

GIOVANNA D'ALFONSO*

*La procedura di «notice and take down» e la responsabilità civile
dell'hosting provider. Prospettive comparative e riflessioni critiche
per un intervento armonizzante di hard law ***

Sommario: 1. Interpretazione evolutiva della regolamentazione europea sulla responsabilità civile dei 'fornitori di ospitalità. L'elaborazione pretoria della figura «atipica» dell'«hosting attivo». - 2. La procedura di «notice and take down» tra ambiguità definitorie della c.d. «direttiva sul commercio elettronico» e le distinte soluzioni degli Stati membri. Una comparazione con altri ordinamenti. - 3. La procedura di «notice and take down» nel nostro sistema e la sua applicazione giurisprudenziale al caso concreto. - 4. Le spinte in ambito europeo verso l'adozione di meccanismi di «notice and take down». La portata dell'incisività degli atti di soft law e la necessità di una riforma sistematica.

1. Interpretazione evolutiva della regolamentazione europea sulla responsabilità civile dei 'fornitori di ospitalità. L'elaborazione pretoria della figura «atipica» dell'«hosting attivo»

La disciplina europea e di diritto interno, in materia di responsabilità civile degli *hosting providers* per i danni arrecati a terzi dai contenuti illeciti pubblicati dagli utenti dei portali digitali da loro gestiti, ha sollevato problematiche di non poco momento per vari ordini di ragioni, tra i quali il carattere obsoleto di talune disposizioni, dovuto al mancato adeguamento delle stesse a seguito di rilevanti innovazioni tecnologiche, e le ambiguità definitorie.

In tale cornice, l'interpretazione dottrinale¹ e giurisprudenziale² hanno esercitato un ruolo decisivo e, senza dubbio, le soluzioni applicative prospettate dal formante dottrinale

* *Professoressa Associata di Diritto privato presso l'Università degli Studi della Campania "Luigi Vanvitelli".*

** *Contributo sottoposto positivamente al referaggio secondo le regole del double blind peer-review.*

¹ Sul ruolo della dottrina nell'interpretazione delle norme, alla luce e nel rispetto del principio di legalità costituzionale, cfr. P. PERLINGIERI, *La dottrina del diritto civile nella legalità costituzionale*, in *Rass.dir.civ.* 2007, p. 497 ss.

hanno indirizzato orientamenti giurisprudenziali che, inizialmente minoritari, si sono col tempo consolidati.

Si procederà alla disamina dell'evoluzione delle decisioni giurisprudenziali che, in linea con un autorevole insegnamento dottrinale, hanno operato un'interpretazione *evolutiva* della disciplina vigente, ponendosi in un'ottica sistematica ed assiologica³. Le corti si sono pronunciate in ordine all'applicabilità della normativa europea a tutte quelle figure emergenti di prestatori di servizi di *internet*⁴ che si sono gradualmente caratterizzate per l'innovatività

² Come osservato da autorevole dottrina, l'interpretazione non è soltanto la ricerca di un'autonoma e presunta verità del dato normativo, ma deve essere riferita ad un contesto che è la realtà esterna. L'ermeneutica (la teoria dell'interpretazione) rivela il collegamento essenziale tra l'interpretazione e la realtà (sul punto cfr. P. PERLINGIERI e P. FEMIA, *Diritto positivo come diritto interpretato*, in P. PERLINGIERI (a cura di), *Manuale di diritto civile*, Napoli, 2014, p. 111). L'interpretazione della norma non va prospettata in astratto, ma in relazione ad un fatto concreto, valutato nella sua peculiarità ed avendo riguardo al momento storico dell'emanazione ed a quello dell'applicazione della norma, considerando che l'inevitabile sopravvenire della discontinuità, nella *societas*, incide sulle modalità attuative della stessa (cfr. P. PERLINGIERI, *Applicazione e controllo nell'interpretazione giuridica*, in *Riv.dir.civ.*, 2010, p. 307 ss.). La dottrina precisa come la trasformazione del sistema delle fonti imponga un corrispondente mutamento della teoria dell'interpretazione, laddove le sue regole debbano essere adeguate al mutato quadro del sistema giuridico, caratterizzato dalla presenza della Costituzione e del diritto dell'Unione Europea. Nel rispetto del principio di legalità, la norma deve, dunque, essere posta in «relazione dialogica» con il fatto da regolare e l'interpretazione di una disposizione è il risultato del coordinamento con le altre norme dell'ordinamento giuridico e dell'armonizzazione con i principi costituzionali. Si supera, di conseguenza, in tal modo, la tecnica della «sussunzione», in quanto il fatto non può più essere «meccanicamente incasellato» in una determinata fattispecie astratta che, molte volte, non è neanche rinvenibile. Al fine di individuare la disciplina «più adeguata» al caso concreto, il fatto dovrà essere valutato, prendendo in considerazione gli interessi ed i valori che esprime, avendo riguardo al contesto storico-giuridico di riferimento. L'interprete ha, in definitiva, il compito non di garantire il rispetto della lettera della norma, quanto diversamente di individuare ed applicare al caso concreto la disciplina «più adeguata», operando un bilanciamento degli interessi e dei principi e dei valori normativi che i fatti concreti, oggetto di attenzione, esprimano. Per tali riflessioni, cfr. P. PERLINGIERI (*Interpretazione ed evoluzione dell'ordinamento*, *Riv.dir.priv.*, 2011, p. 160 ss.) che, ponendosi in posizione critica verso l'orientamento che identifica l'interpretazione nell'analisi del linguaggio, rinvia alle argomentazioni di E. BETTI, *Teoria generale della interpretazione*, II, Milano, 1955, p. 797 ss. Sull'operazione giudiziale di bilanciamento, cfr. P. PERLINGIERI, *Formazione dei giudici e Scuola superiore della magistratura*, in *Giust.proc.civ.*, 2007, p. 313, che afferma che il «bilanciamento degli interessi e dei valori, ragionevolezza, adeguatezza, proporzionalità, valenza dei principi sono canoni ermeneutici (...) che, come tali, contribuiscono (insieme) al ridimensionamento di vecchi brocardi, duri a morire, come *in claris non fit interpretatio* e *dura lex sed lex*, che dovranno essere (...) conformi alla legalità costituzionale ed europea». Sulla «ragionevolezza» quale «canone ermeneutico ed argomentativo», «filo conduttore» di ogni ragionamento giuridico, per il contenimento di principi ed interessi, in coerenza col sistema giuridico di riferimento e tutti i suoi valori, cfr. G. PERLINGIERI, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015, pp. 16-29, p. 43, p. 135. Sul tema si v. P. PERLINGIERI, «Principi generali» e «interpretazione integrativa» nelle pagine di Emilio Betti, in *Rass.dir.civ.*, 2019, p. 105 ss; P. FEMIA, *Valori normativi e individuazione della disciplina applicabile*, in *Aa.Vv.*, *Temi e problemi della civilistica contemporanea*, Napoli, 2005, p. 521 ss.

³ Sul punto cfr. P. PERLINGIERI, *Interpretazione sistematica e assiologica, situazioni soggettive e rapporto giuridico*, Napoli, 2006, *passim*, ID., *Il «giusto rimedio nel diritto civile»*, in *Giusto proc. civ.*, 2011, p. 3 ss.

⁴ O meglio i prestatori che, operando nella società dell'informazione, offrono liberamente servizi di connessione, trasmissione e memorizzazione di dati. Tali soggetti sono comunemente definiti «intermediari di servizi», giacché forniscono un collegamento tra coloro che vogliono comunicare un'informazione ed i loro desti-

delle funzioni svolte, rispetto a quelle già individuate dalla direttiva 2000/31/CE del Parlamento europeo e del Consiglio⁵, c.d. «direttiva sul commercio elettronico». Le Corti hanno dovuto anche affrontare ulteriori questioni che si sono poste per l'assenza di chiarezza di certe regole che hanno condotto ad ambiguità definitorie in merito a numerose locuzioni, in particolare in relazione a quelle relative alla procedura di «*notice and take down*»⁶.

Avendo riguardo al primo profilo menzionato, si osservi innanzitutto che la direttiva europea, nel regolamentare (agli artt. 12-16) la responsabilità civile degli *internet service providers*, li ha classificati in tre categorie, prevedendo distinti regimi di responsabilità⁷.

Nell'effettuare la tripartizione, il legislatore europeo ha preso in considerazione gli operatori maggiormente noti nell'esperienza concreta in quel determinato momento storico (quasi venti anni or sono) in relazione alle loro caratteristiche, ai servizi forniti ed al ruolo più o meno passivo assunto nel processo di trasmissione o diffusione dei dati in rete⁸. Più precisamente, la direttiva 2000/31/CE ha qualificato la posizione giuridica del *mere conduit*

natari. Cfr. 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 *Riv.dir.ind.*, 2017, p. 57.

⁵ «Relativa a taluni aspetti giuridici della società dell'informazione, in particolare il commercio elettronico, nel mercato interno». Per V. ZENO-ZENCOVICH (*La libertà di espressione. Media, mercati, potere della società dell'informazione*, Bologna, 2004, *passim*) si dovrebbe più opportunamente parlare, piuttosto che di «società dell'informazione», di «società della conoscenza». Sulle dimensioni etiche della società dell'informazione, si v. P. COSTANZO, *Osservazioni sparse su nodi, legami e regole su internet*, in P. PASSAGLIA, D. POLETTI (a cura di), *Nodi virtuali, legami informali: internet alla ricerca di regole*, Pisa, 2017, p. 28. Si v. R. PETRUSO, *La responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, Torino, 2019, p. 134, che evidenzia come la regolamentazione delle responsabilità degli *internet providers* ponga al centro dell'attenzione la disciplina dell'informazione che rappresenta, come noto, uno dei beni più importanti della società dell'informazione.

⁶ A. QUARTA, *La responsabilità civile*, in A. QUARTA, G. SMORTO (a cura di), *Diritto privato dei mercati digitali*, 2020, p. 286, rimarca come almeno tre elementi che caratterizzano l'attività di intermediazione della rete abbiano provocato un'interpretazione evolutiva del regime speciale della responsabilità: l'attività dell'*hosting provider* che ha assunto, nel tempo, carattere attivo; la segnalazione dei contenuti illeciti da parte dei privati e la circostanza che le piattaforme utilizzino sistemi automatizzati per filtrare i contenuti illeciti.

⁷ Per un commento all'articolata disciplina della responsabilità civile delle tre distinte figure di *Internet service providers* cfr., *ex multis*, G.M. RICCIO, *La responsabilità civile degli internet service providers*, Torino, 2002, p. 57 ss.; G. PONZANELLI, *Verso un diritto uniforme per la responsabilità degli internet service providers*, in *Danno resp.*, 2002, p. 5 ss.; 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*, Milano, 2002, p. 195 ss.; F. DI CIOMMO, *Evoluzione tecnologica e regole di responsabilità civile*, Napoli, 2003, *passim*; R. BOCCHINI, *La responsabilità civile degli intermediari del commercio elettronico. Contributo allo studio dell'illecito plurisoggettivo permanente*, Napoli, 2003, *passim*; A. MANTELERO, *La responsabilità degli intermediari di rete nella giurisprudenza italiana alla luce del modello statunitense e di quello comunitario*, in *Contr. impr./Eur.*, 2010, p. 529 ss. Da ultimo, si v. R. PETRUSO, *Le responsabilità degli intermediari*, cit., che analizza, in chiave comparativa, la disciplina europea, incentrando l'attenzione sulle evoluzioni ordinamentali, anche extraeuropee, in termini di responsabilità, dell'attività degli *internet service providers*.

⁸ Cfr. M. GAMBINI, *Gli hosting providers tra i doveri di diligenza professionale e assenza di un obbligo generale di sorveglianza sulle informazioni memorizzate*, in *www.costituzionalismo.it*, 2011, fasc. 2, p. 6.

provider (art. 12) che svolge l'attività di («semplice trasporto») fornire l'accesso alla rete o di trasmettere su una rete di comunicazione informazioni date dal destinatario del servizio; la figura del *caching provider* (*ex art. 13*) che, nell'eseguire la funzione di trasmissione su una rete di comunicazione di informazioni fornite dall'utente del servizio, svolge una memorizzazione automatica, intermedia e temporanea al solo fine di rendere i dati immediatamente disponibili per il recupero che l'utente ne voglia effettuare; infine, la figura dell'*hosting provider* (*ex art. 14*) che si obbliga a locare uno spazio di memoria sul proprio *server* e fornisce la specifica attività di memorizzazione duratura, su tale spazio, delle informazioni provenienti dai destinatari dei servizi.

Orbene, nel dettare la disciplina della responsabilità civile degli *internet service providers*, il legislatore europeo ha fissato delle regole che superassero le divergenze tra le normative e le giurisprudenze nazionali (considerando n. 40 della direttiva 2000/31/CE), prefiggendosi l'obiettivo di promuovere la libera circolazione dei servizi della società dell'informazione all'interno del mercato telematico allora nascente ed, in tal guisa, di garantirne il buon funzionamento. A tal uopo, si è fatta una scelta di politica del diritto al fine di raggiungere un «punto di equilibrio tra i vari interessi in gioco» (considerando 41 della direttiva 2000/31/CE) dei fornitori dei servizi dell'informazione e dei loro destinatari⁹.

La direttiva suddetta ha, così, optato per una soluzione intermedia tra le due opposte: l'esclusione della responsabilità civile dei *providers* e la previsione di criteri di imputazione della medesima troppo rigorosi¹⁰.

La *ratio* ispiratrice della normativa parte dal convincimento che gravare gli intermediari della rete di obblighi di diligenza eccessiva nell'erogazione del servizio avrebbe penalizzato in modo sproporzionato la loro posizione, caricandoli di costi di oneri tecnici (si

⁹ Sul punto cfr. M. GAMBINI, *Gli hosting providers*, cit., p. 2.

¹⁰ Cfr. G. PONZANELLI, *Verso un diritto uniforme*, cit., p. 9 s., ove sottolinea come la scelta europea del regime di limitazione della responsabilità a favore degli *internet service providers* sia stata dettata dall'esigenza di evitare una nuova ipotesi di responsabilità oggettiva. Nel condividere tale opzione, si precisa che l'utilizzo della regola di diligenza, quale criterio di valutazione della condotta del *provider*, evita gli effetti gravosi dell'inversione dell'onere della prova, propria del modello della responsabilità oggettiva che oltretutto potrebbe provocare le patologie di *overdeterrence*, e rappresenta, per tale ragione, «uno strumento flessibile ed equilibrato, ben più della regola dell'imputazione oggettiva della responsabilità». Sull'opportunità della scelta del legislatore europeo di evitare di assoggettare i gestori dei portali a modelli di responsabilità oggettiva o per rischio d'impresa, così come a modelli di responsabilità aggravata, sulla falsariga della regola accolta dall'art. 2050 c.c., in materia di attività pericolosa, si v. L. NIVARRA, *La responsabilità degli intermediari*, in *Ann. it. dir. aut.*, 2002, p. 37 ss.

pensi ai sistemi di filtraggio), per evitare e prevenire la commissione di illeciti. Ciò sarebbe equivalsa a paralizzare o quantomeno a porre dei freni all'attività imprenditoriale in via di sviluppo al momento dell'emanazione della direttiva¹¹ - correndosi, tra l'altro, il rischio di alimentare nel mercato oligopoli degli operatori economicamente più forti. Inoltre, si è considerato che un riconoscimento generalizzato della responsabilità civile degli *internet service providers* avrebbe implicato una limitazione della libertà di manifestazione del pensiero degli utenti di *internet*, poiché i primi, in particolar modo gli *hosting providers*, per evitare il rischio di incorrere nella responsabilità civile, sarebbero stati indotti a censurare i contenuti di utenti potenzialmente lesivi di diritti di terzi¹².

In tale prospettiva, la normativa ha introdotto, all'art. 15 (recepito, nel nostro ordinamento, dall'art. 17, comma 1, d.lgs. 9 aprile 2003, n. 70), il principio generale¹³ in forza del quale non grava in capo a nessuno degli intermediari della rete l'obbligo generale di sorveglianza delle informazioni che trasmettono o memorizzano, né un obbligo generale di ricerca attiva di fatti o circostanze che indichino la presenza di attività illecite. Qualora lo Stato membro lo imponga - come, nel nostro ordinamento, l'art. 17, comma 2, d. lgs. 2003/70 -, la direttiva 2000/31/CE non dispensa tuttavia tali soggetti dall'obbligo di informare prontamente le autorità pubbliche su eventuali presunte attività o materiali illeciti degli utenti dei loro servizi di cui vengano a conoscenza; né dall'obbligo di fornire, a richiesta delle autorità competenti, le informazioni in loro possesso che consentano l'identificazione del destinatario del servizio.

Dalla mancata previsione di un obbligo di sorveglianza si è fatta conseguire l'esclusione della responsabilità dell'*internet service provider*¹⁴ per le informazioni trasmesse o memorizzate e le operazioni compiute dall'utente del servizio, purché il primo non intervenga in alcuna modalità sul contenuto o sullo svolgimento delle stesse. Tale regime speciale si differenzia, di fatto, dalle regole generali sulla responsabilità civile, in quanto la sua applicazione determina l'esonero di responsabilità del *provider*, nel caso in cui sussistano le condizioni ivi previste: il fornitore del servizio *on line* non è obbligato a conoscere le infor-

¹¹ Cfr. G.M. RICCIO, *Anonimato e responsabilità in internet*, in *Dir.inf.*, 2000, p. 335.

¹² Cfr. M. GAMBINI, *Gli hosting providers*, cit., p. 2; G. PONZANELLI, *Verso un diritto uniforme*, cit., p. 8.

¹³ Cfr. M. ZARRO, *La tutela della reputazione digitale quale «intangibile asset»*, in *Rass.dir.civ.*, 2017, p. 1521.

¹⁴ Per le considerazioni che seguono cfr. L. VIZZONI, *Recensioni non genuine su Tripadvisor; quali responsabilità?*, in *Resp.civ.prev.*, 2018, p. 710 s.

mazioni trasmesse o memorizzate e non risponderà della loro illiceità, se non ne conosca il contenuto. Sarà, quindi, responsabile solamente quando, pur essendo a conoscenza dell'illecito, non faccia nulla per prevenirlo e/o evitarlo, tenendo, in tal modo, una condotta non diligente¹⁵.

La disciplina speciale statuisce, in sostanza, un «regime di favore» per l'*internet service provider*, fondando la sua responsabilità civile sul criterio di imputazione della colpa, per violazione del dovere di diligenza professionale¹⁶.

In riferimento alla responsabilità civile dell'*hosting provider*, il d. lgs. 2003/70 statuisce un principio di non responsabilità delle informazioni memorizzate che viene meno: qualora costui sia effettivamente a conoscenza del fatto che l'attività oppure l'informazione è illecita e, per quanto riguarda le azioni risarcitorie, sia al corrente di fatti o circostanze che rendano «manifesta» l'illiceità dell'attività e dell'informazione (art. 16, comma 1, lett. a)); non appena a conoscenza di tali fatti¹⁷, non agisca prontamente per rimuovere le informazioni oppure per disabilitarne l'accesso (art. 16, comma 1, lett. b)) oppure se, ai sensi dell'art. 17, comma 2, lett. b), informato di fatti o circostanze che rendano manifesto il carattere illecito o pregiudizievole per qualcuno dell'attività o dell'informazione, non si attivi per informare l'autorità competente¹⁸. Ai fini della responsabilità civile dell'*hosting provider*, si impone la valutazione della «colpa per negligenza», a fronte dell'allegazione della conoscenza sostanziale di attività o informazioni illecite oppure di fatti o circostanze che rendano l'illiceità dell'attività o dell'informazione manifesta; tutto ciò non comporta tuttavia l'attivazione del *provider* nel controllare i contenuti memorizzati, salvo che vi sia una specifica segnalazione da parte «delle autorità competenti»¹⁹.

