Una parte della dottrina ha assunto una posizione critica nei confronti di questo orientamento giurisprudenziale, ritenendo necessaria una conoscenza qualificata[27], sia per il tenore letterale della norma – in particolare per il diritto penale vi sarebbe il vincolo

---

[24] Tribunale di Bari, 13 giugno 2006, in *Dir. internet*, 2006, 563; Tribunale di Trani, 14 ottobre 2008, in *Danno resp*., 2009, 1059; Tribunale di Roma, 22 gennaio 2010, inedita; Corte d'Appello di Milano, 7 gennaio 2015, cit.; Tribunale di Roma, 5 maggio 2016, inedita.

[25] Se il *provider* non potesse in ogni caso attivarsi autonomamente perderebbe di significato il divieto ex art. 17 D.lgs. n. 70/2003 di un obbligo generale di sorveglianza – conclusione condivisa dalla X Commissione parlamentare (atto n. 172), la quale nel suo parere sullo schema del D.lgs. n. 70/2003 ha espressamente affermato che «in relazione a quanto previsto dall'articolo 16 (…), al fine di evitare che sia vanificata qualsiasi azione efficace ed immediata tesa alla rimozione dalla rete di materiale illecito appare opportuno precisare che la comunicazione delle autorità non costituisce condizione necessaria per la rimozione delle informazioni o per la disabilitazione dell'accesso; conseguentemente, all'articolo 16, comma 1, lettera b), le parole: "su comunicazione" potrebbero essere sostituite dalle seguenti: "anche a seguito di comunicazione"». Lo stesso articolo 17 permetterebbe di ricavare la sussistenza di un obbligo a fronte di una conoscenza acquisita "passivamente".

[26] Secondo il quale «*per godere di una limitazione della responsabilità, il prestatore di un servizio della società dell'informazione consistente nella memorizzazione di informazioni deve agire immediatamente per rimuovere le informazioni o per disabilitare l'accesso alle medesime non appena sia informato o si renda conto delle attività illecite*». Lo stesso considerando poi prosegue affermando che: «*la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime devono essere effettuate nel rispetto del principio della libertà di espressione e delle procedure all'uopo previste a livello nazionale* (…)».

[27] 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, 2, p. 536 ss.; A. INGRASSIA, *La sentenza della Cassazione sul Caso Google*, in questa *Rivista*, 6 febbraio 2014. A favore: R. BOCCHINI, *La responsabilità di Facebook,* cit.

del principio di tassatività[28] –, sia per arginare il rischio di affidare una funzione di censura all'ISP, il quale, nei casi in cui l'illiceità dei contenuti sia di difficile e incerta valutazione, potrebbe rimuoverli "cautelativamente".

Sembrerebbe tuttavia prevalere l'orientamento che ritiene non necessaria una formale comunicazione dell'autorità per l'attivazione dell'obbligo di rimozione a carico dei *provider*[29], soprattutto in considerazione del necessario bilanciamento degli interessi coinvolti e della natura del *Cyberspace* stesso, nel quale le dinamiche temporali vivono di una incalzante velocità e diffusività, incompatibile con le tradizionali, e più lente, procedure formali delle istituzioni[30].

La questione rimarrà in ogni caso aperta fintanto che non vi sarà un intervento legislativo chiarificatore. Ed a fronte di tutte le considerazioni che precedono, emerge come l'introduzione da parte del legislatore europeo di uno specifico meccanismo potrebbe risolvere la maggior parte delle incertezze in materia: la previsione e regolamentazione di procedure c.d. di *notice and take down*.

Si tratta di una procedura formalizzata che ha trovato il suo primo riconoscimento normativo nella legge federale statunitense detta *Digital Millennium Copyright Act* del 1998[31], con la quale è stata prevista una procedura che permette ai soggetti, il cui diritto di proprietà intellettuale sia stato leso, di notificare al *provider* l'avvenuta lesione, con contestuale obbligo a carico dello stesso di rimuovere il contenuto segnalato.

La previsione a livello europeo di meccanismi formali che regolino in modo uniforme e dettagliato, con tempistiche certe e cadenzate, le procedure di notifica ad

---

[28] F. Di Ciommo, *Responsabilità dell'*Internet hosting provider, cit.

