

Il ruolo delle reti sociali nel contrasto ai reati commessi all'interno del web.

Tendenze evolutive e prospettive di sviluppo*

Sofia Braschi

Abstract

Il saggio analizza il ruolo delle reti sociali nel contrasto ai reati commessi all'interno del web. Dopo una breve introduzione relativa al rapporto fra autorità pubblica e *provider*, l'Autrice si sofferma sul fondamento politico-criminale dell'attuale domanda di responsabilizzazione dei fornitori di servizi di *social networking*. L'attenzione si sposta quindi sulle posizioni recentemente assunte dalla dottrina e dalla giurisprudenza italiane, per concentrarsi infine sulle *notice and action procedure* come possibile strumento per assicurare una maggiore effettività della tutela penale.

The paper addresses the role of social networks in tackling cybercrime. After a short introduction on the relationship between the law enforcement authorities and the Internet Service Providers, the Author focuses on the criminal-political basis of the current request for accountability of Social Networks. The attention then moves to the positions recently held by Italian doctrine and case law; finally, it focuses on notice and action procedures as a possible means to ensure a more effective criminal protection.

Sommario

1. Premessa. – 2. Il concetto di “rete sociale” e la relativa disciplina. – 3. Il fondamento politico-criminale dell'attuale tendenza alla responsabilizzazione dei Social Network. – 4. Le soluzioni proposte dalla giurisprudenza e dalla dottrina. – 5. Le prospettive di sviluppo della materia: le “*notice and action procedure*”. – 6. Considerazioni finali.

Keywords

responsabilità penale dell'Internet Service Provider - reati informatici - Social Network - *notice and action procedure* - *Digital Services Act*.

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

1. Premessa

Nel settore della criminalità informatica¹, la collaborazione fra pubblico e privato costituisce una necessità, che tuttavia solleva molteplici problemi.

Se, infatti, i servizi di connettività sono forniti da operatori privati (gli *Internet Service Provider*, di seguito *ISP*), i quali dispongono di dati essenziali per l'individuazione dei responsabili degli illeciti commessi nella rete, va peraltro considerato che i principali *ISP* sono grandi società che operano su un mercato globale: per tale ragione, per poter acquisire informazioni la pubblica autorità deve generalmente sottostare ai vincoli della cooperazione giudiziaria internazionale, con apprezzabili ricadute in termini di effettività della tutela penale². D'altra parte, però, l'imposizione di doveri di collaborazione che implicino un più diretto coinvolgimento degli *ISP* e una loro conseguente co-responsabilizzazione è in grado di impattare non solamente sulla libertà di iniziativa economica di questi operatori, bensì anche sulla libertà di comunicazione e informazione degli internauti; ne discende che l'intervento repressivo incontra limiti ulteriori, fondati sulla necessità di assicurare la funzione sociale di internet³. Infine, non si può trascurare che oggigiorno le grandi piattaforme sociali sono in grado di esercitare un'influenza significativa sulla vita politica delle nazioni⁴: il conferimento ad esse di

¹ * Il presente lavoro costituisce il testo aggiornato e integrato dell'intervento tenuto al X Corso di formazione interdottrale di diritto e procedura penale "Giuliano Vassalli" per dottorandi e dottori di ricerca – VIII Convegno della sezione "giovani penalisti" del gruppo italiano dell'Association Internationale de Droit Pénal (AIDP), svoltosi a Siracusa (22-24 ottobre 2020), ed è destinato al volume *I nuovi volti del sistema penale fra cooperazione pubblico-privato e meccanismi di integrazione fra hard law e soft law*.

Con questa espressione s'intende qui individuare non solamente i reati informatici in senso stretto, ma anche i c.d. reati cibernetici, cioè gli illeciti comuni commessi per il tramite della rete: su questa distinzione e sull'opportunità del suo superamento S. Seminara, *Internet (diritto penale)*, in *Enc. dir.*, 2014, Ann. VII, 567 s., e la letteratura ivi citata.