¹⁵ Cfr. G. PONZANELLI, *Verso un diritto uniforme*, cit., p. 8.

¹⁶ Cfr. M. ZARRO, *La tutela della reputazione digitale*, cit., p. 1521. R. PETRUSO, *Le responsabilità degli intermediari*, cit., p. 135, parla di «confini mobili» della direttiva 2000/31/CE che detta, per l'appunto, una regolamentazione solo «minima» della responsabilità degli intermediari della rete.

¹⁷ «Su comunicazione delle autorità competenti».

¹⁸ L'art. 16, comma 3, d.lgs. 2003/70, prevede che l'autorità giudiziaria o quella amministrativa competente possa esigere, anche in via d'urgenza, che l'*hosting provider*, nell'esercizio delle proprie attività, impedisca oppure ponga fine alle violazioni commesse. Sulla tutela inibitoria, nell'interpretazione della Corte di Giustizia dell'Unione Europea, e sulla tutela preventiva e specifica nel diritto nazionale, con particolare riferimento agli ordini inibitori nell'esperienza giuridica francese ed italiana, si v. R. PETRUSO, *Le responsabilità degli intermediari*, cit., pp. 193 ss., 204 ss., 218 ss.

¹⁹ Cfr. M. COCUCCIO, *La responsabilità civile per fatto illecito dell'internet service provider*, in *Resp. civ. prev.*, 2015, p. 1319.

Esiste, pertanto, per tale figura di *provider*²⁰ una «generale esenzione di responsabilità» che non si applicherà, però, qualora, pur essendo a conoscenza di fatti illeciti, non intervenga immediatamente, in conformità a quanto previsto dal legislatore²¹.

In ogni caso, l'*hosting provider* potrà beneficiare dei limiti della responsabilità, ai sensi dell'art. 14 della direttiva 2000/31/CE, in linea con quanto previsto dal considerando 42 della medesima, unicamente quando si connoti per lo svolgimento di un'attività «neutra» o

²⁰ Avendo riguardo all'attività del *provider* di *mere conduit*, l'art. 14, d.lgs. 2003/70 statuisce che costui non sarà responsabile delle informazioni trasmesse, purché non dia origine alla loro trasmissione, non le selezioni, né le modifiche e non selezioni il destinatario. In sostanza, il *provider* sarà responsabile solo qualora produca il contenuto, selezioni i destinatari e/o compia altre operazioni di filtraggio: ciò vuol dire che l'esonero della responsabilità dipende dalla circostanza che lo stesso abbia una posizione di «assoluta neutralità rispetto all'informazione veicolata». Per quanto concerne la figura del *caching provider*, l'art. 15, d.lgs. 2003/70 stabilisce che, nel prestare il servizio della società dell'informazione, consistente nel trasmettere su una rete di comunicazione le informazioni conferite da parte del destinatario del servizio, il fornitore del servizio non è responsabile della memorizzazione automatica, intermedia e temporanea, effettuata al solo fine di rendere più efficace il successivo inoltramento ad altri destinatari, a condizione che: non modifichi le informazioni; si conformi alle loro condizioni di accesso ed alle loro norme di aggiornamento che siano indicate in modo ampiamente riconosciuto ed impiegato dalle imprese del settore; non interferisca con l'uso lecito di una tecnologia che sia diffusamente riconosciuta ed utilizzata nel settore, allo scopo di ottenere dati sull'impiego delle informazioni. Inoltre la responsabilità del *provider* sarà esclusa unicamente qualora agisca «prontamente» per rimuovere le informazioni che abbia memorizzato oppure per disabilitare l'accesso alle stesse, «non appena» venga «effettivamente» a conoscenza della circostanza che le informazioni siano state rimosse dal luogo in cui si trovavano inizialmente sulla rete o che l'accesso alle stesse sia stato disabilitato oppure che l'autorità giudiziaria oppure amministrativa ne abbia disposto la rimozione o la disabilitazione. Dalla lettera delle disposizioni menzionate, appare evidente come il regime di *favor* legislativo, previsto per il *caching provider*, sia più limitato rispetto a quello statuito per il *mere conduit provider*, laddove il primo dovrà osservare una serie di condizioni più stringenti, per essere esonerato dalla responsabilità rispetto ai terzi. Per tali osservazioni, cfr. M. COCUCIO, *La responsabilità civile*, cit., pp. 1316-1318. La ragione del differente regime di responsabilità è, senza dubbio, da ricercarsi nel differente livello di «passività», ossia di neutralità, delle due categorie di intermediari della rete. Difatti, se, per un verso, i *mere conduit providers* trasportano enormi quantità di dati per destinatari che nemmeno conoscono e si prevede, perciò, che svolgano un ruolo strettamente passivo; differentemente, i *caching providers* possono essere coinvolti più *attivamente* nei confronti dei loro utenti, in quanto è loro permesso di selezionare i dati o il destinatario del servizio - anche se non è loro consentito di modificare la copia locale dei dati memorizzati. In sostanza, la possibilità di selezionare i dati o il destinatario è una «caratteristica chiave» di un fornitore di *caching* che potrebbe voler limitare l'accesso ai propri servizi o che potrebbe voler filtrare le informazioni messe a disposizione dei propri utenti. Sul punto cfr. *EU Study on the Legal analysis of a Single Market for the information society. New rules for a new age? 6. Liability of online intermediaries*, in ec.europa.eu › newsroom › document, November 2009, p. 8.

²¹ Come dichiarato nell'ordinanza Trib. Roma, 20 ottobre 2011, in www.leggioggi.it, l'*hosting provider* non sarà responsabile, se non quando venga a conoscenza e non intervenga, secondo le modalità previste dal legislatore, proprio in ragione della circostanza che non sussiste, in via generale, in capo a costui né l'obbligo generale di sorveglianza, né l'obbligo di ricerca attiva su fatti e circostanze che indichino la presenza di attività illecite. Si specifichi (cfr. M. COCUCIO, *La responsabilità civile*, cit., p. 1319) che, ai sensi dell'art. 16, comma 2, d.lgs. 2003/70, oggetto di attenzione, l'esenzione non si applica, qualora il destinatario del servizio agisca sotto l'autorità o il controllo del prestatore; l'*hosting provider* risponderà per fatto illecito altrui, ex art. 2049 c.c., in concorso con l'autore del medesimo, nei casi in cui quest'ultimo, agendo sotto il controllo dell'organizzazione aziendale del primo, ponga in essere attività che ledano diritti dei terzi.

meglio per un ruolo «meramente tecnico, automatico e passivo» che implica che il prestatore di servizi non conosca e non controlli le informazioni immesse e memorizzate in rete²².

Ciò posto, a fronte di tale quadro normativo, la giurisprudenza si è trovata a dover affrontare la questione se siano tuttora riconducibili alla figura del fornitore di ospitalità, tipizzata dalla direttiva europea venti anni or sono, gli *hosting providers* le cui attività siano, nel corso del tempo, divenute assai più ampie e variegate, in ragione dell'evoluzione tecnologica²³. Si è incentrata l'attenzione²⁴ precipuamente sui servizi offerti dai motori di ricerca

²² In tal senso si è sviluppato l'indirizzo, ormai consolidato, della Corte di Giustizia dell'Unione Europea. Sul punto si v. R. PETRUSO, *Le responsabilità degli intermediari*, cit., p. 152 ss. Famoso è il *leading case* della Corte giust. (Grande sezione), 23 marzo 2010 (domande di pronuncia pregiudiziale, proposte dalla *Cour de Cassation* - Francia), cause riunite da c. 236/08 a c. -238/08, *Google France SARL e Google Inc. c. Louis Vuitton Malletier SA* (c. 236/08), *Google France SARL c. Viaticum SA e Luteciel SARL* (c. 237/08), *Google France SARL c. Centre National de recherche en relations humaines (CNRRH) SAR, Pierre Alexis Thonet, Bruno Raboin e Tiger SARL* (c. 238/08) – citata in T. SCANNICCHIO, N.A. VECCHIO, *I limiti della neutralità: la Corte di giustizia e l'eterno ritorno dell'hosting attivo*, in *www.filodiritto.it*, 17 gennaio 2018, nt. 2. In tale decisione, la Corte, in via di interpretazione del considerando 42 della direttiva - secondo il quale i limiti di responsabilità, previsti dagli artt. 12-14 della direttiva, sono applicabili alla sola condizione che il *provider* non svolga un «ruolo attivo» che gli consentirebbe la conoscenza ed il controllo dei dati forniti dai suoi clienti-, definisce tale criterio, precisando che l'attività di *mera* «ospitalità», dallo stesso svolta, sussiste unicamente qualora non ricopra «un ruolo attivo che gli consenta la conoscenza o il controllo dei dati memorizzati». Allineandosi a tali argomentazioni, si v. anche la celebre sentenza della Corte giust., 12 luglio 2011, c. 324/09, *l'Oréal SA e altri c. eBay International AG*, in *Ann. it. dir. aut.*, 2011, p. 480 ss., con nota di J.B. NORDEMANN, *Liability of Social Networks for IP Infringements (Latest News): The Eu Law Regime after l'Oréal/eBay*, la pronuncia Corte giust., 7 agosto 2018, c. 521-17, *Coöperatieve Vereniging SNB-React U.A. c. D.M.*, in T. SCANNICCHIO, N.A. VECCHIO, *I limiti della neutralità*, cit.) che afferma la piena responsabilità degli *hosting providers* che svolgano un ruolo attivo, permettendo ai propri clienti l'ottimizzazione della loro attività di vendita *online*. Si v. la decisione della Corte giust., 14 giugno 2018, c. 610/15, *Stichting Brein c. Ziggo BV e XS4All Internet BV* che sottolinea come, a seguito dell'evoluzione tecnologica, il ruolo dell'intermediario della rete non si limiti più alla funzione di «mero trasportatore di informazioni *online*», delineando, in capo a costui, il dovere di attivarsi per la tutela dei diritti della persona nel *web*. Sul punto cfr. S. SCUDERI, *La responsabilità dell'internet service provider alla luce della giurisprudenza della Corte di Giustizia Europea*, causa c-610/15, 14 giugno 2018, in *Diritto Mercato Tecnologia*, 20 luglio 2018. In materia di diffamazione *on line*, si v. la sentenza Corte giust., 11 settembre 2014, c. 291/13, *Sotiris Pappasavvas c. O Fileleftheros Dimosia Etaireia Ltd., Takis Kounnafi, Giorgio Sertis*, in cui il ricorrente lamentava un danno subito, a seguito della pubblicazione di taluni articoli diffamatori sul sito *internet* di un quotidiano, con la quale la Corte ha dichiarato l'inapplicabilità della disciplina europea di esonero della responsabilità civile del *provider*, sostenendo che la casa editrice aveva pubblicato la versione *online* di un giornale ed era, dunque, a conoscenza delle informazioni, esercitando sulle stesse un controllo – cfr. E. TOSI, *Contrasti giurisprudenziali*, cit., p. 63, nt. 17.

²³ Circostanza che induce a riflettere sulla necessità della rivisitazione della disciplina della direttiva, la cui redazione risale a quasi un ventennio fa e risulta essere non più attuale. In tal senso, *ex multis*, cfr. F. DI CIOMMO, *Programmi di filtro e criteri di imputazione/esonero della responsabilità on line. A proposito della sentenza Google/Vivi Down*, in *Dir. inf.*, 2010, p. 474; L. BUGIOLACCHI, *(Dis)orientamenti giurisprudenziali in tema di responsabilità degli internet provider (ovvero del difficile rapporto tra assenza di obblighi di controllo e conoscenza dell'illecito)*, in *Riv. dir. ind.*, 2010, p. 328; G. FINOCCHIARO, *Due recenti decisioni giurisprudenziali inducono a riflettere sul tema della responsabilità della Rete*, in *www.blog-studiolegalefinocchiaro.it*.

²⁴ Per le notazioni che seguono cfr. E. TOSI, *Contrasti giurisprudenziali*, cit., p. 84 ss.

(come, a titolo esemplificativo, *Google*), dai *social network* (come *Facebook*) e dagli aggregatori di contenuti pubblicati da terzi, i c.dd. *user generated content* (come, ad esempio, *Youtube*).

La giurisprudenza²⁵ ha evidenziato come tali prestatori di servizi *on line* svolgano attività di indicizzazione, selezione, organizzazione e filtraggio di contenuti digitali diffusi in rete, al fine conseguire utili d'impresa (tramite la raccolta pubblicitaria), puntualizzando che esse costituiscono, in realtà, «indici rivelatori di un'attività di interferenza» degli operatori sui contenuti pubblicati dagli utenti sulle piattaforme digitali, in quanto i primi finiscono con l'avere un, seppur minimo, grado di “consapevolezza” degli stessi.

Successivamente le corti sono pervenute alla conclusione che, non potendosi considerare codeste attività degli *hosting providers* meramente automatizzate e passive, tali soggetti debbano essere ascritti ad nuova categoria “più evoluta” e distinta da quella “tipica” prevista dal legislatore²⁶, con la conseguenza dell'esclusione dell'operatività delle deroghe fissate dalla disciplina europea ed italiana.

Un filone giurisprudenziale²⁷ ha, così, forgiato la nuova figura soggettiva «atipica» di fornitore dei servizi *on line*, il c.d. «*hosting attivo*», sostenendo che debba essere sottoposto al regime generale della responsabilità civile aquiliana²⁸.

Tale posizione, sebbene sia stata oggetto di critiche dottrinali²⁹ ed abbia subito battute d'arresto, in ragione dello svilupparsi di un diverso orientamento che ha, all'opposto, ne-

²⁵ Sul punto, cfr. E. Tosi, *Contrasti giurisprudenziali*, cit., p. 63. Si v. anche R. GELLI, *False recensioni su TripAdvisor: accolta l'azione inibitoria promossa dal ristoratore diffamato*, in *Corr. giur.*, 2016, p. 89, secondo il quale, in tali ipotesi, il fornitore di servizi informatici diventerebbe «in una certa misura, *dominus* dei contenuti caricati sul sito».

²⁶ In tal senso, cfr. R. GELLI, *False recensioni*, cit., p. 90.

²⁷ Il dibattito giurisprudenziale e dottrinale sulla questione è stato aperto dal noto «*leading case*» RTI c. *Yahoo*, sul quale si è pronunciato il Trib. Milano, sez.spec.prop.ind. e intellettuale, il 9 settembre 2011, n. 10893, segnando, per la prima volta, l'elaborazione della figura dell'«*hosting attivo*» (pronuncia pubblicata in *Riv. dir. ind.*, 2012, p. 364 ss., con nota di A. SARACENO, *Note in tema di violazione del diritto d'autore tramite Internet; la responsabilità degli Internet service provider*). Nei gradi processuali successivi, se, per un verso, la Corte App. Milano, sez. impr., 7 gennaio 2015, n. 29 aveva riformato la decisione del Tribunale di Milano, puntualizzando che tutti gli *hosting provider* beneficerebbero dell'esenzione di responsabilità, quando non siano a conoscenza diretta del contenuto caricato dell'utente (pubblicata in *Dir. ind.*, 2016, p. 166 ss., con nota di M. IASELLI, *Caso Yahoo! Video: la Corte di Appello di Milano non vede responsabilità nell'operato dell'internet provider*); diversamente, di recente, la Cass., I sez., 19 marzo 2019, n. 7708, cit., ha riconosciuto la distinzione tra *hosting* passivi ed attivi, cassando con rinvio la sentenza della Corte d'Appello stessa. Per un commento, cfr. F. FRIGERIO, *Responsabilità dell'hosting provider: la Cassazione conferma la distinzione tra attivo e passivo*, in *www.filodiritto.it*, 18 aprile 2019.

²⁸ Cfr. E. TOSI, *Contrasti giurisprudenziali*, cit., p. 62 s. Per una ricostruzione dell'evoluzione giurisprudenziale sulla figura dell'*hosting attivo*, si v. 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 ss.; R. BOCCHINI, *La responsabilità di Facebook per la mancata rimozione di contenuti illeciti*, in *Giur. it.*, 2017, p. 638 ss.

gato la rilevanza della distinzione tra *hosting providers* attivi e passivi³⁰, si è comunque consolidato. È, per di più, corroborato dalla pronuncia Cass., I sez., 19 marzo 2019, n. 7708 (cit.) che, in quanto prima decisione dei giudici di legittimità su tale linea, ha, senza dubbio, un ruolo «persuasivo» sulle decisioni dei giudici di merito³¹.

Secondo la suddetta impostazione, alla figura soggettiva dell'*hosting provider* «attivo» si tornano ad applicare le regole di diritto comune, poste dall'art. 2043 c.c., per *culpa in vigilando*³². Più specificamente, se, da un lato, di norma, l'*hosting provider* è tenuto a svolgere la propria attività, osservando il criterio di diligenza professionale, ex art. 1176, comma 2, c.c. che gli impone di intervenire immediatamente, qualora venga effettivamente a conoscenza di contenuti illeciti pubblicati sul portale gestito; dall'altro lato, l'*hosting provider* «attivo» sarà tenuto a prestare la cura, l'attenzione e la perizia che gli sono imposte dal tipo di attività esercitata. Ne deriva che, proprio in ragione della particolare caratterizzazione della stessa, l'*hosting provider* «attivo» potrebbe ricorrere a strumenti tecnici di filtraggio e monitoraggio che individuino la sussistenza di contenuti illeciti -quali, ad esempio, dichiarazioni diffamatorie, piuttosto che espressioni di odio e di razzismo-, al fine di rimuoverli prontamente o di disabilitarne l'accesso³³. In altri casi, potrebbe anche impiegare soluzioni per impedire *a priori* comportamenti illeciti dei propri utenti: in relazione ai siti che pubblichino le recensioni su prodotti e servizi proposti da strutture recettive, l'*hosting provider* potrebbe prevedere

²⁹ Tra le numerose critiche dottrinali, cfr. O. POLLICINO, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider*, in *www.giurcost.org*, p. 13, secondo il quale l'interpretazione che ha condotto la giurisprudenza a coniare la figura dell'*hosting* attivo sarebbe una «forzatura del dato legislativo».

³⁰ Si v., *ex multis*, la pronuncia di App. Milano, 7 gennaio 2015, n. 29, citata; la decisione del Trib. Roma, sez. XVIII, 15 febbraio 2019, n. 3512 che ha dichiarato la responsabilità del *social network* Facebook per la pubblicazione sul portale di contenuti audiovisivi di terzi, per mezzo di *link* non autorizzati conducenti ad un'altra piattaforma (*Youtube*). Secondo il giudice, la dimostrazione dell'effettiva conoscenza dei contenuti illeciti da parte del *provider* rende del tutto irrilevante controllare se l'attività svolta sia riconducibile alla figura dell'*hosting* attivo o a quella dell'*hosting* passivo, dal momento che, anche quest'ultimo dovrà attivarsi per consentire la rimozione di informazioni illecite immesse sul sito o impedirne l'accesso, non appena riceva la notizia dell'illecito commesso dai fruitori del suo servizio, in ottemperanza all'adempimento del dovere di diligenza professionale, richiesta dal tipo di attività economica svolta. La sentenza è pubblicata in *www.francocrisafi.it > web_secondario > sentenze 2019 > tribunale civile*.