[29] Si segnala inoltre una recente sentenza della Corte di Appello civile di Roma, 19 febbraio 2018, n. 1065, inedita, la quale ha ulteriormente chiarito l'operatività e i requisiti della dinamica segnalazione-rimozione che vede coinvolti *provider* e utenti. L'importanza del contributo di tale sentenza risiede nella specificazione del contenuto necessario della *notification.* Infatti secondo la Corte d'Appello una segnalazione, per poter dar corso a un conseguente obbligo di rimozione a carico dell'ISP, deve contenere non generiche affermazioni, ma «contestazioni specifiche e puntuali». Il caso di specie concerneva la pubblicazione su un sito web di contenuti aventi carattere diffamatorio. In questo caso, secondo la Corte la notifica deve necessariamente contenere: «le singole affermazioni ritenute non veritiere; le ragioni della asserita falsità e le fonti idonee a comprovarlo; le modifiche suggerite così da consentire alla comunità degli utenti e agli amministratori l'esecuzione dei controlli richiesti, a seguito dei quali, se positivi, si può procedere alla modifica richiesta». Solo dunque una notifica avente tali caratteristiche può condurre a una eventuale presunzione di effettiva conoscenza da parte dell'ISP, legittimante il successivo obbligo di rimozione.

[30] Dello stesso avviso è la giurisprudenza della Corte di Giustizia europea, la quale, nella sentenza del 12 luglio 2011, L'Oréal e a., C-342/09, EU:C:2011:474, punti 120 e 121, ha affermato che per la sussistenza della circostanza per la quale l'ISP è considerato «al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione […] è sufficiente, affinché il prestatore di un servizio della società dell'informazione non possa fruire dell'esonero dalla responsabilità previsto all'art. 14 della direttiva 2000/31, che egli sia stato al corrente di fatti o di circostanze in base ai quali un operatore economico diligente avrebbe dovuto constatare l'illiceità di cui trattasi […]. Inoltre, affinché non siano private del loro effetto utile, le norme enunciate all'art. 14, n. 1, lett. a), della direttiva 2000/31 devono essere interpretate nel senso che riguardano qualsiasi situazione nella quale il prestatore considerato viene ad essere, in qualunque modo, al corrente di tali fatti o circostanze».

[31] Legge federale statunitense (Public law 195-304-OCT. 28, 1998) che disciplina peraltro le sole violazioni in materia di diritto d'autore. Si approfondirà il punto in seguito.

opera delle vittime di contenuti illeciti in Rete e i successivi obblighi di rimozione a carico degli ISP, risolverebbe numerose questioni. Un intervento in tal senso dovrebbe chiarire quali siano i requisiti necessari per ottenere una "effettiva conoscenza", risolvendo i dubbi suscitati dal caso italiano esaminato, e quale debba essere il contenuto della notifica per garantire la sua efficacia esplicativa[32]. Una normativa chiara in materia di *notification* semplificherebbe inoltre l'onere della prova gravante sull'utente danneggiato, il quale deve dimostrare in sede processuale il presupposto dell'effettiva conoscenza da parte del *provider* della presenza del contenuto illecito, conoscenza che si realizzerà attraverso il perfezionamento della notifica.

In ambito europeo, anche se la Direttiva sul commercio elettronico all'art. 21 c. 2 prevede un necessario adeguamento periodico della normativa, che può avere ad oggetto anche l'eventuale adozione di procedure di "notifica e rimozione" (*notice and take down*) e la determinazione della responsabilità a seguito della rimozione del contenuto, non è stato ad oggi adottato alcun provvedimento in materia. Ma il tema è stato recentemente oggetto di una comunicazione della Commissione europea, nella quale è stata sottolineata l'importanza e l'esigenza di una maggior e pur sempre bilanciata responsabilizzazione degli ISP, che passa attraverso la previsione di specifiche procedure di segnalazione-rimozione[33].

Interventi normativi concernenti le procedure sopra descritte possono essere rintracciati tuttavia nei singoli ordinamenti nazionali, sulla scorta del citato modello statunitense rappresentato dal DMCA[34].