² Sul punto ampiamente C. Conti – M. Torre, *Spionaggio digitale nell'ambito dei social network*, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2019, 553 ss. Come noto, sull'effettività della tutela penale rispetto ai reati commessi tramite internet incide anche la volatilità del dato digitale; per approfondimenti sulla disciplina della *data retention* nel quadro eurounitario R. Flor, *Cyber-criminality: le fonti internazionali ed europee*, in A. Cadoppi – S. Canestrari – A. Manna – M. Papa (diretto da), *Cybercrime*, Torino, 2019, 131 ss.

³ A conferma di ciò si consideri la *Décision n° 2020-801 DC du 18 juin 2020* del *Conseil Constitutionnel* francese, che ha dichiarato l'illegittimità costituzionale degli artt. 1, 4, 5, 7, 8, 9 e 18 della *LOI n° 2020-766 du 24 juin 2020*, che introduceva fra l'altro una serie di obblighi in capo ai gestori delle piattaforme sociali, volti ad assicurare la pronta rimozione dei contenuti illeciti caricati dagli utenti; nel dichiarare la contrarietà a Costituzione della legge, la Corte ha evidenziato l'attitudine delle suddette disposizioni a porre un limite non necessario e comunque sproporzionato alla libertà di espressione degli utenti (c.d. *chilling effect*: sul punto torneremo *infra*, § 6). Per un inquadramento generale della dimensione costituzionale della rete, in relazione al nostro sistema, vd. invece F. Donati, *Internet (diritto costituzionale)*, in *Enc. dir.*, 2014, Annali VII, 531 ss.

⁴ Il riferimento va anzitutto alle pratiche di manipolazione del consenso realizzate tramite *Facebook*, che come noto sembrano avere influenzato la vittoria di Donald Trump alle elezioni presidenziali americane del 2016 e l'esito del *referendum* sulla c.d. Brexit (su questi episodi e sulla loro importanza per l'emersione del fenomeno delle *fake news* T. Guerini, *Fake news e diritto penale. La manipolazione digitale del consenso nelle democrazie liberali*, Torino, 2019, 30 ss.); nemmeno si può ignorare la recente tendenza delle piattaforme digitali a prendere esse stesse posizione all'interno del dibattito pubblico (da ult. vd. la decisione di alcuni *social* di bloccare l'*account* di Donald Trump in seguito all'assalto al Congresso americano: *E Zuckerberg oscura i profili del presidente americano: «Mina la legalità, rischio troppo grande»*, in *Corriere della sera*, 8 gennaio 2020). Sul piano giuridico, questa realtà è alla base dell'attuale

poteri di controllo si deve quindi confrontare con il principio della sovranità statale. Come si vede, nel settore in esame il tema della collaborazione fra pubblico e privato è denso di risvolti problematici, che in questa sede non è possibile esaminare. Il mio intervento si concentrerà dunque sul ruolo di una particolare categoria di *ISP*, cioè i fornitori di servizi di *social networking*, rispetto alla repressione dei reati informatici che si realizzano mediante la pubblicazione di immagini, pensieri o informazioni: partirò dall'attuale tendenza a responsabilizzare i gestori delle piattaforme sociali, per poi analizzare le possibili implicazioni in campo penale della previsione di più stringenti obblighi di collaborazione in capo ai suddetti *provider*⁵.

2. Il concetto di “rete sociale” e la relativa disciplina

Prima di entrare nel vivo del problema, è utile definire il concetto di rete sociale e ripercorrere i tratti essenziali della relativa disciplina. Con riferimento al primo profilo, si può affermare che i Social Network (di seguito *SN*) sono siti che mettono a disposizione uno spazio virtuale, all'interno del quale l'utente ha la possibilità di comunicare e divulgare contenuti, nonché creare un'identità personale e una rete di contatti con la quale condividere le proprie connessioni⁶; rispetto a questa schematizzazione generale, le maggiori piattaforme sociali si connotano altresì per l'offerta di un servizio gratuito e lo sfruttamento commerciale delle informazioni generate dai singoli fruitori. Alla luce delle annotazioni che precedono non sorprende che, per questi operatori, venga comunemente esclusa l'applicabilità dell'art. 57 c.p., che come noto disciplina lo statuto di responsabilità dei *media* più tradizionali (quotidiani su carta stampata e, da ultimo, anche *on-line*)⁷: a tacer d'altro, nelle reti sociali la comunicazione ha carattere interattivo, di talché viene meno la tradizionale distinzione fra produttore e destinatario dell'informazione. L'attività dei *SN* è stata ricondotta invece al d. lgs. 9 aprile 2003, n.