³¹ In tal senso cfr. F. FRIGERIO, *Responsabilità dell'hosting provider: la Cassazione conferma*, cit.

³² Cfr. R. GELLI, *False recensioni*, cit., p. 90 s.; M. ZARRO, *La tutela della reputazione digitale*, cit., p. 1523, che condivide le argomentazioni di M. GAMBINI, *Diritti di proprietà intellettuale in rete: criticità e prospettive degli strumenti di tutela nei confronti dei prestatori dei servizi Internet*, in *Rass. dir. civ.*, 2016, p. 139, secondo la quale non si dovrebbe negare aprioristicamente la fattispecie della *culpa in vigilando* degli *internet service providers*, dal momento che gli illeciti in rete avvengono proprio in virtù dell'attività svolta da costoro che dovrebbero, per tale ragione, essere coinvolti nelle responsabilità e nelle operazioni di prevenzione e rimozione dei dati.

³³ Per tale soluzione, cfr. M. ZARRO, *La tutela della reputazione*, cit., p. 1523.

un meccanismo -adottato solo da taluni, come *Airbnb* o *Booking*, e non da altri, quali *TripAdvisor*- che permetta ai fruitori del servizio di pubblicare un'opinione, solamente qualora abbiano effettivamente usufruito del bene o del servizio offerto dall'impresa.

Ne conseguirà che gli *hosting providers* «attivi» che omettano l'uso di tali strumenti tecnici, valutabili alla luce di soluzioni organizzative di un *provider* medio, risponderanno dell'inosservanza degli obblighi di diligenza- cui siano tenuti in qualità di operatori professionali-, in forza dell'art. 2043 c.c., per violazione dei livelli qualitativi da rispettare nell'esercizio dell'attività economica d'impresa³⁴.

La loro responsabilità potrebbe escludersi, solo rilevando che l'adozione di tali misure "preventive" dell'evento dannoso non siano esigibili dagli *hosting providers*, in quanto troppo onerose o impossibili da attuare: circostanza che non si verifica, invece, come si evince dai potenziali interventi prospettati nel caso concreto, proprio in ragione della struttura organizzativa sottesa ai fornitori di ospitalità così descritti³⁵.

2. La procedura di «notice and take down» tra ambiguità definitorie della c.d. «direttiva sul commercio elettronico» e le distinte soluzioni degli Stati membri. Una comparazione con altri ordinamenti

La «direttiva sul commercio elettronico» si caratterizza, in taluni punti, per l'assenza di chiarezza di certe regole, derivante dalla necessità di contemperare interessi contrapposti, quali: da un lato, la salvaguardia dell'indipendenza della rete, comunemente definita «*marketplace of ideas*»³⁶ - dal momento che, caratterizzandosi per l'assenza di limiti, l'immediatezza e l'economicità, assurge a luogo quanto più libero di circolazione di idee ed informazioni, proteggendo l'individuo dai rischi di censure - e, quindi, della libertà di manifestazione del pensiero³⁷ e, in senso più ampio, della libera esplicazione della personalità umana, ai sensi

³⁴ Cfr. M. GAMBINI, *Diritti di proprietà intellettuale*, cit., p. 139.

³⁵ Cfr. M. ZARRO, *La tutela della reputazione digitale*, cit., p. 1523.

³⁶ Cfr. M. MANETTI, *Libertà di pensiero e anonimato in rete*, in *Dir. inf.*, 2014, p. 142 s.

³⁷ La dottrina puntualizza come il significato della libertà di manifestazione del pensiero, il cui fondamento costituzionale è nell'art. 21, assuma in *internet* nuove implicazioni di ordine giuridico. Cfr. V. ZENOVICH, *La libertà di espressione. Media*, cit., p. 125 ss; T.E. FROSINI, *Il diritto di accesso in internet*, in T.E. FROSINI, O. POLLICINO, E. APA e M. BASSINI (a cura di) *Diritti e libertà in internet*, Milano, 2017, p. 41 ss., il quale precisa come l'esplicarsi della libertà di espressione sia strettamente correlato al diritto di accesso a *Internet*, da qualificarsi come «diritto sociale», o meglio una pretesa soggettiva nei confronti delle istituzioni nazionali al servizio universale di *internet* che deve essere garantito a tutti i cittadini, al pari dell'istruzione, della sanità e della previdenza.

dell'art. 2 cost.³⁸, nonché della protezione della *privacy* dei cibernauti; dall'altro lato, l'interesse a non rinunciare del tutto al controllo su quanto pubblicato sulle piattaforme digitali e a tutelare i soggetti che potrebbero essere danneggiati da contenuti illeciti³⁹.

Tra le ambiguità definitorie in merito a numerose locuzioni⁴⁰, si evidenziano: «servizi della società dell'informazione»; «attività o informazione illecita» ed, in particolare, nel fissare le condizioni alle quali il *caching provider* e l'*hosting provider* possano beneficiare del regime di responsabilità speciale, si impone loro di rimuovere «immediatamente» ovvero di disabilitare l'accesso ad informazioni illegali, non appena vengano «effettivamente a conoscenza» o «siano al corrente» di tali fatti.

In realtà, la disciplina europea non ha offerto alcuna indicazione rispetto alle procedure di «*notice and take down*», lasciando alla discrezionalità degli Stati membri ed all'operato dei *providers* la definizione in concreto di tali meccanismi⁴¹.

Il legislatore europeo si è, così, discostato dal modello statunitense, laddove, per la prima volta, nel 1998, è stata introdotta una procedura di «*notice and take down*» nel contesto relativo alla tutela del diritto d'autore *on line*, con la disciplina dettata dal *Digital Millenium Copyright Act* (c.d. «*DMCA*»)⁴². Si tratta di un meccanismo articolato che si connota per i tempi determinati di attivazione del *provider* e per l'intervento di diverse figure. Esso attribuisce un ruolo pregnante all'oggetto della contestazione, alla garanzia del contraddittorio tra le diverse parti interessate e al contenuto informativo che debba essere pubblicato dai

³⁸ Ciò vale sia per il singolo, sia per i gruppi che si formino in rete al fine di manifestare critiche, reclamare pretese, partecipare al dibattito pubblico - circostanza che assume preminente valenza, quando si tratti di minoranze etniche, di genere, sociali, etc. Sul punto si v. G. RESTA, *Anonimato, responsabilità, identificazione: prospettive di diritto comparato*, in *Dir. inf.*, 2014, p. 171 (§ 2.1.)

³⁹ Cfr. E. TOSI, *Contrasti giurisprudenziali*, cit., p. 71 s. In riferimento all'esigenza di contemperare la libertà di espressione ed i diritti fondamentali, con specifico riguardo ai *social networks*, si v. l'attenta analisi dell'evoluzione giurisprudenziale, in C.M. BIANCA, A.M. GAMBINO e R. MESSINETTI (a cura di), *Libertà di manifestazione del pensiero e diritti fondamentali. Profili applicativi nei social networks*, Milano, 2016, *passim*.

⁴⁰ Cfr. *EU Study on the Legal analysis*, o.c., p. 10 ss.

⁴¹ Si v. A. QUARTA, *La responsabilità civile*, cit., p. 282.

⁴² Si precisi (R. PETRUSO, *Le responsabilità degli intermediari*, cit., pp. 2 ss., 21 ss., 48 ss.) che il precedente *Communication Decency Act* del 1996 si è diversamente posto nell'ottica della prevalenza della libertà di espressione, non imponendo alcun dovere di rimozione in capo agli intermediari della rete. Ciononostante, a fronte della loro completa deresponsabilizzazione, legislativamente stabilita, la maggior parte degli *internet providers* cura le piattaforme di condivisione, intervenendo sui contenuti, dando la precedenza ad alcuni rispetto ad altri, rimuovendoli o deindicizzandoli. Si giunge, in tal guisa, al risultato di un modello di responsabilità che, nella prassi, non rispecchia la difesa della libertà di espressione in rete, normativamente avvalorata.

providers nelle proprie pagine *web*, per assicurare a coloro che assumano essere stati lesi la trasparenza della procedura⁴³.

⁴³ Sul punto e sull'analisi critica dei capisaldi della disciplina statunitense sui quali ci si soffermerà qui di seguito si v. S. SICA, V. D'ANTONIO, *La procedura di deindicizzazione*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di) *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Roma, 2015, p. 164 s. Specificamente, secondo il meccanismo procedimentale previsto dal modello statunitense, in forza del disposto della sec. 512, (c) (2), 17 U.S.C., il *provider*, per evitare di essere dichiarato responsabile per eventuali violazioni del *copyright*, deve, in primo luogo, nominare un soggetto preposto alla ricezione ed al vaglio delle notifiche di *infringement* dei titolari di diritti d'autore (c.d. *designated agent*). Affinché costui sia facilmente identificabile dal pubblico, il gestore deve comunicare le modalità per contattarlo, indicando un apposito *link* che sia ben visibile sulla *homepage* della piattaforma gestita. Le generalità dell'*agent* devono, poi, essere trasmesse al *Register of Copyright*, organismo statale sul cui *web* sono pubblicate alcune pagine informative, facilmente accessibili, sulle procedure di rimozione. In riferimento alla *notification*, comunicazione scritta che il soggetto che assume essere stato leso deve inviare al *designated agent*, si precisi che essa deve contenere i seguenti elementi: a) la firma (autografa o elettronica) del soggetto interessato o del legale rappresentante; b) l'indicazione dell'opera protetta che si ritiene essere stata utilizzata abusivamente; c) la specificazione dell'URL che consenta la corretta collocazione dei materiali lesivi; d) le informazioni che siano ragionevolmente idonee ad identificare il presunto autore della violazione che permettano al *provider* di contattarlo; e) un'espressa dichiarazione in cui il ricorrente afferma di agire in buona fede a tutela dei propri diritti; f) un'ulteriore dichiarazione che confermi l'esattezza delle informazioni fornite, nonché la legittimazione ad agire avverso le condotte oggetto del reclamo. Una segnalazione priva di tali elementi non può costituire prova dell'effettiva conoscenza in capo al prestatore di servizi di eventuali violazioni e, pertanto, non rileverà ai fini dell'esenzione di responsabilità, di cui alla sec. 512 (c) (1) (A). Quando le informazioni fornite siano parzialmente incomplete – e quando esse sostanzialmente integrino i requisiti previsti dalle lettere b), c) e d) – il fornitore del servizio viene considerato non a conoscenza della violazione unicamente se contattati immediatamente l'autore della notifica, invitandolo a rettificarne il contenuto. La sec. 512 (g) prevede, dappoi, una generica presunzione di irresponsabilità a favore del prestatore di servizi che abbia provveduto, in buona fede, a disabilitare l'accesso o a rimuovere contenuti ed attività, basandosi su fatti o circostanze che ne comprovassero l'apparente illiceità, indipendentemente dal fatto che l'apparenza abbia trovato oppure meno conferma, a seguito di ulteriori accertamenti. Questa presunzione non trova, viceversa, applicazione nelle ipotesi in cui il *provider* non garantisca un contraddittorio minimo tra il titolare del *copyright* che si presume violato e l'autore delle attività o dei contenuti oggetto di notifica. Ne discende che il *provider* è obbligato ad avvertire prontamente l'utente del portale, destinatario della misura restrittiva dell'avvenuta rimozione, ponendolo, così, in condizione di produrre una contro notifica (c.d. *counter notification*). Con tale atto costui contesta l'avvenuta rimozione o disabilitazione all'accesso del contenuto. Trattasi di una dichiarazione in forma scritta in cui il *subscriber* è obbligato ad indicare la precisa localizzazione fisica del contenuto (consistente quasi sempre nell'URL); deve, altresì, affermare, pena la condanna per falsa testimonianza (*perjury*), di avere buone ragioni per ritenere («*a good faith belief*») che i contenuti siano stati rimossi a causa di un errore o di una non corretta identificazione. Il sottoscrittore della contro notifica è, infine, obbligato a firmare un'apposita clausola nella quale dichiara di rimettersi alla giurisdizione della competente *Federal District Court*, accettando contemporaneamente che l'*agent* provveda ad inviare il contenuto della contro notifica alla controparte/*claimant*. L'*agent*, una volta ricevuta la *counter notification*, è tenuto a comunicarla immediatamente all'autore della segnalazione, informandolo che, entro dieci giorni, provvederà alla rimessione in pristino dei contenuti che siano stati rimossi. Il *provider* deve provvedere al ripristino dopo non meno di dieci e non più di quattordici giorni lavorativi dalla ricezione della contro-notifica, a meno che l'*agent* stesso riceva dal *claimant* la comunicazione dell'avvio di un'azione legale, mirante al conseguimento della cessazione dei comportamenti ritenuti illeciti rispetto ai materiali oggetto di notifica. Per un'articolata analisi della differenza tra «conoscenza effettiva» e «conoscenza imputabile» del fatto illecito, alla luce dell'applicazione giurisprudenziale della sec. 512, c.d. «DMCA», si v. R. PETRUSO, *Le responsabilità degli intermediari*, cit., p. 76 ss. L'A. pone altresì in luce come l'adozione di tecnologie di riconoscimento dei contenuti su base volontaria e l'automazione del processo di invio di richieste di rimozione potrebbe porre in crisi il modello di bilanciamento dei contrapposti interessi, prospettato dal legislatore statunitense, proponendo una “messa a punto” della procedura di «notice and take

La circostanza e la genericità delle espressioni adottate ha sollevato serie perplessità su quando si possa correttamente affermare che il *provider* sia «a conoscenza» di un fatto illecito, in base a quanto stabilito dal legislatore europeo. Qualora⁴⁴ si sia sentito dire che su un portale vi sia un contenuto illecito? Qualora ciò sia riferito dalla stampa? Quando il soggetto danneggiato lo denunci al gestore del sito? Quando vi sia una conoscenza indiretta o indiziaria ovvero quando ciò sia accertato dall'autorità amministrativa o giudiziaria?

A fronte di tale incertezza normativa⁴⁵, gli Stati membri hanno messo a punto pratiche diverse, per verificare la presenza del livello di conoscenza richiesto.

In taluni Stati membri che non hanno previsto legislativamente una procedura formale, i presupposti per la sussistenza della «conoscenza effettiva» sono stati sviluppati dalla dottrina, dalla giurisprudenza oppure in altri sedi.

A titolo esplicativo, i lavori preparatori della legislazione dei Paesi Bassi hanno espressamente specificato come una semplice segnalazione del contenuto illecito, pubblicato sul portale, non sia sufficiente, mentre, al contrario, lo è un ordine del Tribunale⁴⁶.

La giurisprudenza tedesca, con riferimento alle azioni a tutela del diritto d'autore, si è espressa nel senso dell'inadeguatezza della segnalazione che non sia dettagliata⁴⁷.

down», per colmare, in particolare, la lacuna insita nella sec. 512, c.d. «DMCA», che non prevede contromisure efficaci all'utilizzazione di tecnologie di riconoscimento automatizzato di contenuti. Tra i numerosi commenti alla disciplina statunitense, si v. L. NIVARRA, *Responsabilità del provider*, in *Dig. disc. priv., Sez. civ.*, XVII, Torino, 2003, p. 1195 ss.; M. FRANZONI, *La responsabilità del provider*, in *Resp. com. impr.*, 1997, p. 767 ss., e G.M. RICCIO, *La responsabilità civile degli internet providers*, cit., p. 50 ss. Si v. O. POLLICINO, *La prospettiva costituzionale sulla libertà di espressione nell'era di internet*, in *MediaLaws, Rivista di diritto dei media*, 2018, vol. 1, p. 1 ss., che sottolinea come la comune matrice liberale che connota l'Europa e gli Stati Uniti non abbia impedito la regolamentazione della responsabilità civile per comunicazioni diffuse in rete, con evidenti contraccolpi sullo statuto costituzionale della libertà di espressione.

⁴⁴ Per i quesiti posti nel corpo del testo, cfr. E. TOSI, *Contrasti giurisprudenziali*, cit., p. 72 s.

⁴⁵ Per la sintesi che segue sulla disciplina, dettata in tale ambito, dagli Stati membri, menzionati nel corpo del testo, si v. *EU Study on the Legal analysis, o.c.*, pp. 19-20.

⁴⁶ Si fa riferimento al *Legislative Decree Stb. 2004, 210, Law implementing E-Commerce Directive (2000/31/EC)* che, nel recepire gli articoli 12-14 della direttiva, ha aggiunto un nuovo articolo al Codice Civile olandese (DCC) nella sezione relativa alla responsabilità civile. La sezione 6:196c del DCC elenca le limitazioni della responsabilità degli *internet service providers* nei paragrafi da (1) a (4). La sezione 6:196c (5) indica che le limitazioni della responsabilità non precludono la possibilità dell'autorità amministrativa o giudiziaria di imporre ingiunzioni ai *providers*. La previsione, di cui all'art. 15 della direttiva, che gli Stati membri dell'UE non debbano imporre agli *internet service providers* obblighi generali di controllo, non ha portato a modifiche del codice civile olandese. Cfr. <https://wilmap.law.stanford.edu/entries/legislative-decree-stb-2004-210-law-implementing-e-commerce-directive-200031ec-article>

⁴⁷ La Germania ha recepito le disposizioni della direttiva sul commercio elettronico, relative alla responsabilità degli *internet service providers*, quasi pedissequamente, nei §§ 8-11 *Telemediengesetz* (emanato il 26 febbraio 2007 (BGBl. I S. 179, S. 251) e modificato, da ultimo, dall'art. 11 della Legge 11 luglio 2019 (BGBl. I S. 1066, 1076).

Altri Stati membri non hanno previsto una procedura formale a livello legislativo, ma hanno comunque stabilito che la notifica debba rispettare criteri civilistici.

Secondo la legislazione portoghese, il *Decreto-Lei N° 7/2004, Transpõe a Directiva 2000/31/CE, relativa a certos aspectos legais dos serviços da sociedade da informação, em especial do comércio electrónico, no mercado interno*⁴⁸, l'hosting provider non è tenuto a rimuovere un contenuto oppure a bloccarne l'accesso, per il solo fatto che un soggetto privato segnali la sussistenza di un contenuto illecito sul portale: circostanza questa che delimita la portata delle segnalazioni private.

Nel Regno Unito⁴⁹, l'atto di legislazione secondaria *the Regulations 2002, (the "E-Commerce Regulations")*, on 21st August 2002, n. 22, nel recepire, agli artt. 17, 18 e 19, quasi alla lettera, rispettivamente gli articoli 12, 13 e 14 della direttiva 2000/31/CE, ha apportato talune modifiche⁵⁰.

Il regolamento effettua delle precisazioni sulla portata della locuzione «conoscenza effettiva», dettando un elenco non esaustivo di elementi che una segnalazione di contenuti illeciti, ad opera di un soggetto che assuma essere stato danneggiato, debba contenere e che l'autorità giudiziaria debba verificare, al fine di decidere se l'*internet service provider* abbia ricevuto una notifica 'idonea' ad indurlo ad effettuare una verifica. Si impone, così, all'autorità giudiziaria di valutare le segnalazioni che specificino i dati identificativi del mittente e descrivano accuratamente sia la natura illecita dell'informazione, sia il luogo specifico ove sia stata pubblicata. Inoltre, l'art. 6, paragrafo 1, lettera c), *the Regulations 2002* impone ai *providers* l'obbligo di fornire all'utente del servizio determinate informazioni di contatto che faci-

Per un'analisi dei punti salienti delle problematiche, sollevate dal recepimento di tali disposizioni della direttiva nell'ordinamento tedesco, e sull'evolversi degli indirizzi giurisprudenziali su tali questioni, cfr. *Gutachten zur Zivilrechtlichen Verantwortlichkeiten von Internet-Service Providers in Deutschland, Frankreich, Dänemark, dem Vereinigten Königreich und den Vereinigten Staaten von Amerika*, Avis 14-106 Lausanne, den 29. September 2015, *Stand der Länderberichte* 30.06.2015, in <https://www.bj.admin.ch/dam/data/bj/aktuell/news/2015/2015-12-110/gutachten-sir-d.pdf>, pp. 29 -40.