4. Le esperienze degli ordinamenti statunitense, tedesco e italiano.

Il Titolo II del DMCA, che ha introdotto il § 512 nel Capitolo 5, titolo 17 del Codice degli Stati Uniti, disciplina la responsabilità dei fornitori di servizi in rete in materia di

---

[32] È stato posto infatti il dubbio se la diffida del soggetto leso nei confronti dell'ISP debba contenere a pena di invalidità l'indicazione degli URL (*Uniform Resource Locator* – «sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa in Internet, tipicamente presente su un *server*»; così come riportato in P. PIRUCCIO, *Diritto d'autore e responsabilità del* provider, in *Giur. merito*, 2012, vol. n. 12, p. 2617). Sul punto si segnalano: A. CONTALDO, F. PELUSO, *La tutela del diritto d'autore nel settore audiovisivo e la responsabilità civile degli ISP*, in *Dir. aut*., 2015 vol. n. 1, p. 144; TOSI, *Contrasti giurisprudenziali in materia,* cit.

[33] In particolare la recente Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, *Lotta ai contenuti illeciti online. Verso una maggiore responsabilizzazione delle piattaforme online,* COM(2017) 555 *final* del 28 settembre 2017, nella quale viene espressamente ripreso il considerando n. 40 della direttiva europea sull'*e-commerce*, secondo il quale la direttiva dovrebbe «*costituire la base adeguata per elaborare sistemi rapidi e affidabili idonei a rimuovere le informazioni illecite e disabilitare l'accesso alle medesime*». In questo senso la Commissione ha maggiormente articolato l'obbligo facente capo agli ISP, riabilitando una sua attività *ex ante,* si legge infatti che «le piattaforme online dovrebbero adottare misure proattive efficaci volte a individuare e rimuovere i contenuti illegali online e non solo limitarsi a reagire alle segnalazioni ricevute».

[34] Il modello USA è stato definito, a differenza di quello individuato dalla Direttiva 2000/31/CE, un «sistema a tutela verticale», che «fa ricorso a più plessi normativi, tendenzialmente pensati (…) come se si trattasse di compartimenti stagni», in questo senso PETRUSO, *Responsabilità degli intermediari,* cit., p. 451 ss.

proprietà intellettuale[35]. In particolare, per quanto interessa la presente trattazione, esso regola un puntuale meccanismo di *notice and take down.* Dopo la previsione di cui al § 512(c), il quale impone, da una parte, la designazione ad opera dei *provider* di un apposito soggetto preposto alla ricezione dei reclami dei titolari dei diritti d'autore (n. 2, *designated agent*) e, dall'altra, un'elencazione precisa dei contenuti che deve avere la *notification* (n. 3), il testo normativo presenta due pregi in particolare: una regolamentazione improntata al rispetto del contraddittorio tra le diverse parti e la previsione di correttivi necessari per un suo corretto esercizio.

Il contraddittorio è garantito dalla previsione di una *counter notification*, dichiarazione scritta con la quale l'utente contesta l'avvenuta rimozione o la disabilitazione dell'accesso ad un contenuto segnalato. Nell'ipotesi in cui il *provider* riceva una contro-notifica, il § 512(g) disciplina una procedura che lo stesso dovrà seguire per poter garantire il contradditorio tra le due parti[36].

Nell'intento di tutelare la posizione di sostanziale irresponsabilità degli ISP, sono stati inoltre previsti due correttivi, in particolare: (i) una responsabilità dell'utente per *misrepresentation*, dato che, in caso di falsa rappresentazione della violazione di diritto d'autore, ai sensi del § 512(f), sarà responsabile colui che ha avanzato la falsa notifica e dovrà risarcire tutti i danni sofferti dai soggetti coinvolti; (ii) una presunzione di irresponsabilità dell'ISP, che abbia in buona fede disabilitato l'accesso o rimosso i contenuti a seguito della ricezione di una notifica.

Quello delineato dal DMCA è dunque un procedimento tra privati, all'interno del quale nessuna valutazione in merito alla fondatezza della segnalazione è richiesta al *provider*[37]– elemento di maggiore criticità che potrebbe condurre ad una eccessiva irresponsabilità degli ISP[38]. Si tratta tuttavia di un procedimento che risulta integrato da «meccanismi formalizzati di coordinamento tra la fase del controllo di matrice privatistica e quella, pubblicistica, affidata ad organi statali»[39].