dibattito relativo allo statuto costituzionale delle piattaforme sociali: per il riconoscimento ad esse di una funzione pubblicistica vd. l'isolata posizione di Trib. Roma, sez. impresa, ord. 11-12 dicembre 2019, RG n. 59264/2019, con cui è stato accolto il ricorso di Casa Pound Italia contro la decisione di *Facebook* di oscurare pagine e *account* riferibili all'associazione e ai suoi rappresentanti, accusati di avere pubblicato contenuti inneggianti all'odio. Per alcune considerazioni critiche intorno a tale ultima decisione P. Falletta, *Controlli e responsabilità dei social network sui discorsi d'odio online*, in *questa Rivista*, 1, 2020, 147 ss. e 155 ss.; più in generale, per una panoramica delle opinioni espresse sullo statuto costituzionale di questi *provider*, M. Monti, *Privatizzazione della censura e Internet platforms: la libertà di espressione e i nuovi censori dell'agorà digitale*, in *Riv. it. inf. dir.*, 1, 2019, 41 ss.

⁵ Si precisa che l'attuale tendenza alla responsabilizzazione degli *ISP* non involge solamente i fornitori di servizi di *social networking*, bensì si proietta anche su altre piattaforme digitali, come i motori di ricerca; nell'impossibilità di una trattazione completa del tema, mi limiterò a esaminare la posizione delle reti sociali, che è stata recentemente al centro di alcune innovative decisioni in campo penale (*infra*, § 4).

⁶ La definizione riportata nel testo si trova ad esempio in S. Martinelli, *L'autorità privata del provider*, in P. Sirena – A. Zoppini (a cura di), *I poteri privati e il diritto della regolazione*, Roma, 2018, 556 s. Si precisa che a una sì ampia nozione di *SN* possono essere ricondotti anche siti come *blog* e piattaforme di *video-sharing*; sul punto cfr. C. Conti – M. Torre, *Spionaggio digitale*, cit., 543 s., testo e nt. 19.

⁷ Per l'estensione dell'art. 57 c.p. ai quotidiani *on-line* Cass., sez. V, 11 dicembre 2017, n. 13398, in *Guida dir.*, 17, 2018, 83; conf. da ult. Id., sez. V, 23 ottobre 2018, n. 1275, in *Guida dir.*, 15, 2019, 85; in dottrina, per alcune considerazioni critiche intorno a tale soluzione, I. Pisa, *La responsabilità del direttore di periodico on-line tra vincoli normativi e discutibili novità giurisprudenziali*, in *Dir. pen. proc.*, 3, 2019, 407 ss.

70, di attuazione della direttiva 2000/31/CE (c.d. Direttiva sul commercio elettronico); tale disciplina s'impenna sul principio di neutralità del prestatore di servizi nella rete e, in maniera coerente con questo presupposto, da un lato esclude un «obbligo generale di sorveglianza [del *provider*] sulle informazioni che trasmette o memorizza», dall'altro stabilisce all'art. 16 che il gestore del sito non risponde dell'eventuale memorizzazione di informazioni illecite a meno che, venuto a conoscenza «su comunicazione delle autorità competenti» del carattere illecito di tali informazioni, egli non agisca immediatamente per la loro rimozione. Dinanzi al quadro delineato, si è ritenuto che i gestori delle piattaforme sociali siano punibili solamente nei casi di partecipazione attiva ai reati commessi dagli utenti ovvero nell'ipotesi di mancata rimozione dei contenuti illeciti oggetto di segnalazione istituzionale⁸.

Nei tempi più recenti, però, va diffondendosi la convinzione che la suddetta disciplina sia inadatta a regolare l'attività dei grandi *social media*, la quale invero va ben oltre la mera memorizzazione delle informazioni generate dagli internauti: sulla scorta di questa considerazione, un indirizzo giurisprudenziale vieppiù consistente riconosce in capo ai *provider* più penetranti doveri di intervento e conseguentemente allarga i presupposti per la configurazione della responsabilità civile e penale.