⁴⁸ Sul punto cfr. http://www.uaipit.com/uploads/legislacion/files/0000005643_LEY_7_transposicion_directiva_comercio_electronico_2004_01_07.pdf.

⁴⁹ Per le riflessioni che seguono, si v. *Gutachten zur Zivilrechtlichen Verantwortlichkeiten*, o.c., p. 53.

⁵⁰ Una differenza importante è data dalla circostanza che il regime speciale di responsabilità degli *internet service providers*, previsto dalla direttiva, si applica quando il contenuto pubblicato sulla piattaforma digitale, gestita dal *provider*, sia illecito dal punto di vista sia civile, sia penale. Si consideri anche che il *Defamation Act* del 2013 ha statuito una procedura di segnalazione e rimozione in contraddittorio, prevedendo regole semplificatorie dell'agire dell'intermediario, a tutela della libertà di espressione e della reputazione del singolo. Sul punto si v. R. PETRUSO, *Le responsabilità degli intermediari*, cit., p. 184 ss.

litino la comunicazione rapida e diretta con lo stesso (come la posta elettronica, un indirizzo, un numero di telefono e altre informazioni di contatto) «in una forma [...] che sia facilmente, direttamente e permanentemente accessibile».

Peculiare è, poi, l'approccio del legislatore francese che, nella *loi du 21 juin 2004*, n. 575 *pour la confiance dans l'économie numérique*, c.d. «LCEN», di attuazione della direttiva, ha previsto una procedura di notifica opzionale⁵¹.

Si premetta che, ai fini della sussistenza della responsabilità civile dell'*hosting provider*, c.d. *hébergeur*, vengono fissate due condizioni: la conoscenza effettiva dell'illegittimità del contenuto e, dal momento in cui la si acquisisca, il mancato intervento tempestivo per la rimozione dei dati in questione o la disabilitazione al loro accesso.

Per agevolare la prova dell'effettiva conoscenza della natura illecita del contenuto, la legge prevede una presunzione semplice di conoscenza dei fatti illeciti da parte dell'*hébergeur*, quando riceva la notifica di diversi elementi elencati dall'art. 6-I-5 «LCEN», quali: la data del fatto illecito; le generalità complete della persona fisica o giuridica notificante e l'indicazione del legale rappresentante, se si tratti di un ente; il nome ed il domicilio o la sede legale del destinatario della notifica; la descrizione dei fatti contestati e la loro puntuale localizzazione nella rete; le ragioni per le quali dovrebbe essere rimosso il contenuto informativo pubblicato, in linea sia con quanto previsto *ex lege*, sia con la situazione di fatto; la copia della corrispondenza, previamente indirizzata all'autore del contenuto illecito pubblicato, del quale si sia richiesta la rimozione o la modifica, e l'eventuale specificazione che non sia stato possibile contattare codesto soggetto. Tale procedura di notifica facoltativa permette di dimostrare che l'*hébergeur* conosca il contenuto illegale che ospita e, perciò, lo obbliga ad agire immediatamente. Ciononostante, secondo il testo di legge, se la segnalazione consente di presumere la conoscenza effettiva del carattere illecito del contenuto, la si potrà anche provare in modalità differenti. Ad ogni modo, non è sufficiente comunicare l'esistenza di contenuti illegali, affinché l'*hébergeur* sia riconosciuto responsabile della manca-

⁵¹ La legge ha statuito un'apposita disciplina, a seconda del tipo di servizio fornito dall'*internet service provider*, distinguendo, all'art. 6, II, comma 1, tra i *fournisseurs d'accès*, ossia i fornitori di accesso ad *internet*, ed i *fournisseurs d'hébergement internet*, c.dd. *hébergeurs*. Per le considerazioni che seguono sulla disciplina francese, si v. *Gutachten zur Zivilrechtlichen Verantwortlichkeiten*, o.c., pp. 41, 46. Sul punto si v. anche F. CHOPIN, *Cybercriminalité*, in *Dalloz.fr*, mars 2014, p. 352; E. RICBOURG-ATTAL, *La responsabilité civile des acteurs de l'internet, du fait de la mise en ligne de contenus illicites*, Larcier, 2014, p. 191.

ta tempestiva loro rimozione dalla piattaforma digitale. La notifica non ha, infatti, valore coercitivo tale da imporre al fornitore di ospitalità la rimozione dei contenuti illegali segnalati, dal momento che quest'ultimo è dotato di potere discrezionale nella valutazione dell'illegittimità o meno dei contenuti stessi.

Avendo, poi, precipuo riguardo alla segnalazione del contenuto illecito all'*hébergeur* da parte del soggetto offeso, si osservi altresì che un orientamento giurisprudenziale ha sostenuto che, qualora i ricorrenti non si conformino alle previsioni legislative sulla procedura di notifica, non menzionando tutte le informazioni ivi previste, la loro richiesta di rimozione di contenuti illeciti debba essere respinta, rendendo, in tal guisa, il formalismo dettato dalla legge una condizione per la validità della conoscenza effettiva⁵².

Un diverso filone giurisprudenziale ha, viceversa, puntualizzato come, secondo il dato normativo, il meccanismo di notifica crei una semplice presunzione di effettiva conoscenza della natura illecita dei contenuti “ospitati” dai gestori delle piattaforme digitali, con la conseguenza che il mancato rispetto della procedura stessa non comporterebbe automaticamente la mancanza della conoscenza effettiva dell'*hébergeur* e, dunque, il rigetto della domanda⁵³.

⁵² In tal senso, si v., in particolare, la sentenza della *Cour de Cassation*, I sez. civ., 17 febbraio 2011, n. 09.67896, (pubblicata in www.legifrance.gouv.fr (27.01.2015)), in merito alla controversia giudiziaria, avviata dalla società di produzione detentrica dei diritti del film “*Joyeux Noël*” che aveva citato in giudizio, per contraffazione e concorrenza sleale, la società *Dailymotion*, in ragione del fatto che il motore di ricerca del sito dava accesso allo *streaming* gratuito del film, chiedendo sia la rimozione del contenuto illecito dalla piattaforma di condivisione, sia il risarcimento dei danni subiti. La Corte di legittimità, dopo aver affrontato la questione della qualifica del gestore del portale, incentrando l'attenzione sul ruolo tecnico e passivo dello stesso, si è pronunciata sul contenuto della notificazione del video oggetto di contestazione, precisando che chiunque intenda far rimuovere da un portale contenuti illegali e conseguire dal fornitore di ospitalità il risarcimento del danno che assuma aver subito, a seguito della loro pubblicazione, deve attenersi scrupolosamente alle procedure di notifica, previste dall'art. 6-I-5 «*LCEN*». A fronte delle argomentazioni addotte dalla società di produzione del video che ha contestato al gestore della piattaforma di condivisione di non aver ottemperato all'obbligo di rimuovere il *file* segnalato come illegale, la Corte di legittimità, sulla base della premessa che la legge «*LCEN*» prescrive una serie di dichiarazioni da includere nella notifica, ha rilevato come le informazioni comunicate al fornitore di ospitalità non soddisfacessero l'obbligo di “descrivere” e “localizzare” il fatto oggetto della segnalazione. È, in tal modo, pervenuta alla conclusione che non potesse essere ascritto alla società *Dailymotion* l'inadempimento dell'obbligo di rimuovere immediatamente il video contestato o di disabilitarne l'accesso, sostenendo che la società abbia, in realtà, avuto «conoscenza effettiva» del contenuto contestato, solo a seguito della proposizione della domanda giudiziale. Cfr. *La Cour de Cassation confirme le statut d'hébergeur de Dailymotion*, 18 febbraio 2011, in <https://www.legalis.net/actualite/la-cour-de-cassation-confirme-le-statut-dhebergeur-de-dailymotion/>

⁵³ Si v. in tal senso la sentenza del *Tribunal de Grand Instance de Paris* del 10 luglio 2009 che ha precisato come, d'altra parte, secondo quanto previsto *ex lege*, la conoscenza effettiva possa altresì essere dimostrata con qualsiasi altro mezzo giuridico.

La dottrina ha, d'altra parte, evidenziato come, se, per un verso, si possa comprendere la preoccupazione di prevenire gli abusi di notifiche di contenuti illegali ai fornitori di ospitalità (l'articolo 6.I.4 della «LCEN» prevede un reato simile alla denuncia calunniosa) o le richieste non fondate, va, per altro verso, notato che la previsione di criteri stringenti della formulazione della segnalazione porrebbe i titolari dei diritti o le vittime di contenuti illegali in una situazione spesso molto delicata, sotto il punto di vista della rivendicazione dei loro diritti. Dal momento che l'autore della pubblicazione del contenuto illegale è sovente anonimo e che, in tale ipotesi, l'*hébergeur* è l'unica persona identificabile, la rimozione delle dichiarazioni in questione e, ancor di più, la pretesa del risarcimento dei danni costringerebbe, di fatto, l'attore a chiedere l'assistenza di un legale, non solo per garantire la comunicazione degli elementi di notifica prescritti dalla legge, ma altresì per formulare contestazioni che siano precisamente argomentate dal punto di vista giuridico, soprattutto in ambiti altamente tecnici, quali in materia di contraffazione o diffamazione, per evitare che i gestori dei portali, sulla scorta di consulenti legali, finiscano col non accoglierle, poiché non dettagliate ovvero imprecise⁵⁴.

In altri Stati membri, quali la Spagna e l'Italia, sebbene il legislatore abbia disposto che il *provider* sia obbligato a rimuovere il contenuto illecito oppure a disabilitarne l'accesso, su ordine «dell'autorità competente», le Corti hanno prevalentemente interpretato la regolamentazione, discostandosi dal dato letterale.

Sul modello italiano, si tornerà *infra* nel paragrafo successivo.

In Spagna, il legislatore, all'art. 16 della *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*, ha interpretato restrittivamente la locuzione europea di «conoscenza effettiva» (*conocimiento efectivo*) dell'illiceità dei contenuti pubblicati sui portali, statuendo che essa sussista quando un organo competente la dichiara preventivamente oppure ordini al *provider* la rimozione di tali informazioni o la disabilitazione al loro accesso, pur facendo salve le procedure di rilevamento del carattere illecito che siano predisposte dagli stessi *providers* e quelle che siano il prodotto di accordi di autoregolamentazione, nonché gli altri mezzi di conoscenza efficace che potranno essere individuati in futuro⁵⁵.

⁵⁴ Sul punto si v. A. RICHARD, H. MARQUETT, *La responsabilité des hébergeurs sur internet*, in <http://legalnews.fr/>, 1 giugno 2011.

⁵⁵ Cfr. *EU Study on the Legal analysis*, p. 20.

Per «organo competente»⁵⁶ si intendono tutte le autorità giudiziarie ed amministrative che operano nell'esercizio delle proprie competenze istituzionali; ma, non esistendo, in Spagna, alcun organo amministrativo preposto a tale specifico compito, ne deriva che l'unico organo che abbia la competenza di definire la liceità o l'illiceità dei contenuti pubblicati sui portali sia l'autorità giudiziaria.

Cionondimeno tale stringente procedura non è seguita dalle corti spagnole che riconoscono la responsabilità civile dei *providers*, quand'anche non si siano attivati, a seguito della segnalazione del privato che assuma essere stato lesa dalla pubblicazione di contenuti illeciti da parte degli utenti delle piattaforme digitali da costoro gestite.

È il caso di sottolineare, infine, che taluni Stati membri hanno introdotto una disciplina speciale della «*notice and take down procedure*».

In Italia, la l. 29 maggio 2017 n. 71, «Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del *cyberbullismo*»⁵⁷ ha previsto la possibilità del minore ultraquattordicenne⁵⁸ che sia stato vittima di uno degli illeciti (oppure del genitore ovvero del soggetto esercente la responsabilità genitoriale), riconducibili all'art. 1, comma 2, di fare una segnalazione al titolare del trattamento oppure al «gestore del sito *internet* o del *social media*», affinché quest'ultimo provveda alla rimozione o al blocco dei contenuti oggetto delle condotte aggressive avvenute *on line*.

Tale meccanismo presenta dei limiti.

In primis, esso concerne unicamente i dati personali diffusi in rete e reputati lesivi della personalità dei minori di anni quattordici.

⁵⁶ Per le osservazioni che seguono cfr. 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.*, 2011, p. 287.

⁵⁷ Per le notazioni che seguono, cfr. B. PANATTONI, *Il sistema di controllo successivo: obbligo di rimozione dell'ISP e meccanismi di notice and take down*, in *www.dirittopenalecontemporaneo.it*, 2018, n. 5, p. 260.

⁵⁸ I. GARACI, *La "capacità digitale" del minore nella società dell'informazione. Riflessioni sul corretto esercizio della responsabilità genitoriale fra esigenze di autonomia e protezione*, in *Nuovo diritto civile*, 2019, p. 69, evidenzia come il riconoscimento della "capacità digitale" al minore ultraquattordicenne, in tale ambito regolamentare, così come nella disciplina per la protezione dei dati personali dettata dal Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, si riveli, in concreto, funzionale all'esercizio delle libertà fondamentali riconosciute nella rete e coerente con il contesto normativo internazionale ed interno, ove si è assistito alla graduale emersione del diritto all'autodeterminazione del minore, nell'esercizio di diritti fondamentali a contenuto non patrimoniale.

In secundis, esso non solo non disciplina in maniera puntuale l'obbligo di rimozione a carico dell'*internet service provider*, ma non statuisce neanche un impianto sanzionatorio *ad hoc*. Il gestore di servizi *online* non sarà, in effetti, sanzionato nel caso in cui non rimuova i contenuti segnalati entro le ventiquattro ore dalla notifica, quand'anche si tratti di un contenuto manifestamente illecito o lesivo della dignità e della personalità del minore. Qualora, entro ventiquattro ore dalla ricezione della richiesta, il prestatore del servizio non abbia preso in carico l'istanza ed entro le quarantotto ore non vi abbia provveduto, l'interessato potrà proporre analoga richiesta al Garante della *privacy* che, entro quarantotto ore dalla ricezione, potrà adottare i provvedimenti previsti dagli art. 143 e 144 del d.lgs. 30 giugno 2003, n. 196, aggiornato dalla l. 27 dicembre 2019, 160, c.d. Codice della *privacy*. In sostanza, l'Autorità garante della protezione dei dati personali potrà invitare il titolare del trattamento a compiere il blocco spontaneo del trattamento illecito; potrà prescrivere a costui le misure opportune o necessarie, per rendere il trattamento conforme alle disposizioni vigenti; potrà disporre il blocco o vietare, in tutto o in parte, il trattamento che risulti illecito o idoneo a provocare un pregiudizio rilevante per uno o più soggetti interessati; potrà vietare, in tutto o in parte, il trattamento di dati relativi ai singoli soggetti o a categorie di soggetti, quando si ponga in contrasto con interessi rilevanti della collettività. Il *provider* che non si attivi sarà, in via conclusiva, sanzionabile esclusivamente quando non adempia agli obblighi imposti dal Garante della *privacy*, in forza dell'art. 170 del Codice della *privacy*⁵⁹.

Sotto un altro profilo, tale disciplina ha il sicuro pregio di dettare una normativa che predispone strumenti di tutela del minore, in via preventiva rispetto al rimedio risarcitorio⁶⁰.

In Germania il primo ottobre 2017 è, poi, entrato in vigore il *Netzwerkdurchsetzungsgesetz*, la nuova legge per “migliorare la tutela dei diritti sui *social network*”⁶¹ che ha introdotto, per la prima volta in uno Stato membro dell'Unione Europea, strumenti nuovi per contrastare gli illeciti⁶² sui portali di comunicazione del *web 2.0*.

⁵⁹ Cfr. A. INGRASSIA, *Responsabilità penale degli internet service provider: attualità e prospettive*, in <https://www.quotidianogiuridico.it/documents/2017/12/21>, p. 1628

⁶⁰ Cfr. P. PITTARO, *La legge sul cyberbullismo*, in *Fam. dir.*, 2017, p. 819 ss.

⁶¹ Si tratta del *Gesetz zur Verbesserung der Rechtsdurchsetzung in soziale Netzwerken* del 1 settembre 2017 (BGBl. I S. 3352). Per le riflessioni che seguono, cfr. G. GIANNONE CODIGLIONE, *La nuova legge tedesca per l'enforcement dei diritti sui social network*, in *Dir.inf.*, 2017, p. 728 ss.

⁶² Il legislatore non ha fornito una definizione generica di «contenuto illecito»; ha richiamato, piuttosto, al § 1, comma 3, numerose disposizioni del Codice penale tedesco, *Strafgesetzbuch*, in tema di: utilizzo di simboli e

La disciplina si applica unicamente ai servizi della società dell'informazione che abbiano almeno due milioni di utenti registrati in Germania e che offrano, per scopo di profitto, spazi virtuali di condivisione di contenuti. Sono espressamente esclusi i portali di informazione in cui la responsabilità dei contenuti pubblicati sia dell'editore, oltre che le piattaforme che offrano servizi di comunicazione individuale oppure trasmissioni di contenuti specifici, quali, a titolo esplicativo, le *app* di messaggistica istantanea.

La normativa pone, in capo ai *social media*, due tipologie di obblighi.

In primo luogo, impone al gestore del sito che abbia ricevuto più di cento segnalazioni di contenuti illeciti in un anno solare l'obbligo di fornire, entro un mese dalla fine di ogni semestre di riferimento, un resoconto da pubblicare sulla Gazzetta Federale e sulla propria *home page*. Il resoconto deve contenere una descrizione generale sulle modalità di svolgimento delle attività e sulle risorse impiegate, sui criteri adottati per verificare ogni singolo caso, nonché una sezione attinente alle statistiche sul numero di segnalazioni ricevute, sui risultati raggiunti, sulle tempistiche di chiusura della pratica e sulle tipologie di soggetti che abbiano inviato e su quelli che abbiano valutato la segnalazione.

In secondo luogo, la legge statuisce l'obbligo del *provider* di gestire i reclami concernenti i contenuti illeciti, rimuovendoli o disabilitandone l'accesso, secondo una procedura trasparente e tempestiva. Precipuamente i *social media* devono, anzitutto, predisporre un sistema di notifica dei contenuti illeciti efficace e facilmente accessibile e son tenuti a nominare una persona autorizzata a ricevere le notifiche nella Repubblica Federale tedesca, dandone notizia sul proprio portale.