In seguito al DMCA e nonostante il silenzio della Direttiva sul commercio elettronico, l'ordinamento di uno Stato membro dell'Unione Europea si è dotato di tali meccanismi di *notice and take down,* regolandone la disciplina anche più dettagliatamente di quanto abbiano fatto i legislatori statunitensi. La Germania ha infatti recentemente

---

[35] Tra i commenti alla legge americana si segnala: E.A. MCNAMARA – J.H. BLUM – D. GOUGH, *Online Service Provider Liability under the Digital Millennium Copyright Act*, in *The Internet & Communications Law*, 1999, 17 Comm. Law., p. 5 ss.; nella dottrina italiana: M. DE CATA, *La responsabilità civile dell'*internet service provider, Milano, 2010, p. 102 ss.; M. BELLIA – G.A.M. BELLOMO – M. MAZZONCINI, *La responsabilità civile dell'Internet Service Provider per violazioni del diritto d'autore*, in *Dir. ind.*, 2012, 4, p. 349 ss.; M. DEL SIGNORE, *Il sistema U.S.A.,* in AIDA, 2014, 1, p. 3 ss.; F. DI CIOMMO, *Programmi filtro e criteri di imputazione/esonero,* cit., p. 837 ss.

[36] L'ISP deve contattare l'originario proponente la rimozione, fornire copia della contro-notificazione, informarlo che provvederà al reinserimento dei contenuti rimossi allo scadere di dieci giorni lavorativi, reinserire i contenuti sulla rete a partire dal decimo giorno lavorativo dalla ricezione della *counter notification* e, comunque, non oltre il quattordicesimo, a meno che il provider non riceva, prima della scadenza di tale termine, una comunicazione da cui si evinca che il *copyright owner* abbia intentato un'azione contro l'autore diretto dell'illecito.

[37] DEL SIGNORE, *Il sistema USA,* cit., p. 1 ss.

[38] DE CATA, *La responsabilità civile,* cit., p. 128.

[39] S. SICA – V. D'ANTONIO, *La procedura di de-indicizzazione,* in *Dir. inform.*, 2014, 4-5, p. 703 ss.

adottato la "Legge per migliorare la tutela dei diritti sui *social network*" (*Netzwerkdurchsetzungsgesetz – NetzDG*), la quale è entrata in vigore il 1° ottobre 2017[40].

In prospettiva comparatistica vanno evidenziati, da una parte, gli elementi ripresi dal DMCA, dall'altra, le differenze rispetto alla legge statunitense. Elementi simili delle due discipline sono: (i) l'organizzazione dell'obbligo di rimozione attraverso tempistiche definite: gli ISP hanno infatti 24 ore di tempo per rimuovere i "contenuti illeciti"[41] segnalati, se manifestatamente illeciti, mentre hanno sette giorni nei casi di contestazione o rimessione della decisione ad un organo di autoregolamentazione; (ii) la possibilità di inoltrare una *counter notification*; (iii) la nomina di una figura apposita, addetta alla ricezione delle notifiche, a livello federale nella Repubblica tedesca; (iv) obblighi informativi nei confronti degli utenti coinvolti.

Mentre le differenze e le novità rispetto al DMCA possono essere riassunte nei seguenti punti: (i) la differenziazione degli obblighi di rimozione sulla base del grado d'illiceità dei contenuti ospitati sopra descritta e la previsione di un organo di autoregolamentazione; (ii) l'ISP nel *NetzDG* deve autonomamente valutare se il contenuto sia illecito e vada rimosso, senza che sia prevista alcuna clausola di salvaguardia della sua irresponsabilità in caso di rimozione illecita; (iii) l'ambito di applicazione: il *NetzDG*, da una parte, si applica ai soli gestori di *social network* con utenti registrati in Germania che raggiungano almeno due milioni, dall'altra parte essa riguarda invece tutte le fattispecie criminose richiamate dall'art. 1, mentre il DMCA riguarda solo i *copyright infrigments*; (iv) l'ISP è inoltre sottoposto, ai sensi del *NetzDG*, ad un obbligo di resoconto della propria attività di gestione delle segnalazioni.