Data l'esiguità del tempo a disposizione, non è possibile analizzare le posizioni assunte dalle diverse corti, anche sovranazionali⁹; soffermiamoci invece sul fondamento politico-criminale dei suddetti orientamenti pretori, per poi riflettere sullo strumento tecnico più adeguato a realizzare un maggior coinvolgimento delle piattaforme sociali nel contrasto ai reati commessi per il mezzo della rete.

3. Il fondamento politico-criminale dell'attuale tendenza alla responsabilizzazione dei Social Network

Alla base dell'attuale domanda di responsabilizzazione dei *SN* vi è in primo luogo la considerazione di carattere generale secondo cui l'enorme espansione del mercato digitale ha determinato il venir meno delle esigenze economiche che, all'inizio degli anni duemila, avevano giustificato la creazione di aree di impunità a favore dei prestatori di servizi nella rete; per tale ragione, sembra invero ragionevole chiedere ai *provider* una più consistente partecipazione alla gestione dei rischi connessi all'utilizzo della rete e ai

⁸ Così, ad esempio, Cass., sez. V, 19 febbraio 2018, n. 16751, in *Cass. pen.*, 11, 2018, 3743 ss. Per approfondimenti sul tema D. De Natale, *La responsabilità dei fornitori di informazioni in internet per i casi di diffamazione on line*, in *Riv. trim. dir. pen. ec.*, 3, 2009, 572 ss.; I. Salvadori, *I presupposti della responsabilità penale del blogger per gli scritti offensivi pubblicati su un blog da lui gestito*, in *Giur. mer.*, 4, 2007, 1074 ss.

⁹ Per una ricognizione degli orientamenti giurisprudenziali relativi alla responsabilità degli intermediari digitali per gli illeciti commessi dagli utenti M. R. Allegri, *Ubi social, ibi ius. Fondamenti costituzionali dei social network e profili giuridici della responsabilità dei provider*, Milano, 2018, 61 ss. e 134 ss., in relazione rispettivamente alla tutela del diritto d'autore e alla fattispecie di diffamazione; con specifico riferimento alla giurisprudenza sovranazionale vd. invece L. Picotti, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in *Cybercrime*, cit., 81 ss. In questa sede ci limitiamo a richiamare l'attenzione sul concetto di "*host provider* attivo", enucleato dalla Corte di giustizia dell'Unione europea e penetrato anche nel nostro sistema: la nozione viene utilizzata per individuare i *provider* che agiscono sui dati memorizzati al fine di ottimizzarne la fruizione e che per questa ragione non potrebbero godere delle esenzioni di responsabilità previste dalla direttiva 2000/31/CE.

derivanti costi in termini di prevenzione. Peraltro, la capacità di internet di raggiungere una cerchia sempre più estesa di persone rende quanto mai grave l'offesa derivante dagli illeciti commessi nel web; si spiega così la necessità di assicurare una pronta rimozione dei materiali illeciti caricati dagli utenti.

A queste osservazioni si aggiunge che i *SN* costituiscono un terreno particolarmente fertile per la proliferazione di alcuni fenomeni criminali. Infatti, la possibilità per l'utente di nascondere la propria identità personale, unita alla facoltà di costruire una propria rete di connessioni, comporta il venir meno dei freni inibitori tipici della comunicazione reale; di qui la diffusione dei tradizionali reati di opinione e dei discorsi d'odio, i quali destano un peculiare allarme sociale anche per via della capacità di fuoriuscire dalla dimensione virtuale, sfociando nella commissione di azioni violente¹⁰. Inoltre, occorre considerare che il profitto dei grandi *SN* si basa sullo sfruttamento commerciale delle informazioni condivise dagli utenti; fra l'altro, tale caratterizzazione comporta che la rete sia organizzata in modo da attribuire una particolare visibilità ai materiali che suscitano un interesse maggiore¹¹. Poiché, però, la popolarità di un contenuto prescinde dalla liceità della sua pubblicazione, ben può accadere che una simile funzionalizzazione della piattaforma allo scopo di profitto del *provider* entri in conflitto con le esigenze di protezione degli interessi degli internauti, conferendo particolare visibilità, ad esempio, a materiali offensivi o discriminatori¹². Infine, con specifico riferimento agli *hate speech* non si può trascurare che la "politica d'impresa" seguita dalle maggiori piattaforme digitali sembra contribuire alla radicalizzazione dei fruitori della rete: invero, l'uso di programmi di intelligenza artificiale per offrire un'informazione targettizzata concorre a determinare la creazione di *filter bubble* che spingono l'utente a rafforzare le proprie opinioni e ad esacerbare il registro della comunicazione¹³.