In aggiunta, una volta che la segnalazione sia ricevuta, per il gestore del sito scattano distinti obblighi. Costui dovrà rimuovere o disabilitare l'accesso al contenuto che sia considerato "manifestamente illecito" entro ventiquattro ore dalla ricezione della segnalazione, a meno che non abbia concordato un termine diverso con l'Autorità competente. Il *provider* sarà obbligato a rimuovere o a disabilitare l'accesso di "tutti" i contenuti illeciti, entro sette

propaganda politica vietata; preparazione e incitazione alla commissione di gravi crimini contro lo Stato; falso per l'alto tradimento dello Stato; pubblica incitazione alla violenza; disturbo della pace pubblica con la minaccia dei crimini; associazione criminale o terroristica; sedizione; diffusione di contenuti violenti; ricompensa e approvazione di crimini; diffamazione religiosa o ideologica; distribuzione, acquisto o detenzione di materiale pedopornografico; violazione della riservatezza attraverso la creazione o diffusione di fotografie; ingiuria; calunnia; diffamazione; minaccia e falsificazione di prove.

giorni dalla ricezione della segnalazione oppure, se il caso lo richieda, a prorogare di sette giorni il termine allo scopo di garantire un contraddittorio minimo con l'utente che abbia pubblicato o condiviso il contenuto, oggetto di segnalazione; oppure, entro sette giorni dalla ricezione della segnalazione, a rimettere la questione alla decisione vincolante di un organo indipendente di autoregolamentazione che sia accreditato dall'autorità amministrativa competente, ai sensi dei §§ 3, 4 della legge⁶³.

Il gestore del sito sarà, inoltre, tenuto a comunicare all'utente che abbia pubblicato sul portale i contenuti sia la decisione assunta, sia le motivazioni sulle quali si basa. Il soggetto che assuma essere stato leso dai contenuti pubblicati e non rimossi o disabilitati, a seguito dell'attivazione della procedura di segnalazione, potrà rivolgersi al giudice di merito, al fine di conseguire la revisione della soluzione adottata dal *provider*.

La legge prevede, infine, al § 4, sanzioni di diverse tipologie, graduandole nell'ammontare, specificamente per il caso di mancata nomina di una persona autorizzata alla ricezione delle notifiche nel territorio della Repubblica Federale tedesca o quando il prestatore non risponda alle richieste di informazioni; per il caso di violazione dell'obbligo di resoconto e di tutti gli obblighi riguardanti il funzionamento della procedura di segnalazione.

3. La procedura di «notice and take down» nel nostro sistema e la sua applicazione giurisprudenziale al caso concreto

Avendo precipuo riguardo alla disciplina italiana di attuazione della normativa europea, occorre preliminarmente rimarcare che il legislatore, nell'art. 16, comma 1, lett. b), d.lgs. 2003/70, nel recepire la disposizione dell'art. 14, comma 1, lett. b) della direttiva 2000/31/CE - che esclude la responsabilità dell'*hosting provider* per le informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore agisca immediatamente, per rimuovere le informazioni o per disabilitarne l'accesso, non appena

⁶³ Trattasi, ai sensi delle disposizioni menzionate, di un organo finanziato dai gestori delle piattaforme digitali, tenuti ad adempiere gli obblighi legislativamente previsti, e provvisto di una struttura organizzativa capace di ricevere e controllare le istanze, attuando parametri procedurali e di discrezionalità predeterminati che prevedano anche il possibile riesame delle decisioni. Cfr. G. GIANNONE CODIGLIONE, *La nuova legge tedesca*, cit., p. 731.

sia a «conoscenza dei fatti» (*ex lett. b*)-, ha aggiunto l'inciso «su comunicazione delle autorità competenti».

Le Corti italiane sono state chiamate a sciogliere il nodo gordiano se l'*hosting provider* sia obbligato ad intervenire unicamente a seguito della comunicazione da parte dell'autorità competente e, quindi, solamente quando acquisisca una conoscenza «qualificata» del fatto illecito; ovvero se tale obbligo sorga in maniera autonoma, non appena il *provider* venga a conoscenza del contenuto illecito pubblicato, tramite la segnalazione da parte del privato che assuma essere stato leso - pur in assenza dell'ordine dell'autorità competente⁶⁴.

La giurisprudenza prevalente non si è cristallizzata sugli esiti della *mera* interpretazione letterale, procedendo ad un'interpretazione sistematica ed assiologica della norma in questione, per pervenire, in linea con talune ricostruzioni dottrinali e con gli indirizzi della giurisprudenza spagnola, alla conclusione di ritenere sufficiente la mera diffida del soggetto danneggiato, ai fini della sussistenza dell'«effettiva conoscenza» della condotta illecita dell'utente del servizio.

Prima di analizzare l'evoluzione giurisprudenziale in tale ambito, è d'uopo precisare che dall'analisi normativa compiuta emerge come non sia delineabile una responsabilità civile *ex ante* dell'*hosting provider* che deriverebbe dal mancato controllo preventivo e generale dei contenuti ospitati, trasmessi e memorizzati dallo stesso, dal momento che la disciplina esclude un obbligo di sorveglianza preventivo⁶⁵. Il legislatore europeo ha, al contrario, spostato l'obbligo di sorveglianza dalla fase anteriore dell'immissione da parte degli utenti dei dati sulle piattaforme digitali alla fase successiva, al momento in cui il *provider*, pur avendo effettivamente conoscenza della presenza di un contenuto illecito, non si attivi per rimuoverlo o disabilitarne l'accesso⁶⁶.

È proprio alla luce di tali osservazioni che appare evidente il ruolo fondamentale delle corti nella fissazione dei criteri necessari ai fini della configurabilità della conoscenza «effettiva», da parte dell'*hosting provider*, dei contenuti illeciti pubblicati sulla piattaforma da costui gestita.

⁶⁴ Cfr. B. PANATTONI, *Il sistema di controllo successivo*, cit., p. 255.

⁶⁵ Cfr. B. PANATTONI, *Il sistema di controllo successivo*, cit., p. 249.

⁶⁶ Cfr. E. TOSI, *Contrasti giurisprudenziali*, cit., p. 71.

Ciò detto, secondo un primo indirizzo giurisprudenziale sviluppatosi sin dalle prime applicazioni della norma menzionata, poi fatto proprio dalla giurisprudenza maggioritaria, ai fini dell'insorgere dell'obbligo di intervento *ex post* del *provider*, sarebbe sufficiente la conoscenza, comunque acquisita, e, pertanto, anche la conoscenza derivante dalla diffida di chi assuma essere titolare del diritto leso, pur in assenza di formali comunicazioni dell'autorità amministrativa o giudiziaria⁶⁷.

Tale presa di posizione risiede in diverse ragioni.

Si considera innanzitutto che l'ambiguità della formulazione atecnica ed equivoca delle previsioni, di cui all'art. 16, comma 1, lett. a) e lett. b), d.lgs. 2003/70, piuttosto che essere frutto di una ponderata scelta di politica del diritto, appaia, all'opposto, essere il risultato di un «infelice *drafting* normativo»⁶⁸. In aggiunta, si è arguito come l'interpretazione della norma che si limitasse a ritenere esigibile l'obbligo di intervento dell'*hosting provider*, solo in seguito al ricevimento dell'ordine dall'autorità competente, ai sensi della lett. b), finirebbe con lo svuotare di contenuto la portata della previsione della lett. a); pervenendo, in tal modo, ad una *interpretatio abrogans* dell'art. 16, lett. a), oltre che dell'art. 17 d.lgs. 2003/70 che, come visto, ai fini dell'esonero della responsabilità civile del *provider*, gli impone di in-

⁶⁷ Cfr. 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, pp. 540-541. Tra le pronunce in tal senso si v. la sentenza del Trib. Catania, 29 giugno 2004, in *Resp. civ. prev.*, 2005, 188, con nota di L. BUGIOLACCHI, *La responsabilità dell'host provider alla luce del d.lgs. n.70 del 2003: esegesi di una disciplina "dimezzata"*. Nella medesima direzione, si v. le pronunce Trib. Bari, 13 giugno 2006, in *Dir. internet*, 2006, p. 563, e Trib. Trani, 14 ottobre 2008, in *Danno resp.*, 2009, p. 105; l'ordinanza Trib. Roma, 11 febbraio 2010, in *Dir.inf.*, 2010, p. 275, secondo la quale è ammissibile l'emissione di un provvedimento cautelare che ordini al *provider* – nel caso di specie, *YouTube LLC, Google Inc., Google UK Ltd* – la rimozione di frammenti audiovisivi di un'opera protetta che siano stati diffusi abusivamente in *Internet*, qualora costui abbia avuto «conoscenza effettiva» dell'illiceità dei contenuti, pubblicati sulla piattaforma gestita, dal titolare dei diritti (nel caso di specie RTI s.p.a.): in sostanza, si correla l'obbligo di rimozione immediata del contenuto illecito alla ricezione della diffida del soggetto offeso, non ravvisando la necessità dell'ordine dell'autorità competente. Si vedano anche l'ordinanza Trib. Milano, 20 gennaio 2011, n. 7680, in *Dir. ind.*, 2012, p. 255, con nota di A. BELLAN, *Per una reasonable liability: critiche alla responsabilità oggettiva dei provider e tutela dei diritti su internet*; si v. le ordinanze Trib. Torino, 5 maggio 2014, Trib. Torino, 23 giugno 2014, entrambe pubblicate in www.marchiebrevettiveb.it; si v. l'ordinanza Trib. Napoli Nord, sez. civ., II, 3 novembre 2016, in *Giur. it.*, 2017, p. 629 ss., con nota di R. BOCCHINI, *La responsabilità di Facebook per la mancata rimozione di contenuti illeciti*; la decisione Trib. Torino, sez. impr., 7 aprile 2017, n. 1928, in *Danno resp.*, 2018, p. 87 ss. – che ha ampliato ulteriormente la portata dell'obbligo di rimozione del *provider*, sostenendo che esso, ai sensi del dato normativo, implicherebbe, in virtù degli strumenti tecnici di cui sia dotato, anche l'impedimento di nuovi caricamenti che abbiano ad oggetto informazioni già segnalate sulle piattaforme digitali.

⁶⁸ Cfr. R. GELLI, *False recensioni su TripAdvisor*, cit., p. 87.

formare l'autorità competente, non appena abbia avuto conoscenza del carattere illecito di un contenuto del quale ammetta la pubblicazione⁶⁹.

Tale considerazione ha costituito una delle argomentazioni fondanti la motivazione della pronuncia del Trib. Napoli Nord, sez. civ., II, 3 novembre 2016⁷⁰ che ha puntualizzato come la scelta di non ritenere, quale presupposto necessario, la comunicazione dell'autorità competente, si basi, altresì, sul tenore del considerando 46 della direttiva europea che afferma che, per godere del regime speciale di limitazione della responsabilità, l'*internet provider* debba agire «immediatamente» nella rimozione delle informazioni o nel disabilitarne l'accesso «non appena sia informato o *si renda conto* delle attività illecite»- locuzione che non restringe in alcun modo le modalità in cui il *provider* possa venire a conoscenza del contenuto illecito ad un ordine di un'autorità competente⁷¹.

Tale posizione è stata oggetto di critiche dottrinali⁷², espresse nel solco del diverso orientamento giurisprudenziale⁷³ che ha fissato dei presupposti molto rigorosi, ai fini dell'individuazione dell'esistenza della «conoscenza effettiva» da parte dell'*hosting provider*, sostenendo che debbano contemporaneamente esservi entrambe le condizioni previste dall'art. 16, comma 1, lett. a) e b), d.lgs. 2003/70. In tale prospettiva, il *provider*, quand'anche venisse a conoscenza di contenuti manifestamente illeciti, non sarebbe responsabile della

⁶⁹ Cfr. G. CASSANO, I.P. CIMINO, *Il nuovo regime di responsabilità dei providers: verso la creazione di un novello "censore telematico"*, in *Corr. giur.*, 2004, p. 91; concorde con tale ricostruzione R. GELLI, *False recensioni su TripAdvisor*, cit., p. 87.

⁷⁰ L'ordinanza Trib. Napoli Nord, sez. civ., II, 3 novembre 2016, cit., nell'accogliere parzialmente il reclamo presentato da *Facebook*, diretto a richiedere la riforma del precedente provvedimento cautelare- con il quale il Tribunale aveva accolto la domanda, proposta *ex art.* 700 c.p.c. da un'utente nei confronti di *Facebook*, ordinando "l'immediata cessazione e rimozione dalla piattaforma del *social network* di ogni *post* o pubblicazione contenente immagini (foto e/o video) o apprezzamenti riferiti specificamente alla persona del ricorrente"- affronta, in modo dettagliato, la problematica della responsabilità civile del *provider* di contenuti manifestamente illeciti. Il giudice ordina a *Facebook* la rimozione delle pagine *web* che hanno violato i diritti personalissimi della ricorrente, a seguito della richiesta da parte dell'interessata. In aggiunta, nel motivare la decisione, fa discendere la responsabilità civile del *provider* dal mancato intervento, a seguito di segnalazione del privato, specificando come non sia necessario, ai fini della configurabilità dell'obbligo del fornitore di servizi *internet* in tal senso, l'ordine dell'autorità giudiziaria o amministrativa.

⁷¹ In tal senso si v. anche S. SICA, V. D'ANTONIO, *La procedura di deindicizzazione*, cit., p. 168.

⁷² Cfr. L. BUGIOLACCHI, *I presupposti dell'obbligo*, cit., pp. 540-541; G.M. RICCIO, *La responsabilità civile degli internet providers*, cit., p. 210; S. SICA, *Responsabilità del provider: per una soluzione "equilibrata" del problema*, in *Corr. giur.*, 2013, p. 509; F. BRAVO, *Commercio elettronico*, in *Enc. dir., Annali*, Milano, 2012, p. 311 ss.

⁷³ Si v. l'ordinanza Trib. Firenze, 25 maggio 2012, in *Dir. inf.*, 2012, p. 1210, con nota di T. SCANNICCHIO, *La responsabilità del motore di ricerca per la funzione "auto-complete"* - che sottolinea come le diffide dei terzi non siano sufficienti a far sorgere, in capo al *provider*, l'obbligo di intervento, dal momento che si tratta, pur sempre, di prospettive unilaterali; si v. la sentenza App. Milano, 7 gennaio 2015, n. 29, cit.

loro mancata rimozione o della disabilitazione al loro accesso, finchè non riceva l'ordine dell'autorità competente.

Al fine di corroborare tale tesi, la dottrina ha affermato⁷⁴ che l'indirizzo della giurisprudenza maggioritaria finirebbe col non approfondire affatto le conseguenze sul piano costruttivo-generale dell'inciso relativo alla «denuncia delle autorità competenti», introdotto alla lett. b), che rappresenta una rilevante novità rispetto al testo della «direttiva sul commercio elettronico». Si è viepiù posto l'accento⁷⁵ sul tenore letterale della norma che, in particolare per il diritto penale, imporrebbe il vincolo del principio di tassatività. Si è, poi, affermato⁷⁶ che la configurazione della necessità dell'ordine dell'autorità competente delimiterebbe il rischio di conferire all'*internet provider* la funzione di censura «sostanziale» che, nei casi in cui i contenuti siano di valutazione difficile ed incerta, potrebbe tendere a rimuoverli in maniera cautelativa; la soluzione a tale problematica sarebbe, dunque, ravvisabile nell'esclusivo operare di una censura «funzionale» della libertà di espressione degli internauti, ad opera dell'autorità giudiziaria, nel rispetto della legalità⁷⁷.

⁷⁴ Cfr. L. BUGIOLACCHI, *I presupposti dell'obbligo di rimozione*, cit., pp. 540-541.

⁷⁵ Cfr. F. DI CIOMMO, *Responsabilità dell'internet hosting provider, diffamazione a mezzo Facebook e principio di tassatività della norma penale: troppa polvere sotto il tappeto*, nota alla sentenza Cass. pen., 27 dicembre 2016, n. 54946, in *Foro it.*, 2017, c. 251 ss.

⁷⁶ Cfr. B. PANATTONI, *Il sistema di controllo successivo*, cit., p. 256.

⁷⁷ Si richiamano nel testo le due figure di censure, riconducibili alla c.d. «censura *de jure*»: la censura «sostanziale», una sorta di delega conferita, su spinta giurisprudenziale, ai gestori delle piattaforme digitali di valutare nella sostanza l'illiceità del contenuto da rimuovere, e la censura «funzionale» che consisterebbe nell'obbligo di tali soggetti di rimuovere i contenuti, solo se specificamente predeterminati da una legge oppure da una sentenza. Sul tema si v. M. MONTI, *Privatizzazione della censura e Internet platforms: la libertà d'espressione e i nuovi censori dell'agorà digitale*, in *Riv. it. inf. dir.*, 2019, 1, p. 35 ss. L'autore, in realtà, nel definire la «censura *de jure*» fa specifico riferimento a quella derivante (unicamente) dalle disposizioni normative vigenti in uno specifico territorio. Sul tema si v. anche J.M. BALKIN, *Free speech is a triangle*, 118 *Columb. L. Rev.*, 2018, p. 2011 ss., il quale puntualizza come i problemi di censura, in tale ambito, derivino dalla peculiare circostanza che i soggetti che gestiscono le piattaforme digitali sono, al contempo, coloro che vigilano sui contenuti che vengono pubblicati, in quanto sono preposti alla loro selezione, organizzazione e rimozione. Si v. anche G. PITRUZZELLA, *La libertà di informazione nell'era di internet*, in *Media Laws, Rivista del diritto dei Media*, 2018, p. 17, che precisa come le informazioni pubblicate dall'utente in rete vengano selezionate in maniera opaca dagli algoritmi dei portali. Si rammenti che, d'altronde, la Commissione Europea (nella Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, dal titolo «Lotta ai contenuti illeciti *on line*. Verso una maggiore responsabilizzazione delle piattaforme digitali», 28 settembre 2017, COM (2017) 555 *final*, punto 21) definisce gli intermediari della rete «guardiani dei contenuti». In tal senso si v. R. PETRUSO, *Le responsabilità degli intermediari*, *Presentazione*, cit., p. XVIII.

Di fondamentale rilevanza sulle problematiche attinenti alla censura è la sentenza Cort. giust., 3 ottobre 2019, C- 18/18, *Eva Glawischnig Piesczek c. Facebook Ireland Limited*, pubblicata in <http://www.medialaws.eu/la-corte-di-giustizia-la-direttiva-e-commerce-e-il-controllo-contenutistico-online-le-implicazioni-della-decisione-c-18-18-sul-discorso-pubblico-online-e-sul-ruolo-di-facebook/>, 15 ottobre 2019, con commento di M. MONTI *La Corte di giustizia, la direttiva e-commerce e il controllo contenutistico online: le implicazioni della decisione C 18-18 sul discorso pubblico online e sul ruolo*

Pur tuttavia, a livello giurisprudenziale, prevale la tesi che, ai fini dell'attivazione dell'*hosting provider*, ritiene sufficiente la conoscenza acquisita tramite la segnalazione da parte della persona offesa.

Si condivide tale posizione interpretativa, frutto dell'operazione, compiuta a livello giurisprudenziale, di superare la tecnica della “sussunzione” del fatto ad una determinata fattispecie astratta prevista dal legislatore, pervenendo all'individuazione della disciplina «più adeguata» al caso concreto, per mezzo della valutazione del fatto, effettuata prendendo in considerazione gli interessi, i valori ed i principi che lo stesso esprima, calandolo nel contesto storico-giuridico di riferimento⁷⁸.