Una carenza della legge tedesca rispetto al DMCA statunitense può essere individuata nella mancata elencazione e descrizione delle informazioni che deve contenere la *notification* e la *counter-notification*, lasciando dunque irrisolte le incertezze al riguardo. Mentre un suo importante contributo risiede nella prospettiva che differenzia l'obbligo di rimozione rispetto al tipo di contenuto illecito controverso. Nella consapevolezza, infatti, che i *service provider* rimangono in ogni caso soggetti privati, privi di quelle capacità tecniche e giuridiche che consentono di valutare correttamente l'illiceità delle informazioni che transitano o vengono ospitate sui propri *server*, il legislatore tedesco ha trovato un efficace bilanciamento nel differenziare l'obbligo di rimozione tra quei contenuti che sono manifestamente illeciti e quei contenuti che non lo sono e che danno dunque adito a contestazione o a consultazioni nel merito degli stessi[42].

---

[40] G.G. CODIGLIONE, *La nuova legge tedesca per l'*enforcement *dei diritti sui social media*, in *Dir. inform.*, 2017, p. 728 ss.

[41] Il *NetzDG* dà una definizione di "contenuto illecito" richiamando alcune norme del codice penale tedesco, senza fornire dunque un'articolazione del suo significato.

[42] L'improntare tali procedure all'interno di uno schema strettamente legato alla cooperazione con le autorità è elemento imprescindibile per una corretta esecuzione di tali meccanismi. È importante infatti la presenza di un organismo terzo che abbia le competenze per valutare i contenuti oggetto di segnalazioni e che lavori dunque in stretta sinergia con gli ISP.

Per quanto riguarda l'esperienza italiana, infine, l'unica previsione riguardante i meccanismi di *notice and take down* è contenuta nella legge 29 maggio 2017 n. 71[43], che ha introdotto disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del *cyberbullismo*. Essa prevede, infatti, la possibilità per il minore ultraquattordicenne – o per il genitore ovvero per il soggetto responsabile –, vittima di uno degli illeciti riconducibili ex art. 1 c. 2 L. n. 71/2017 al *cyberbullismo,* di inoltrare al titolare del trattamento o al gestore del sito internet un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi altro dato personale del minore stesso diffuso in Internet.

Il meccanismo di segnalazione delineato dalla legge italiana presenta tuttavia alcuni limiti: in primo luogo esso riguarda esclusivamente i dati personali diffusi online che ledono la personalità dei minori[44] e, in secondo luogo, non viene scandito in modo dettagliato l'obbligo di rimozione a carico dell'ISP. Peraltro, in caso di mancata attivazione, gli ISP saranno sanzionabili solamente laddove non adempiano agli obblighi imposti dal Garante, adito successivamente dalla vittima[45], ex art. 170 D.lgs. n. 196/2003[46].

Un'ulteriore problematica è data dal raggio d'azione della legge. Essa infatti si rivolge al "gestore del sito internet", definito all'art. 1 c. 3 della legge sul *cyberbullismo* come il 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* (…)». Vengono pertanto esclusi dall'applicabilità della normativa in esame i *provider* che prestino servizi di *mere conduit, caching* e *hosting:* scelta discutibile considerando che pacificamente i gestori dei *social network* – con riferimento ai quali con più probabilità si potranno riscontrare le condotte illecite integranti le fattispecie incriminatrici rilevanti ex art. 1 c. 2 L. n. 71/2017 – sono da qualificare quali *hosting provider*[47].

Le considerazioni di cui sopra rivelano l'intento che persegue la legge sul *cyberbullismo,* la quale mira a disegnare una normativa che vuole affrontare tale fenomeno in via preventiva[48], piuttosto che attraverso una regolamentazione puntuale di sistemi rimediali e sanzionatori.

Dalla breve analisi dei recenti interventi normativi concernenti l'ordinamento tedesco e italiano, emerge un quadro eterogeneo e non armonizzato. Lo svilupparsi di legislazioni

---

[43] Si segnala anche il Disegno di Legge S.3001, presentato il 14 dicembre 2017 e in attesa di assegnazione, contenente «norme generali in materia di *social network* e per il contrasto della diffusione su internet di contenuti illeciti e delle *fake news*», proposto su iniziativa del Senatore Luigi Zanda, contro-firmatario Senatore Rosanna Filippin, il cui testo ripropone l'impianto della legge tedesca sopra esaminata.

[44] CODIGLIONE, *La nuova legge tedesca,* cit., p. 733.

[45] La legge n. 71/2017 non prevede un impianto sanzionatorio *ad hoc*, gli ISP non verranno dunque sanzionati laddove non rimuovano i contenuti segnalati entro le 24 ore dalla segnalazione, anche nel caso in cui si tratti di un contenuto manifestatamente illecito e lesivo per la dignità e la personalità del minore.

[46] INGRASSIA, *Responsabilità penale,* cit., p. 1628.

[47] M. SENOR, *Un primo commento alla legge sul cyberbullismo,* 30 settembre 2017, disponibile al sito www.medialaw.eu. Correttivo a tale esclusione potrebbe individuarsi nel ruolo del Garante per la protezione dei dati personali, la cui azione potrà rivolgersi nei confronti di tutte le tipologie di *provider*.

[48] P. PITTARO, *La legge sul cyberbullismo,* in *Fam. dir.*, 2017, 8-9, p. 819 ss.

diverse a livello nazionale non contribuisce certo all'uniformità delle procedure rimediali contro i contenuti illeciti presenti online, accrescendo invece il numero e la frammentarietà delle formalità che i *provider* devono seguire sulla base dell'ordinamento all'interno del quale operano. Circostanza che contrasta palesemente con la natura globale e sovranazionale di Internet e dei servizi che gli operatori gestiscono nel *Cyberspace*[49].

5. Prospettive *de jure condendo:* la difficile armonizzazione degli interessi e delle fonti.

Dall'analisi sopra svolta, emergono due esigenze di armonizzazione. La prima riguarda le diverse posizioni soggettive coinvolte nelle dinamiche della criminalità cibernetica, che si riflette nei meccanismi di segnalazione-rimozione che interessano *provider,* utenti e autorità. La seconda riguarda la multiformità delle attività e dei soggetti operanti nel *Cyberspace*, la quale rimanda alla diversità e frammentarietà delle fonti da cui scaturiscono le relative discipline in materia.

La natura nuova e articolata della realtà virtuale mette in discussione i parametri che tradizionalmente hanno regolato le dinamiche tra le diverse soggettività, rendendo sempre più difficoltoso il raggiungimento di un'equa e pacifica armonizzazione delle diverse istanze ed esigenze di tutela. Di qui il difficile bilanciamento tra i diritti e gli interessi facenti capo rispettivamente ai *provider*, alle vittime della criminalità cibernetica, agli utenti.

Circoscrivendo questa plurilaterale relazione all'ambito dei possibili meccanismi di segnalazione-rimozione, le posizioni che confliggono possono essere ricondotte al diritto alla libertà d'impresa del *provider*, che rimane pur sempre un soggetto privato al quale non può demandarsi una generale valutazione giuridica e qualitativa delle informazioni presenti online, pena il rischio di introdurre la inaccettabile figura definita, da più voci in dottrina, di un "censore privato"; i diritti soggettivi anche fondamentali delle vittime della criminalità nel *Cyberspace*, che vanno dai diritti della personalità a quelli patrimoniali e richiedono interventi immediati, nei casi più gravi, soprattutto quando vedano il coinvolgimento di minori; i diritti alla libera manifestazione del pensiero e all'informazione degli utenti del Web, che verrebbero inevitabilmente compromessi dall'introduzione di censori privati, i quali, nella logica di tutelare innanzitutto la propria attività economica, potrebbero rimuovere cautelativamente qualsiasi contenuto segnalato, per paura di incorrere in sanzioni anche penali o controversie giudiziali.

---

[49] COM(2017) 555 *final,* cit., dove si afferma che «attualmente nell'UE non esiste un approccio armonizzato e coerente alla rimozione dei contenuti illegali, bensì diversi approcci a seconda dello Stato membro, della categoria di contenuto o del tipo di piattaforma online. Un approccio più allineato renderebbe più efficace la lotta contro i contenuti illegali. Andrebbe inoltre a beneficio dello sviluppo del mercato unico digitale e ridurrebbe il costo della conformità a un gran numero di norme per le piattaforme online, anche per i nuovi operatori».