In tale direzione⁷⁹, le corti son pervenute ad un bilanciamento tra gli interessi coinvolti nella rete, sottesi alla vicenda, quali: l'iniziativa economica privata dei *providers*, da un lato, e l'esigenza di garantire la libertà di espressione e la tutela dell'indipendenza di *internet*, dall'altro; i diritti facenti capo agli utenti, da un lato, e i diritti dei terzi lesi dai contenuti illeciti da questi caricati, dall'altro. I giudici, nel contemperare i contrapposti interessi, hanno trovato un punto di equilibrio tra la necessità di assicurare l'effettività della tutela giudiziaria dei diritti lesi e l'esigenza di tener conto delle dinamiche ‘temporali’ della rete. Invero, la circostanza che i contenuti pubblicati nel *web* si diffondano con velocità estrema e peculiare pervasività rende inefficiente la scelta di soluzioni interpretative che implicino un prolun-

di Facebook. La Corte europea ha stabilito che è lecito, in base alla «direttiva sul commercio elettronico», che l'autorità giudiziaria o amministrativa richieda all'*hosting provider* la rimozione *seriale* di contenuti, quando essi siano «identici o equivalenti» ad un contenuto ritenuto illecito dalle stesse autorità. I contenuti «equivalenti» da rimuovere devono essere individuati dall'autorità giudiziaria o amministrativa, con la conseguenza che i fornitori di ospitalità non debbano procedere ad valutazione autonoma sugli stessi e che costoro possano rimuovere tali contenuti mediante procedure automatizzate. Il principio così espresso dalla Corte eviterà che gli *hosting providers* pongano in essere, in futuro, procedure di sorveglianza generalizzata o attiva. Si deve, cionon-dimeno, sottolineare che, sebbene la predisposizione di questo meccanismo sia da salutare con favore, non è tuttavia privo di problematiche in tema di discorso pubblico e di libertà di espressione in rete. In effetti, la pronuncia delinea un'ipotesi di «censura funzionale», laddove conferisce a *Facebook* la delega di rimozione di contenuti pubblicati sul *social network*, ma solo una volta che gli stessi siano stati individuati *a priori* dall'autorità giudiziaria o amministrativa. Il meccanismo così profilato potrebbe determinare il rischio di censure sistematiche, insito nella delega al *social network* della rimozione di contenuti senza istruzioni precise da parte di un'autorità pubblica. La Corte di Giustizia, al fine di arginare tale pericolo, avrebbe dovuto opportunamente evidenziare un aspetto procedurale importante suggerito dall'Avvocato Generale nelle sue conclusioni (*Conclusioni AG C 18-18*, par. 65): vale a dire quello della necessità di un meccanismo di controllo sull'operato dei fornitori di ospitalità rispetto alla censura dei contenuti degli utenti che potrebbe garantirsi per mezzo della possibilità di ricorso contro suddetta rimozione. Per tali asserzioni di commento alla pronuncia della Corte europea, si rinvia a M. MONTI, *La Corte di giustizia, la direttiva e-commerce*, cit.

⁷⁸ Secondo l'autorevole insegnamento di P. Perlingieri. Per i riferimenti bibliografici cfr. nt. 2.

⁷⁹ Per le considerazioni che seguono cfr. B. PANATTONI, *Il sistema di controllo successivo*, cit., pp. 255, 256.

gamento eccessivo dei tempi di reazione dell'autorità giudiziaria. Per tale ragione è necessario garantire la tempestiva rimozione dei contenuti illeciti che superi le lungaggini di procedure istituzionali formali.

In tale ottica, quando il contenuto pubblicato sia “manifestamente illecito” – sia quando offenda diritti della personalità umana, sia quando determini una violazione di diritti di natura patrimoniale-, sarebbe «irrazionale» attendere un ordine dell'autorità amministrativa o giudiziaria: in attesa di tale intervento, potrebbe, effettivamente, accadere che i diritti in questione vengano irrimediabilmente pregiudicati e non siano, di seguito, più suscettibili di ristoro⁸⁰.

Quanto, poi, alle critiche mosse dai sostenitori di una posizione interpretativa più rigorosa, in merito al pericolo di ‘privatizzazione della censura’ del pensiero manifestato dagli utenti in rete, può risponderci che esso viene superato dalla circostanza che l'utente, il cui contenuto pubblicato sul portale dovesse essere rimosso o al quale si dovesse disabilitare l'accesso, potrà, pur sempre, avviare una procedura di ricorso all'autorità giudiziaria contro la decisione presa dall'*hosting provider*, al fine di dimostrare l'assenza dei presupposti di un intervento ‘oscurante’ da parte di quest'ultimo.

⁸⁰ Si riprende una delle sei argomentazioni addotte dalla pronuncia del Trib. Napoli Nord, sez. civ., II, 3 novembre 2016, cit. che, per giustificare la non indispensabilità di un ordine specifico dell'autorità competente per la rimozione del contenuto illecito, fa preciso riferimento alla lesione dei diritti della personalità umana – quali il diritto all'immagine, al decoro, alla reputazione, alla riservatezza. Si crede che debba pervenirsi alla medesima conclusione, quand'anche vengano lesi, in maniera “manifestamente” illecita, diritti di natura patrimoniale. Si pensi ai contenuti diffamatori del diritto alla reputazione delle imprese che ha, senza dubbio, una connotazione di natura patrimoniale, giacché la sua lesione incide sul valore competitivo e sull'aspettativa di guadagno della stessa (sul tema, si v. *amplius* Ar. FUSARO, *Informazioni economiche e “reputazione d'impresa” nell'orizzonte dell'illecito civile*, Torino, 2010, *passim*). Un esempio sono le recensioni su ristoranti o strutture recettive che vengano fatte su *Tripadvisor* e che, al di là della veridicità dei contenuti, siano, per le modalità espressive impiegate, di per sé “manifestamente illecite”, in quanto evidentemente diffamatorie: a titolo esplicativo, si pensi alle espressioni quali “ladri, ladri, ladri”. Sul punto è di sicuro interesse la sentenza della Cass. pen., sez. V, 19 novembre 2018- 23 gennaio 2019, n. 3148, pubblicata in http://www.dirittoegustizia.it/allegati/15/0000083521/Corte_di_Cassazione_sez_V_Penale_sentenza_n_3144_19_dep_ositata_il_23_gennaio.html. La Suprema Corte ha chiarito la cornice entro la quale possa estrinsecarsi il diritto di critica, secondo modalità che non integrino gli estremi del reato di diffamazione. Dall'articolazione della motivazione è emerso come la violazione dei limiti alla libertà di espressione si riverberi altresì, dal punto di vista applicativo, sul piano civilistico, determinando la sussistenza degli elementi costitutivi del fatto illecito “manifesto”, con le conseguenze che ne derivano, nella materia *de qua*, sul piano della responsabilità civile del *provider*. Per un approfondimento della tematica degli strumenti di tutela della reputazione digitale d'impresa, mi si consenta di rinviare a G. D'ALFONSO, *Recensioni ‘diffamatorie’ in rete e lesione della reputazione digitale d'impresa. Illecito aquiliano e valutazione comparativa degli interessi dell'impresa e degli internauti, alla luce degli indirizzi giurisprudenziali sui limiti all'esercizio del diritto di critica*, in *Diritto mercato e tecnologia*, 15 ottobre 2019.

Si consideri, ancora, che l'orientamento maggioritario della giurisprudenza di merito è consolidato dalla posizione assunta sul tema dai giudici di legittimità, con una pronuncia di indirizzo delle decisioni delle corti di merito.

Si fa riferimento alla sentenza della Cass. civ., sez. I, del 19 marzo 2019, n. 7708 (*supra* menzionata) che ha stabilito che l'*hosting provider*, anche passivo (nel caso specifico *Yahoo*), è corresponsabile, insieme all'utente che abbia caricato sulla piattaforma contenuti protetti dal diritto d'autore, per la loro mancata rimozione "immediata", nonché per aver continuato a pubblicarli, quando ricorrano congiuntamente le seguenti condizioni: «a) sia a conoscenza dell'illecito perpetrato dal destinatario del servizio»; «b) l'illiceità dell'altrui condotta sia ragionevolmente constatabile, onde egli sia in colpa grave per non averla positivamente riscontrata, alla stregua del grado di diligenza che è ragionevole attendersi da un operatore professionale della rete in un determinato momento storico» e «c) abbia la possibilità di attivarsi utilmente, in quanto reso edotto in modo sufficientemente specifico dei contenuti illecitamente immessi da rimuovere»⁸¹. La Suprema Corte riconosce, in sostanza, che la «conoscenza effettiva» possa derivare da qualsiasi tipo di comunicazione, non, perciò, in maniera esclusiva, da un ordine di diffida emanato da un'autorità competente.

Rappresenta, inoltre, senza dubbio, argomentazione a supporto dell'orientamento giurisprudenziale maggioritario la circostanza che esso si ponga nel solco del principio espresso dalla Corte di Giustizia dell'Unione Europea che, in assenza di un'univoca regolamentazione della procedura di segnalazione e rimozione, ha fornito ai giudici nazionali alcune linee interpretative, adottando un approccio caso per caso nel valutare quali atti siano configurabili come segnalazione rilevante, ai fini di far sorgere, in capo ai *providers*, un dovere di rimozione dei contenuti o di disabilitazione al loro accesso⁸².

La Corte di Giustizia europea, nell'interpretare la nozione di «effettiva conoscenza», ha precisato, in una decisione ben nota⁸³, come il regime speciale di responsabilità

⁸¹ Cfr. M. IASSELLI, *Responsabilità del provider: la Cassazione detta rilevanti principi di diritto*, in <https://www.altalex.com/documents/news/2019/03/20/diritto-d-autore-responsabilita-dell-hosting-provider>.

⁸² Si v. A. QUARTA, *La responsabilità civile*, cit., p. 290.

⁸³ Cfr. Corte giust. (Grande sezione), 23 marzo 2010 (domande di pronuncia pregiudiziale, proposte dalla *Cour de Cassation* - Francia), cause riunite da c. 236/08 a c. -238/08, *Google France SARL e Google Inc. c. Louis Vuitton Malletier SA* (c. 236/08), *Google France SARL c. Viaticum SA e Luteciel SARL* (c. 237/08), *Google France SAR c. Centre National de recherche en relations humaines (CNRRH) SAR, Pierre Alexis Thonet, Bruno Raboin e Tiger SARL* (c. 238/08). Si v. il punto 109 della decisione.

dell'*hosting provider*, di cui all'art. 14 della «direttiva sul commercio elettronico», non si applichi qualora costui ometta di rimuovere i dati pubblicati sul sito o di disabilitarne l'accesso «immediatamente», seppure abbia acquisito conoscenza della natura illecita degli stessi o dell'attività del destinatario del servizio, «mediante informazione fornita dalla persona lesa o in altro modo». Alla medesima stregua, in una successiva pronuncia⁸⁴, la Corte di Giustizia europea ha sostenuto che, ai fini dell'«effettiva conoscenza», è sufficiente che il *provider* sia al corrente di fatti o circostanze, in base alle quali un operatore economico diligente avrebbe dovuto constatare l'illiceità del contenuto pubblicato, specificando che la disposizione, di cui all'art. 14, comma 1, lett. a), debba essere interpretata nel senso che riguardi «qualsiasi situazione nella quale il prestatore» venga «ad essere, *in qualunque modo*, al corrente di tali fatti o circostanze».

Si tenga altresì conto della circostanza di notevole rilievo che il legislatore europeo ha dettato una disciplina 'speciale' che prevede l'obbligo di attivazione del *provider*, a seguito di segnalazione da parte del privato che assuma essere stato lesa dal contenuto illecito ivi pubblicato. Si fa riferimento alla nuova disciplina, dettata dalla direttiva (UE) del Parlamento europeo e del Consiglio del 17 aprile 2019, n. 790, sul diritto d'autore e sui diritti connessi nel mercato digitale unico⁸⁵, c.d. «direttiva *copyright*» che ha riconosciuto, a determinate condizioni, la sussistenza della responsabilità civile di determinate categorie di *providers* che non agiscano tempestivamente per disabilitare l'accesso o rimuovere dal proprio sito contenuti illeciti, «dopo aver ricevuto una segnalazione sufficientemente motivata dai titolari del diritto».

La normativa, nel porsi l'obiettivo di realizzare un processo di modernizzazione della tematica del *copyright*, ha dettato una serie di disposizioni, miranti alla «responsabilizzazione» dei prestatori di servizi *internet* che consentano ai propri utenti la pubblicazione e la condivisione *online* di contenuti protetti da *copyright*, fornendo l'accesso al pubblico, ogni qualvolta

⁸⁴ Cfr. Corte giust., 12 luglio 2011, *l'Oréal SA e altri c. eBay International AG.*, C-342/09, cit., punti 120 e 121.

⁸⁵ La Direttiva (UE) 2019/790 modifica la direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati e la direttiva 2001/29/CE del Parlamento europeo e del Consiglio, del 22 maggio 2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione.

svolgano un «ruolo attivo» (anche per mezzo dell'«ottimizzazione della presentazione dei materiali» o della «loro promozione») ⁸⁶.

L'art. 17 della direttiva introduce un nuovo tipo di responsabilità delle «piattaforme online di condivisione di contenuti», disponendo che il *provider* «attivo» sia responsabile «*ipso facto*», quando il contenuto illecito sia immesso in rete dai propri utenti, come semplice conseguenza del caricamento sul portale. Si delinea, in tal guisa, una responsabilità *ex ante*, diversamente dalla disciplina generale della responsabilità civile degli *internet service providers* che, come detto, opera invece *ex post* ⁸⁷.

Al fine di evitare tale responsabilità, il *provider* dovrà adottare una serie di misure volte ad impedire il caricamento di contenuti illeciti sul portale gestito. In sostanza, graverà sui prestatori di servizi di condivisione di contenuti *online* l'obbligo di ottenere da parte dei titolari di diritti «l'autorizzazione» di comunicazione al pubblico, compresa la messa a disposizione del pubblico di opere e altri materiali protetti dal diritto d'autore, ad esempio mediante un accordo di licenza ⁸⁸.

In assenza di «autorizzazione» dei titolari dei diritti, il *provider* sarà responsabile «per atti non autorizzati di comunicazione al pubblico, di opere e altri materiali protetti dal *copyright*», a meno che non dimostri congiuntamente: di aver compiuto i «massimi sforzi», per ottenere la suddetta autorizzazione; di avere effettuato, nel rispetto di «elevati *standard* di diligenza professionale di settore», i massimi sforzi per assicurare che non siano disponibili le opere e materiali specifici, per i quali abbia ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti; in ogni caso, di aver agito tempestivamente, «dopo aver ricevuto una segnalazione sufficientemente motivata dai titolari del diritto», per disabilitare l'accesso o rimuovere dal proprio sito *web* le opere o altri materiali «oggetto di segnalazione» ed aver compiuto i massimi sforzi per impedire che vengano caricati in futuro ⁸⁹.

⁸⁶ Cfr. V. FALCE, *Direttiva Copyright 2019: fair use ed eccezioni al copyright tra esigenze di «apertura» e necessità di indirizzo*, in *www.filodiritto.com*, 29 luglio 2019.

⁸⁷ Cfr. I. GENNA, *Copyright, tutti i nodi della direttiva per il recepimento in Italia e gli impatti prevedibili*, 1 aprile 2019, in *www.agendadigitale.eu*

⁸⁸ Tale autorizzazione include altresì gli atti compiuti dagli utenti che non agiscono su base commerciale oppure la cui attività non generi ricavi significativi. Cfr. M. ZANCAN, *La nuova direttiva sul diritto d'autore e sui diritti connessi nel mercato unico digitale*, 23 luglio 2019, in *www.medialaws.it*

⁸⁹ A. QUARTA, *La responsabilità civile*, cit., p. 302, evidenzia come la disciplina dettata dall'art. 17 della «direttiva *Copyright*», nel definire in modo più stringente il regime di responsabilità del *provider* per la violazione del diritto d'autore, si differenzi da quella applicabile nelle ipotesi di violazione dei diritti della personalità, cui resta

Con riferimento a tale ultima disposizione⁹⁰, si noti, in primo luogo, che la norma non fa riferimento a contenuti illeciti, bensì a contenuti “*oggetto di segnalazione*”, con la conseguenza che ciò che rileva, ai fini dell’attivazione del *provider* non è l’illiceità –e, dunque, una valutazione che in tal senso venga effettuata da un’autorità competente, con successivo ordine imposto al gestore del sito di intervenire sul contenuto ivi pubblicato-, bensì la valutazione che della stessa venga effettuata dal titolare dei diritti. In secondo luogo, all’obbligo di rimozione e di disabilitazione all’accesso del contenuto, già esistente nella disciplina generale dettata dalla direttiva 2000/31/CE, si aggiunge l’obbligo del *provider* di compiere i massimi sforzi per impedire il caricamento in futuro del contenuto segnalato. Si tratta del c.d. «*notice and stay down*» che prevede, per l’appunto, che il prestatore di servizi debba non solo rimuovere il contenuto segnalato, ma anche prodigarsi affinché esso non venga ricaricato nei *server*: ragion per cui si dovrà attivare per controllare tutti i contenuti che vengano ivi immessi⁹¹.

Si contempi, a titolo di esaustività, che l’art. 17, comma 5 della direttiva c.d. *copyright*, nell’ottica della responsabilizzazione dell’*hosting provider*, stabilisce che l’autorità giudiziaria, nel valutare se costui si sia conformato agli obblighi menzionati, dovrà vagliare, alla stregua del «principio di proporzionalità», i seguenti elementi: il tipo di opere caricate, il pubblico e la dimensione del servizio e la tipologia di opera o altri materiali caricati dagli utenti del servizio; la disponibilità ed il costo di strumenti adeguati ed efficaci per i prestatori di servizi⁹².

applicabile, in maniera esclusiva, la regolamentazione stabilita dalla «direttiva sul commercio elettronico». Sarebbe, di conseguenza, necessario un intervento di coordinamento tra l’art. 17 della Direttiva *Copyright* ed il regime speciale previsto dalla direttiva 2000/31/CE, in quanto la normativa più recente ha introdotto nuove clausole di esonero di responsabilità.

⁹⁰ Per le osservazioni che seguono, si v. B. SAETTA, *Le criticità della direttiva copyright. Analisi dell’articolo più controverso*, in <https://www.valigiablu.it/direttiva-copyright-articolo13>, 14 aprile 2019.

⁹¹ Tale approccio è già stato adottato dalla Corte di Giustizia europea che, nelle due sentenze Sabam (Corte giust. (Terza Sez.), 24 novembre 2011, c.70/10, *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*; Corte giust. (Terza Sez.), 16 febbraio 2012, causa C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) c. Netlog NV*), ha puntualizzato come, sebbene il monitoraggio globale sia in violazione delle norme comunitarie, ciononostante debba ammettersi un monitoraggio specifico ad un singolo contenuto, purché di ordine temporaneamente limitato. Deve, ad ogni modo, evidenziarsi che la direttiva *copyright* non ha, piuttosto, previsto limiti di tempo. Si v. B. SAETTA, *Le criticità della direttiva copyright*, cit.

⁹² Con la conseguenza di una rilevante limitazione degli obblighi nei confronti di *start up* e di piccole e medie imprese, tenendo conto delle tempistiche del loro operato, del loro fatturato e del numero di visualizzazioni individuali. Cfr. M. ZANCAN, *La nuova direttiva sul diritto d’autore*, cit.

In via conclusiva, pur concordandosi con l'interpretazione della giurisprudenza maggioritaria italiana che propende per la sufficienza della segnalazione del privato ai fini della sussistenza dell'effettiva conoscenza dell'*hosting provider*, si ritiene di pregnante importanza arginare il rischio che costui, nell'accogliere indistintamente tutte le segnalazioni che gli vengano rivolte da parte di privati, finisca con l'assumere il ruolo di "censore privato" sui contenuti pubblicati sui portali.