Il punto di equilibrio sembra da ricondurre, come rilevato dalla recente giurisprudenza italiana esaminata, in un sistema di controllo successivo, che potrebbe passare attraverso una regolamentazione dei meccanismi di *notice and take down*, da disciplinare rispettando alcuni principi essenziali, quali la certezza dei tempi e dei contenuti delle *notification*, la trasparenza e l'informazione agli utenti, la garanzia del contraddittorio, la collaborazione con le autorità e la responsabilizzazione degli utenti stessi.

Un'efficace diversificazione degli obblighi di rimozione potrebbe inoltre fondarsi sul grado di gravità e sulla tipologia dei contenuti illeciti segnalati[50] – come nel modello tedesco, che distingue se siano manifestatamente illeciti o meno – ovvero, come suggerito in dottrina, sulla natura del diritto che viene pregiudicato dalla condotta dannosa[51].

Per quanto riguarda l'ulteriore esigenza di armonizzazione segnalata, essa deve fare i conti con le diverse tipologie di servizi dei *provider* operanti in rete e con la pluralità delle condotte lesive, anche "atipiche". Occorrerebbero interventi ordinatori in materia, che cerchino di conciliare i diversi rimedi che stanno emergendo, per cui assieme ai meccanismi di *notice and take down* andrebbero disciplinati anche il diritto alla de-indicizzazione, da un lato, e il diritto alla cancellazione, dall'altro, in conformità alle previsioni del nuovo Regolamento europeo in materia di privacy 2016/679[52].

Inoltre, l'armonizzazione delle fonti e dei rimedi giuridici, per quanto debba partire da una base normativa di matrice sovranazionale e, quindi, in prima istanza europea, non potrà che essere integrata anche da componenti di auto-regolamentazione – come testimoniano le posizioni assunte più volte dalla Commissione europea e dal Consiglio d'Europa in materia – che sono imprescindibili data la natura fluida del

---

[50] Posizione che trae argomentazioni da quanto affermato nella sentenza della Corte d'Appello civile di Roma n. 1065/2018 sopra richiamata (nota n. 29). La ragione del richiedere che il contenuto della *notice* sia preciso e specifico risiede proprio nella difficoltà di qualificare quale lesivo il contenuto segnalato in alcune fattispecie concrete. Il caso di specie concerneva infatti un'ipotesi di diffamazione online, difficilmente riscontrabile in alcuni casi, e secondo i giudici «in virtù della difficoltà di individuazione dell'illiceità del contenuto occorre una diffida molto più dettagliata e sostenuta da un minimo di elementi probatori». Nella sentenza di legge inoltre che «i contenuti non apparivano di per sé ingiuriosi tanto da attivare un obbligo di rimozione del *provider,* anche indipendentemente dall'assenza di un ordine del giudice», elemento che conduce ad ulteriori quesiti. Tra questi se possa appunto essere una soluzione la previsione di una differenziazione tra contenuti manifestamente illeciti, di fronte ai quali il *provider* deve agire con la rimozione autonomamente non appena ne venga a conoscenza; e contenuti di difficile interpretazione, la cui rimozione deve obbligatoriamente passare preventivamente per l'Autorità.

[51] Come suggerito da BOCCHINI, *Responsabilità dell'*hosting provider, cit., p. 637, il quale sostiene, distinguendo tra diritti della personalità e diritti patrimoniali, che «sembra potersi avanzare più di un dubbio rispetto al potere dell'ISP di rimuovere contenuti illeciti laddove questi siano lesivi di diritti patrimoniali».

[52] Sul diritto alla de-indicizzazione, il diritto all'oblio e alla cancellazione cfr. 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, 6, p. 2100 ss.; S. MARTINELLI, *Diritto all'oblio e motori di ricerca: il bilanciamento tra memoria e oblio in Internet e le problematiche poste dalla de-indicizzazione,* in *Dir. inform.*, 2017, 3, p. 565 ss.; G.M. RICCIO, *Il difficile equilibrio tra diritto all'oblio e diritto di cronaca,* in *Nuova giur. civ. comm.*, 2017, 4, p. 549 ss.; SICA – D'ANTONIO, *La procedura di de-indicizzazione,* cit., p. 703 ss.

Cyberspace, il quale non si presta ad essere rigidamente ed esaustivamente disciplinato attraverso gli strumenti e gli schemi del solo diritto pubblico.