A tal uopo, possono prospettarsi una serie di accorgimenti.

In primis, il fornitore di ospitalità dovrebbe chiarire, fornendo delle informazioni sul proprio sito, i requisiti ed i presupposti di operatività del meccanismo di notifica e rimozione dei contenuti illeciti, specificando, innanzitutto, che la segnalazione debba presentare un contenuto minimo necessario, al fine di essere sottoposta ad una verifica. Come già asserito in talune sentenze, la diffida del titolare dei diritti dovrebbe, per l'appunto, contenere «contestazioni specifiche e puntuali» e precisare gli estremi identificativi dei contenuti illeciti da rimuovere⁹³.

Nei casi, poi, in cui l'utente che abbia pubblicato il contenuto potenzialmente offensivo per i terzi sia facilmente identificabile in rete⁹⁴, il fornitore di ospitalità potrebbe adottare la *policy* di accogliere le segnalazioni degli utenti che assumano essere stati lesi, solo qualora dimostrino di aver previamente segnalato il problema al potenziale danneggiante, richiedendogli la rettifica delle informazioni pubblicate ovvero la loro rimozione dal sito, e dichiarino, sotto propria responsabilità, di non avere ricevuto alcuna risposta.

⁹³ Si v. l'ordinanza Trib. Roma, 20 ottobre 2011, cit.; la sentenza App. Milano, sez. impr., 7 gennaio 2015, n. 29, cit.; la sentenza Trib. Roma, sez. impr., 27 aprile 2016, n. 8437, cit. Si v. App. Roma, sez. I civ., 19 febbraio 2018, n. 1065, riguardante un caso di diffamazione *online*, secondo la quale, dal momento che i contenuti non apparivano di per sé ingiuriosi, tanto da imporre l'attivazione del *provider*, senza un ordine dell'autorità competente, la presunzione effettiva di conoscenza di quest'ultimo sarebbe potuta derivare unicamente da una segnalazione dettagliata, contenente «le singole affermazioni ritenute non veritiere; le ragioni della asserita falsità e le fonti idonee a provarlo; 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 sarebbe potuto procedere alla modifica richiesta. Cfr. <http://www.medialaws.eu/wp-content/uploads/2018/05/CA-Roma-sentenza-1922018-Wikimedia-Previti.pdf>

⁹⁴ Sulla problematicità dell'identificazione degli autori delle recensioni e la conseguente questione dell'imputabilità della responsabilità civile in capo ai gestori delle piattaforme digitali che autorizzino la pubblicazione di commenti anonimi o con pseudonimo, mi si consenta di rinviare a G. D'ALFONSO, *Anonimato in rete e responsabilità civile dell'hosting provider nella prospettiva de jure condendo*, in *Diritto mercato tecnologia*, 10 settembre 2019, p. 28 ss.

Si ritiene, infine, opportuno, nell'ottica di preservare la connotazione della rete quale *marketplace of ideas*, 'agorà' virtuale nella quale gli utenti possano liberamente esprimere il proprio pensiero, pur sempre nel rispetto della legalità, che i numerosi gestori delle piattaforme digitali che offrano servizi ai nostri cittadini (e non solo) impieghino delle *policies* di gestione dei reclami quanto più uniformi tra loro, circostanza dalla quale deriverebbe che gli utenti si sentirebbero realmente liberi di spaziare nel *web* e scegliere, senza riserve, tra i numerosi portali ivi presenti. La soluzione più semplice da prospettare, a tal fine, consiste nell'adozione, da parte dei fornitori di ospitalità, di accordi di autoregolamentazione nei quali prevedere delle linee guida comuni da impiegare nel trattamento dei reclami.

4. *Le spinte in ambito europeo verso l'adozione di meccanismi di «notice and take down». La portata dell'incisività degli atti di soft law e la necessità di una riforma sistematica*

È questa, d'altronde, una delle proposte formulate dalle Istituzioni Europee in una serie di atti di *soft law*⁹⁵, nei quali la Commissione ha fornito agli Stati membri incisivi *incipit*

⁹⁵ Si precisa (A. ALGOSTINO, *La soft law comunitaria e il diritto statale: conflitto fra ordinamenti o fine del conflitto democratico?* in *www.costituzionalismo.it*, 2016, fasc. 3, p. 256, pp. 258 ss., 267-268) che la locuzione «*soft law*» si riferisce ad una pluralità di atti eterogenei che, «nella duttilità e flessibilità di forme e legittimazione», presentano l'elemento in comune di esercitare effetti giuridici rilevanti, sebbene non abbiano efficacia giuridica vincolante. In tale contesto, la *soft law* può scaturire sia dalle istituzioni pubbliche, sia da soggetti privati, sia dalla combinazione dell'operato dei soggetti pubblici o privati. In riferimento a quest'ultimo profilo, la dottrina menziona, a titolo esplicativo, i Principi *Unidroit*, elaborati in materia di contratti del commercio internazionale, da parte dell'Istituto internazionale per l'Unificazione del Diritto privato (un'organizzazione intergovernativa indipendente), che raccolgono e coordinano la *lex mercatoria*, finendo col costituire una sorta di *Restatement* delle prassi commerciali dei *global players* internazionali. Tali principi non sono giuridicamente vincolanti, eppure vengono applicati ad ampio raggio negli arbitrati internazionali (*ex multis*, si v., tra i numerosi contributi sul tema dell'autore, F. GALGANO, *Lex mercatoria*, Bologna, 2010, p. 252 ss). I Principi *Unidroit* rappresentano, quindi, un caso emblematico di *soft law*. Tale ricostruzione è in linea con l'insegnamento (T.E. FROSINI, *Legislazione e comparazione*, in *Dir. Pubbl. Comp. ed Europeo*, n. 1/2015, p. 6; ID., *Diritto comparato e diritto globale*, in M. BRUTTI e A. SOMMA (a cura di), *Diritto: storia e comparazione. Nuovi propositi per un binomio antico*, Global Perspectives on Legal History, A Max Plank Institute for European Legal History, volume 11, in <http://global.rg.mpg.de>, 2018, p. 209), secondo il quale «la c.d. globalizzazione - intesa come "dematerializzazione"» ha condotto al diffondersi di «nuove e varie fonti del diritto come la *soft law*» che si espandono sempre più, senza limiti territoriali. Esse «sono frutto di una prassi giuridica che altera la gerarchia normativa e che sottrae agli Stati la titolarità del diritto consentendo ad altri soggetti, soprattutto privati, di partecipare attivamente alla produzione del diritto». Altra dottrina (A. POGGI, *Soft law nell'ordinamento comunitario*, in *www.astridonline*, p. 4 che condivide la ricostruzione di L. SELDEN, *Soft Law in European Community Law*, Oxford, 2004, p. 112) ha puntualizzato come gli atti di *soft law* vengano normalmente classificati, sulla base della funzione che svolgono, in tre categorie: gli atti di «*pre-law*» -ossia gli strumenti preparatori di atti giuridici vincolanti, come i Libri Bianchi, Libri Verdi-; gli atti di «*post-law*» -vale a dire gli strumenti di interpretazione di atti vincolanti, quali le comunicazioni interpretative, le linee guida ed i codici di condotta- e gli atti di «*para-law*» qualificabili come strumenti alternativi ad atti vincolanti, tra i quali si fanno rientrare le comunicazioni non interpretative, le raccomandazioni ed i pareri.

nella promozione di una responsabilizzazione degli *hosting service providers*, maggiore rispetto a quella prevista dalla disciplina attualmente vigente, suggerendo precipuamente agli Stati membri e a questi ultimi l'adozione di procedure trasparenti ed efficienti di «*notice and take down*».

L'obiettivo perseguito da tali atti è la modernizzazione della normativa, in considerazione dell'evoluzione tecnologica che si è avuta, rispetto al momento dell'emanazione della «direttiva *e-commerce*», e di aggiornamento della stessa, al fine di colmare le lacune e superare le incertezze sollevate, nel corso del tempo, dall'applicazione della disciplina europea e delle legislazioni nazionali di recepimento.

Per questa via, la Commissione Europea, il 6 maggio 2015, ha emanato una Comunicazione⁹⁶ al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle regioni, dal titolo «Strategia per il mercato unico digitale»⁹⁷. Al punto 3.3.2. «Contrasto ai contenuti illeciti su *internet*», la Commissione Europea, nel constatare che, in più della metà dei casi, gli interventi contro i contenuti illeciti sono spesso inefficaci e poco trasparenti e che le divergenze tra le diverse prassi nazionali possono ostacolare il rispetto delle norme e minare la fiducia degli utenti nel mondo *online*, ha posto la questione sull'opportunità di innalzare il livello generale di protezione dal materiale illecito su *internet*. La Commissione si è riproposta, pertanto, di vagliare l'esigenza di presentare nuove misure, al fine di fronteggiare i contenuti illeciti in *internet* e di valutare, a tale scopo, l'opportunità di imporre ai *providers* «di esercitare una maggiore responsabilità e diligenza nella gestione delle reti e dei sistemi (doveri di diligenza)».

Di qui hanno fatto seguito ulteriori interventi della Commissione europea.

Si segnala la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, del 28 settembre 2017, dal titolo «Lotta ai contenuti illeciti *online*. Verso una maggiore responsabilizzazione delle piattaforme *on line*», *supra* menzionata.

⁹⁶ Si ritiene (A. POGGI, *Soft law nell'ordinamento comunitario*, cit., p. 18) che le Comunicazioni costituiscano la tipologia di *soft law* più consistente nei settori strategici per la realizzazione del mercato comune: esse sono infatti costruite con la finalità di indirizzare, in determinati settori, l'attività degli Stati membri e dei soggetti privati – nel caso specifico, gli *internet service providers*.

⁹⁷ Documento COM (2015) 192 *final*.

La Commissione europea si è impegnata a verificare l'esigenza di prevedere nuove misure, per garantire l'efficienza e la tempestività degli interventi dei *providers*, non solo nella fase di rimozione dei contenuti illeciti, ma altresì nell'ottica della loro prevenzione. A tal fine, si delinea la valutazione dell'adozione di eventuali misure legislative da parte degli Stati membri, al fine di aggiornare ed adeguare il quadro normativo attualmente vigente⁹⁸.

La Comunicazione⁹⁹ ha offerto una serie di orientamenti e principi, per indirizzare gli *hosting providers* ad incrementare la lotta contro i contenuti illeciti *online*, in cooperazione con le autorità nazionali, con gli Stati membri e con i portatori di interessi pertinenti. Si è posta la finalità di agevolare ed intensificare l'attuazione di "buone pratiche", non solo al fine di rimuovere e disabilitare l'accesso a contenuti illeciti che siano stati segnalati ai *providers*, ma anche per individuarli e prevenirli, mediante l'impiego, da parte di questi ultimi, di «misure proattive». La Commissione ha rilevato come le piattaforme digitali dispongano, ad oggi, solitamente di «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'utilizzo delle tecnologie di individuazione e di filtraggio automatico sta divenendo uno strumento ancora più importante, per contrastare i contenuti illeciti *online*.

Alla Comunicazione ha fatto seguito la Raccomandazione (UE), 1 marzo del 2018, n. 334, della Commissione Europea «sulle misure per contrastare efficacemente i contenuti illeciti *on line*».

Tale atto¹⁰⁰ si è posto nel solco dell'orientamento politico già enunciato dalla Commissione Europea nella Comunicazione del 2017, con l'obiettivo di darvi concreta attuazione. Il provvedimento, seppur privo, *ex art.* 288 del TFUE, di efficacia vincolante nei confronti degli Stati membri dell'Unione Europea ai quali è diretto, sebbene inidoneo ad imporre obblighi giuridici, ha ciononostante posto una serie di principi comuni non vincolanti, suggerendo loro delle linee guida di azione¹⁰¹.

⁹⁸ Si v. M. MAZZONETTO, *Il problema dei contenuti illegali on-line: la risposta della Commissione Europea*, 29 marzo 2018, in www.dirittodellinformatica.it. Si v. anche A. QUARTA, *La responsabilità civile*, cit., p. 294 ss.

⁹⁹ Come precisato nel punto 1 «Introduzione».

¹⁰⁰ Sul punto si v. M. MAZZONETTO, *Il problema dei contenuti illegali on-line*, cit.

¹⁰¹ La raccomandazione è una fonte del diritto europeo, qualificabile, come visto, come atto di *soft law*. Tale provvedimento può essere rivolto sia agli Stati membri, sia ai soggetti di diritto interno, operanti nel settore di riferimento. La raccomandazione permette alle istituzioni europee di rendere note le proprie posizioni sull'evoluzione futura della propria azione e di suggerire linee di azione, senza imporre obblighi giuridici a ca-

Il provvedimento incisivamente esordisce, al punto 1, Capo I, «Obiettivo e definizioni», dichiarando che, in riferimento ai contenuti pubblicati dagli utenti delle piattaforme digitali, gli Stati membri ed i fornitori del servizio di ospitalità sono «incoraggiati ad adottare misure effettive, appropriate e proporzionate», per contrastare i contenuti illeciti *on line*, in conformità ai principi stabiliti nella Raccomandazione stessa¹⁰².

Si prevede¹⁰³ «un doppio canale di misure», destinate ad elevare gli *standard* di diligenza degli *hosting providers*: ossia interventi sia *ex post*, sia *ex ante*.

Sul piano della prevenzione, la Commissione, al fine di garantire una risposta più rapida nella rilevazione e successiva rimozione dei contenuti illeciti, prevede innanzitutto il rafforzamento: della collaborazione tra i prestatori di servizi di *hosting* che, ove opportuno, dovrebbero condividere tra loro esperienze, soluzioni tecnologiche e le “buone pratiche”, anche dando luogo ad iniziative di cooperazione, relative a codici di condotta, protocolli d’intesa ed altri accordi volontari¹⁰⁴; della collaborazione tra *hosting providers* e gli Stati membri che dovrebbero predisporre procedure accelerate, per trattare le segnalazioni che provengano dalle autorità competenti¹⁰⁵; della collaborazione tra gli *hosting providers* ed i «segnalatori attendibili» («comprese le organizzazioni non governative e le associazioni di categoria») ¹⁰⁶, realizzabile tramite la previsione di procedure accelerate, per il trattamento delle segnalazioni di questi ultimi, e la pubblicazione di condizioni chiare e obiettive, per stabilire quali soggetti, che dispongano di competenze necessarie e svolgano la propria attività in modo diligente, possano essere così qualificati¹⁰⁷.

Il provvedimento, facendo proprio il contenuto della Comunicazione, promuove in maniera più analitica l’adozione, da parte degli *hosting providers*, di «misure proattive oppor-

rico dei destinatari. Sul punto si v. G. TESAURO, *Diritto comunitario*, Padova, 2003, pp. 144-146; https://europa.eu/european-union/eu-law/legal-acts_it.

¹⁰² Oltre che nel rispetto della Carta dei diritti fondamentali dell’Unione Europea: precisamente nel rispetto del diritto alla libertà di espressione e di informazione (*ex art.* 10), del diritto alla protezione dei dati personali (*ex art.* 8) e di altre disposizioni europee, relative al commercio elettronico ed alla concorrenza.

¹⁰³ Sul punto, si mutuano le notazioni di G. GIANNONE CODIGLIONE, *La nuova legge tedesca*, cit., p. 734 s.), di commento alla Comunicazione COM (2017) 555 *final*, *supra* menzionata.

¹⁰⁴ Coinvolgendo, in particolare, gli *hosting providers* che abbiano risorse limitate, in ragione della loro dimensione o della scala sui cui operino. Si v. punto 28, Capo II, «Collaborazione tra prestatori di servizi di *hosting*».

¹⁰⁵ Si v. punto 23, Capo II, «Collaborazione tra prestatori di servizi di *hosting* e gli Stati membri».

¹⁰⁶ Si v. considerando 29 della Raccomandazione.

¹⁰⁷ Si v. i punti 25, 26, 27, Capo II, «Collaborazione tra i prestatori di servizi di *hosting* e i segnalatori attendibili».

tune, proporzionate e specifiche» che siano efficaci, nell'individuare e rimuovere i contenuti illeciti, per ridurre i rischi di lesione dei diritti di terzi¹⁰⁸. Tali misure potrebbero comprendere l'uso di strumenti automatizzati, solo quando ciò risulti «appropriato e proporzionato», in taluni casi sotto il controllo dell'intervento umano, e pur sempre a condizione che siano accompagnate da «garanzie effettive ed appropriate», in particolare da «misure di salvaguardia», di cui ai punti 19 e 20¹⁰⁹.

Nell'ambito delle misure operative che gli *hosting providers* debbano adottare *ex post*, la Raccomandazione, al fine di aumentare le tutele dei soggetti danneggiati dagli utenti delle piattaforme digitali, stimola, in primo luogo, l'impiego di misure idonee a garantire una risposta più veloce ed efficace, sia nel rilevare, sia nel rimuovere i contenuti illeciti, pubblicati sui portali: ossia meccanismi «di facile accesso e uso» e chiari, preposti alla raccolta di segnalazioni che devono essere adeguatamente motivate e sufficientemente dettagliate (con chiara indicazione dell'ubicazione dei contenuti), per permettere al prestatore di servizi di prendere «una decisione coscienziosa ed informata»¹¹⁰.

Inoltre, per aumentare la trasparenza, si invitano gli Stati membri ad incentivare i *providers* a pubblicare descrizioni chiare e particolareggiate sulla loro politica di rimozione e disabilitazione all'accesso di contenuti illeciti e a prevedere l'obbligo, per costoro, di pubblicare relazioni su tale attività¹¹¹.

Preme sottolineare che la Raccomandazione, nel disciplinare la segnalazione dei contenuti illeciti ai *providers*, non menziona l'ordine dell'autorità competente: circostanza dalla quale può argomentarsi, *a contrario*, che, ai fini dell'intervento del *provider* di rimozione o disabilitazione all'accesso del contenuto illecito, non si configuri la necessità dell'emanazione dell'ordine preliminare dell'autorità giudiziaria o amministrativa.

¹⁰⁸ Si v. punto 18, Capo II, «Misure proattive».

¹⁰⁹ Il punto 19 precisa come tali misure dovranno garantire un intervento diligente e proporzionato da parte degli *hosting providers* sia durante il trattamento di segnalazioni, sia in fase di decisione di rimozione di contenuti illeciti o di disabilitazione al loro accesso. Il punto 20 puntualizza che l'utilizzo di strumenti automatizzati, da parte degli *hosting providers*, in relazione ai contenuti memorizzati, dovrà essere accompagnato dalla predisposizione di garanzie, quali la verifica e la sorveglianza umana, ove opportuna.

¹¹⁰ Si v. Considerando 17 della Raccomandazione.

¹¹¹ Si v. Capo II, «Trasparenza» che precisa che le relazioni dovrebbero contenere informazioni sulla quantità e sul tipo di contenuti rimossi, sul numero di segnalazioni e di repliche ricevute e sul tempo necessario per intervenire.

Avendo, poi, riguardo all'esigenza di bilanciare gli interessi di coloro che assumono essere stati lesi da contenuti illeciti e gli interessi dei fornitori degli stessi, la Raccomandazione mira a garantire il contraddittorio, contemplando il diritto di replica di questi ultimi che il *provider* è obbligato ad informare della segnalazione ricevuta, qualora sia a conoscenza dei loro recapiti¹¹².

Il provvedimento invita, altresì, gli Stati membri ad agevolare la soluzione stragiudiziale delle controversie, relative alla rimozione di contenuti illegali o alla disabilitazione dell'accesso ai medesimi, ed incoraggia gli *hosting providers* a consentire l'uso di meccanismi per la risoluzione stragiudiziale medesima, se disponibile negli Stati membri¹¹³.

Si osservi, infine, che la Raccomandazione non pone in discussione il regime speciale di responsabilità degli *internet service providers*, in linea con la Comunicazione 28 settembre 2017, ove si puntualizza che l'adozione di misure proattive da parte dei *providers* non implica, di per sé, automaticamente che l'*hosting provider* vada collocato tra gli *hosting* "attivi", con la conseguente perdita del beneficio dell'assoggettabilità dello stesso al regime speciale di responsabilità civile, tracciato dalla direttiva europea. La Commissione ha chiarito (punto 3.3.1.) che i fornitori di ospitalità non dovranno essere scoraggiati, nell'adozione di misure proattive efficaci, dal timore della perdita del beneficio della deroga alla responsabilità civile¹¹⁴.

La Commissione europea non intende, di fatto, sovvertire il «regime di favore», introdotto dalla disciplina europea della responsabilità civile degli *internet service provider*, e ciò appare evidente dalla circostanza che le «misure proattive» previste non intaccano il principio generale, in forza del quale non gravi, in capo a nessuno dei fornitori di servizi *on line*, né l'obbligo generale di sorveglianza delle informazioni che trasmettono e memorizzano, né

¹¹² Ad eccezione delle ipotesi in cui si tratti di reati gravi che comportino una minaccia per la vita o la sicurezza delle persone oppure sussistano motivi di ordine pubblico o di pubblica sicurezza, in particolare di indagini e prevenzione. Si v. i punti 9-13, Capo II, «Informazione dei fornitori di contenuti e repliche». Sempre riguardo a tale aspetto, il punto 24 stabilisce che, qualora vi siano prove di reati gravi o il sospetto di minacce per la vita o per la sicurezza delle persone, derivanti dalla diffusione *online* di contenuti illegali, i *providers* sono obbligati ad informare immediatamente le autorità competenti.

¹¹³ Si v. i punti 14, 15, Capo II, «Risoluzione extragiudiziale delle controversie».

¹¹⁴ Tanto più che tali obblighi preventivi sembrano collocarsi nell'ambito del considerando n. 48 della direttiva 2000/31/CE che prevede che la medesima non pregiudica la possibilità degli Stati membri di chiedere ai prestatori di servizi, che abbiano informazioni sui loro utenti, «di adempiere al dovere di diligenza che è ragionevole attendersi da loro ed è previsto dal diritto nazionale, al fine di individuare e prevenire taluni tipi di attività illecite». In tal senso si v. G. GIANNONE CODIGLIONE, *La nuova legge tedesca*, cit., p. 735, nt. 20.

l'obbligo generale di ricerca attiva di fatti o circostanze che indichino la presenza di attività illecita.

Alla luce di tali osservazioni, può affermarsi¹¹⁵ che la linea direttrice della Raccomandazione sia la promozione della diffusione, su tutto il territorio dell'Unione Europea, di una «responsabilità sociale d'impresa». La Commissione europea stimola la responsabilizzazione sociale degli *hosting providers*, quale strumento che «dal basso» contrasti la diffusione di contenuti illeciti *on line*.

A tal uopo, benché la Raccomandazione non abbia carattere vincolante, non si esclude che possa produrre effetti giuridici a livello nazionale¹¹⁶, sia stimolando gli *hosting providers* ad impiegare le misure operative “virtuose”, delineate dalla Commissione; sia influenzando, sul piano istituzionale, sugli indirizzi delle autorità giudiziarie e sull'evoluzione degli interventi normativi futuri degli Stati membri.

Sotto il primo punto di vista, la responsabilizzazione sociale degli *hosting providers* potrebbe costituire un punto di partenza e di indirizzo per costoro all'impiego di una maggiore diligenza nella gestione delle reti e dei sistemi delle piattaforme digitali. La Commissione stimola tali soggetti all'adozione di protocolli d'intesa, codici di condotta ed accordi privati; anche se deve precisarsi che, senza dubbio, sarebbe più efficace il loro impiego non solo a livello nazionale o europeo, considerando che i maggiori *global players* sono i fornitori di servizi statunitensi. Tali strumenti di autoregolamentazione avrebbero il merito non solo di individuare, prevenire e perciò contrastare i contenuti illeciti, ma anche di arginare il pericolo della perdita di competitività dei fornitori di ospitalità “più attenti” nel contrasto degli illeciti¹¹⁷. Si comprende bene come l'adozione di misure proattive isolatamente, da parte di taluni *providers*, avrebbe difatti l'effetto di indurre gli utenti a stipulare i contratti con le piattaforme digitali “meno attente” al contrasto degli illeciti che non le impieghino, al fine di sentirsi meno controllati sui contenuti da pubblicare e per non correre il rischio della rimozione degli stessi dal sito.

¹¹⁵ Per le notazioni che seguono si v. M. MAZZONETTO, *Il problema dei contenuti illegali on-line*, cit.

¹¹⁶ Secondo l'autorevole insegnamento di G. TESAURO, *Diritto comunitario*, cit., p. 145.

¹¹⁷ Si v. R. NATOLI, *La tutela dell'onore e della reputazione in internet: il caso della diffamazione anonima*, in *Eur. dir. priv.*, 2001, p. 466.

In riferimento al formante legislativo, si precisi che, in realtà, il considerando 41 della Raccomandazione prevede che la Commissione europea monitorerà (oltre alle misure impiegate dagli *hosting providers*) i provvedimenti concretamente assunti dai singoli Stati membri, in risposta alle indicazioni contenute nella medesima.

Si confida sull'effetto "persuasivo" della Raccomandazione che avrà il "potere (europeo) di indirizzo politico" dei legislatori nazionali¹¹⁸. I principi comuni, contenuti nel provvedimento, seppur non vincolanti, costituiranno, senz'altro, linee guida per i legislatori degli Stati membri nella previsione di «misure effettive, appropriate e proporzionate», per fronteggiare i contenuti illeciti *on line*, nell'ottica della maggiore responsabilizzazione degli *hosting providers*.

Due sono le ragioni che inducono a pensare che si approderà a tale risultato.

Si rilevi, anzitutto, che, in tale contesto, si è già creato un circolo "virtuoso" tra la legislazione nazionale e l'operato delle Istituzioni Europee, laddove le istanze di maggiore responsabilizzazione degli *hosting providers*, contenute nella Comunicazione del 2017 e nella Raccomandazione del 2018, ricalcano in certi punti l'approccio normativo del *Netzwerkdurchsetzungsgesetz*, emanato prima di tali provvedimenti¹¹⁹.

È, poi, già accaduto, in altri ambiti, che un provvedimento di *soft law*, quale la Raccomandazione, rendendo nota la posizione delle Istituzioni Europee sull'evoluzione futura della propria azione, senza imporre obblighi giuridici agli Stati membri, li abbia poi influenzati, conducendoli ad emanare provvedimenti legislativi in conformità alle linee di azione ivi suggerite¹²⁰.

¹¹⁸ Pone l'accento sul valore "persuasivo" degli atti di *soft law* R. MANDRELOTI, *Sistema delle fonti e indirizzo politico nelle dinamiche dell'integrazione europea*, Torino, 2004, p. 192. L'autore sostiene che la *soft law*, più che fonte del diritto, sarebbe direttamente collegata al «potere comunitario di indirizzo politico»; ragion per cui gli «atti atipici» costituirebbero «strumenti di diritto mite», corredati di un'efficacia giuridica molto minore rispetto alle fonti tipiche e sarebbero volti a perseguire obiettivi politici, attraverso la loro persuasione.

¹¹⁹ Cfr. G. GIANNONE CODIGLIONE, *La nuova legge tedesca*, cit., p. 734.

¹²⁰ Si fa precipuo riferimento alla Raccomandazione della Commissione europea dell'11 giugno 2013 (2013/396/UE) «relativa a principi comuni per i meccanismi di ricorso collettivo di natura inibitoria e risarcitoria negli Stati membri che riguardano violazioni di diritti conferiti dalle norme dell'Unione», alla quale ha fatto seguito, in linea con l'orientamento politico della Commissione europea di non delimitare lo strumento processuale di tutela collettiva risarcitoria alla sola protezione del consumatore o utente ovvero ad ambiti prettamente settoriali, l'emanazione di provvedimenti innovativi di taluni Stati membri che hanno ampliato l'ambito oggettivo e soggettivo di applicazione della disciplina originaria in materia. Su questa linea, si segnala la legge italiana del 12 aprile 2019, n. 31, recante «Disposizioni in materia di azione di classe», entrata in vigore il 19 aprile del corrente anno; la legge francese la *loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justi-*

Per quanto attiene all'incidenza della Raccomandazione sugli orientamenti giurisprudenziali nazionali¹²¹, assume rilievo specifico il principio espresso, da tempo, dalla Corte giust., (seconda sez.), 13 dicembre 1989, c. 322/88, *Grimaldi c./Fond des maladies professionnelles*¹²², chiamata a pronunciarsi sul valore delle raccomandazioni, nell'ambito di una procedura di rinvio pregiudiziale. In tale sede, dopo aver precisato che tali atti sono normalmente adottati dalle Istituzioni Europee quando non dispongano, in forza del Trattato, del potere di emanare atti obbligatori oppure qualora reputino che non vi sia ragione per adottare atti vincolanti, ha affermato che essi non possono essere considerati privi di effetti giuridici. I giudici nazionali devono, dunque, tener conto delle raccomandazioni, nell'ambito della risoluzione delle controversie sottoposte al loro giudizio, quando esse contribuiscano all'interpretazione sia delle norme nazionali, sia degli altri atti vincolanti europei ovvero al completamento di norme europee, aventi valore vincolante¹²³. Tale obbligo dei giudici nazionali appare, d'altronde, coerente con la necessità del rispetto volontario di atti non vincolanti europei, in quanto «elemento essenziale nella realizzazione degli scopi del Trattato».

ce du XXI^e siècle che ha dettato disposizioni generali sull'*action de groupe devant le juge judiciaire*, pur enunciando che son fatte salve le disposizioni speciali, previste in numerosi ambiti, dalla disciplina: sulla lotta contro la discriminazione; dal *code du travail* (nel settore del lavoro); dal *code de l'environnement* (in ambito ambientale); dal *code de la santé publique* (codice della salute) e dalla disciplina relativa alla protezione dei dati personali. Sui principi espressi dalla Raccomandazione, mi si consenta di rinviare a G. D'ALFONSO, *Illeciti di massa e controversie transfrontaliere. Strumenti di tutela collettiva risarcitoria e competizione tra sistemi giurisdizionali*, in *Rass. dir. civ.*, 2013, p. 150 ss.

¹²¹ Per le riflessioni che seguono cfr. G. TESAURO, *Diritto comunitario*, cit., pp. 145-146.

¹²² Racc. 4407, pubblicata in <https://eur-lex.europa.eu/legal-content/it>

¹²³ Si v., in particolare, la pronuncia della Corte di legittimità, Cass. 19 marzo 2019, n. 7708, cit. che, nel prevedere la configurabilità della responsabilità civile dell'*hosting provider*, ha fatto riferimento al grado di diligenza che è ragionevole attendersi da un operatore professionale della rete alla stregua dello «sviluppo tecnologico esistente all'epoca dei fatti». Nella motivazione, la Corte richiama la Comunicazione del 28 settembre 2017, n. 555, suddetta, nella parte in cui la Commissione europea rileva come le piattaforme digitali, 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». La sentenza è, tra l'altro, una delle prime pronunce italiane che si riferisce all'intelligenza artificiale come strumento di individuazione dei contenuti illeciti caricati in rete. L'intelligenza artificiale rappresenta, d'altronde, un tema di grande attualità giuridica del quale l'Unione Europea ha iniziato ad occuparsi in alcuni provvedimenti di *soft law*, quali la Risoluzione del Parlamento Europeo del 16 febbraio 2017, recante raccomandazioni alla Commissione concernenti norme di diritto civile in materia di robotica, e successivamente la Comunicazione della Commissione europea al Parlamento europeo, al Consiglio, al Comitato Economico e sociale Europeo e al Comitato delle Regioni, del 25 aprile 2018 (COM(2018) 237 final), rubricate *L'intelligenza artificiale per l'Europa*. Più di recente è stato pubblicato il «Libro Bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia», Bruxelles 19 febbraio 2020, COM (2020) 65 final. Sul punto si v. F. MINIO, *Responsabilità dell'Internet Service Provider ed intelligenza artificiale* in http://morrillossetti.it/responsabilita-dell-internet-service-provider-e-intelligenza-artificiale_sb_1175.html, 26 marzo 2019.

In via conclusiva, ponendosi in un'ottica *de jure condendo*, appare evidente che, posto che la Raccomandazione rappresenti un'importante stimolo per l'innovazione legislativa degli Stati membri dell'Unione Europea, la vera spinta verso la maggiore responsabilizzazione degli *hosting providers* ed, in particolare, verso l'introduzione di una procedura trasparente ed efficiente di «*notice and take down*», dovrebbe preferibilmente avvenire con provvedimenti vincolanti, anche se i segnali propulsivi in questa direzione si rinvergono finora unicamente in atti di *soft law*.

Sarebbe opportuno un intervento armonizzante di *hard law* in tal senso, poiché le istanze di evoluzione del mercato digitale sempre più globale necessitano di regole comuni e condivise. Solo la previsione armonizzante, a livello europeo, di misure che determinino una maggiore responsabilizzazione degli *hosting providers* e di interventi (*ex ante* ed) *ex post*, destinati ad elevare gli *standard* di diligenza degli stessi, può essere idonea ad incrementare la fiducia degli utenti nel mercato digitale, rendendo efficiente la strategia di impulso dello stesso.

Si auspica¹²⁴, in particolare, la previsione, a livello europeo, di disposizioni di carattere generale (e non meramente settoriale) che introducano un meccanismo uniforme di «*notice and take down procedure*» che garantisca comportamenti armonici degli *hosting providers*.

Tale regolamentazione, nel fissare i requisiti necessari, in forza dei quali possa assumersi che l'*hosting provider* sia “effettivamente” pervenuto a conoscenza della pubblicazione di contenuti illeciti sulla piattaforma gestita, dovrebbe, innanzitutto, prevedere l'obbligo di quest'ultimo di nominare un soggetto preposto alla ricezione ed al vaglio delle notifiche, sul modello sia della legislazione statunitense, c.d. «*DMCA*»¹²⁵, sia della disciplina speciale tedesca, il c.d. *Netzwerkdurchsetzungsgesetz* che, al § 2, comma 4, statuisce che il resoconto semestrale, pubblicato sulla *homepage* del gestore del sito, debba contenere informazioni su «organizzazione, risorse, competenze tecniche e linguistiche *delle unità responsabili della gestione delle segnalazioni*, nonché sulle attività di formazione e supporto dei soggetti responsabili della gestione delle segnalazioni». Il gestore del portale dovrebbe, poi, comunicare al pubblico, sul proprio sito, le modalità per contattare tale soggetto, indicando un apposito *link* che sia

¹²⁴ Per le notazioni che seguono, cfr. B. PANATTONI, *Il sistema di controllo successivo*, cit., p. 256 s.

¹²⁵ Si v. nt. 43 *supra*.

ben visibile sull'*homepage* della piattaforma gestita ovvero gli si dovrebbe imporre, secondo il modello inglese (ai sensi di quanto previsto dall'art. 6, paragrafo 1, lett. c), *Regulations 2002 (the "E-commerce-Regulations")*), di fornire informazioni di contatto che agevolino una comunicazione rapida con costui- come la posta elettronica o un numero di telefono.

Il legislatore europeo dovrebbe, inoltre, statuire analiticamente il contenuto della notifica, sul modello della legislazione francese, di cui all'art. 6-I-5, c.d. «*LCEN*».

Una regolamentazione in tale direzione finirebbe con l'agevolare, in capo al soggetto danneggiato, l'onere della prova dell'effettiva conoscenza del *provider* che si intenderebbe essere acquisita al momento del perfezionamento della notifica.

Indubbiamente, infine, per pervenire a risultati ottimali in termini di gestione efficiente di rimozione o di disabilitazione all'accesso di reclami concernenti i contenuti illeciti, il legislatore europeo dovrebbe prevedere una procedura trasparente e tempestiva che garantisca un contraddittorio minimo tra chi assuma essere stato offeso e l'utente che abbia immesso in rete il contenuto oggetto di notifica, sul modello di quello introdotto sia dalla disciplina statunitense, c.d. «*DMCA*»¹²⁶, sia, in ambito europeo, dalla disciplina speciale tedesca, dettata dal c.d. *Netzwerkdurchsetzungsgesetz*, estendendola a tutte le piattaforme digitali di condivisione di contenuti.

Appare, infatti, senza dubbio, fondamentale garantire il contraddittorio tra le parti interessate al contenuto illecito oggetto di contestazione. In tale ottica¹²⁷, si dovrebbe imporre al fornitore di ospitalità di agevolare e mediare costantemente un colloquio tra i soggetti, titolari dei contrapposti interessi, con una soluzione modellata sul meccanismo statunitense della *notification* e della *contro notification*. Il rispetto del contraddittorio dovrebbe rappresentare, per il prestatore di servizi, non un semplice obiettivo astratto, bensì un risultato concreto da raggiungere, ogni qualvolta si assistesse all'invio, da parte del soggetto che assuma essere stato leso, ed alla recezione, da parte del *provider*, della segnalazione di un contenuto potenzialmente illecito. Si potrebbe realizzare tale risultato, prevedendo che il *provider* che non si attivi in tal senso debba essere chiamato a rispondere dei danni provocati (all'utente che abbia pubblicato il contenuto sul portale) derivanti da rimozioni arbitrarie.

¹²⁶ Si v. nt. 43 *supra*.

¹²⁷ Si mutuano, in tale sede, le argomentazioni addotte da S. SICA, V. D'ANTONIO, *La procedura di deindicizzazione*, cit., p. 167, in commento alla disciplina dettata dal c.d. «*DMCA*» in merito al contraddittorio.

Infine, sul modello della legislazione statunitense dettata dal c.d. c.d. «DMCA»¹²⁸, il legislatore europeo dovrebbe intervenire per circoscrivere il rischio dei c.dd. *chilling effects*, c.d. effetti del raffreddamento della rete, quale *marketplace of ideas*, che potrebbe derivare dall'abuso da parte dei privati e dalla strumentalizzazione da parte del *provider* della procedura di «*notice and take down*», elaborando un'ipotesi specifica di responsabilità per *misrepresentation*. In linea con la *subsection* (f), si dovrebbe disporre che chiunque effettui intenzionalmente segnalazioni false, erronee o, ancora, riferite a contenuti o attività che vengano poi rimossi o disabilitati erroneamente o a seguito di una segnalazione non corretta, potrebbe essere chiamato a rispondere di tutti i danni che la propria condotta possa cagionare al *subscriber* oppure al *provider*, oltre che essere condannato al pagamento delle spese processuali e legali.

Abstract

The contribution analyzes the Italian discipline of the "notice and take down procedure" and the related civil liability of the hosting provider. Following a careful analysis of the most relevant regulatory interventions of the member states of the European Union, it highlights the need for a harmonizing intervention of hard law, at European level.

Capua, giugno 2020.

¹²⁸ Sul punto cfr. S. SICA, V. D'ANTONIO, *La procedura di deindicizzazione*, cit., p. 166 s.