In breve: l'attività dei grandi *SN* esibisce rischi peculiari, che, dal punto di vista poli-

¹⁰ Sul fenomeno dell'*hate speech*, in rapporto anche alla *hate violence*, per tutti, L. Goisis, *Crimini d'odio. Discriminazioni e giustizia penale*, Napoli, 2019, 202 ss.; con specifico riferimento alle reti sociali A. Spina, *La parola(-)odio*, in *Criminalia*, 2016, 580 ss., secondo il quale la diffusione all'interno dei *SN* dei discorsi d'odio va messa in correlazione con alcuni «meccanismi tipici dell'agire di massa», che tenderebbero a verificarsi anche in queste piattaforme digitali.

¹¹ Per approfondimenti, in prospettiva critica, sul modello economico seguito da alcune grandi piattaforme digitali (*SN* come *Facebook*, ma anche motori di ricerca come *Google*), S. Zuboff, *The age of surveillance capitalism. The fight for a human future at the new frontier of power*, London, 2019, trad. it. a cura di P. Bassotti, *Il capitalismo della sorveglianza*, Roma, 2019, spec. 73 ss.

¹² A conferma delle considerazioni riportate nel testo è sufficiente rammentare la vicenda di Tiziana Cantone, giovane donna ritratta in alcuni video pornografici amatoriali successivamente diffusi senza il suo consenso su *Facebook* e diventati virali: la ragazza si tolse la vita, dopo avere intrapreso una dura battaglia legale volta ad ottenere la rimozione delle pagine che la riguardavano. Per alcune considerazioni sull'accaduto e sulla posizione della piattaforma sociale G. Pitruzzella, *La libertà di informazione nell'era di Internet*, in G. Pitruzzella – O. Pollicino – S. Quintarelli (a cura di), *Parole e potere. Libertà di espressione, hate-speech e fake-news*, Milano, 2017, ora in *questa Rivista*, 1, 2018, 37 ss.

¹³ Per approfondimenti sul punto M. Lamanuzzi, *La disinformazione ai tempi dei social media: una nuova sfida per il diritto penale?*, in *Arch. pen.*, 1, 2020, 14 ss.; peraltro, la creazione di *filter bubble* sembra dover essere ricollegata esclusivamente alla c.d. *pre-selected personalization* (così ampiamente M. Monti, *Regolazione, internet e tecnica: le implicazioni di motori di ricerca e social networks sulla libertà di informazione*, in *federalismi.it*, 24, 2017, 20 ss.). Per una panoramica sui criteri seguiti da *Facebook* nell'organizzazione dei contenuti presenti nella rete vd. invece P. Costa, *Debolezze algoritmiche, umane fragilità. Tecnologie di apprendimento automatico e bias cognitivi nei dispositivi di selezione dei contenuti on-line*, in G. Avanzini – G. Matucci – L. Musselli (a cura di), *Informazione e media nell'età digitale*, Milano, 2019, 363 ss.

tico-criminale, giustificano l'attribuzione a questi *provider* di più stringenti compiti di controllo e d'intervento diretti ad assicurare la legalità delle comunicazioni. Una volta giunti a questa conclusione, però, occorre stabilire cosa precipuamente il *SN* sia tenuto a fare e quali siano le implicazioni in campo penale di una sua eventuale mancata attivazione: consideriamo brevemente le risposte recentemente offerte dalla giurisprudenza e dalla dottrina, per poi delineare i possibili sviluppi della materia.

4. Le soluzioni proposte dalla giurisprudenza e dalla dottrina

Il punto di partenza di qualsivoglia riflessione intorno al ruolo dei *SN* risiede nell'impraticabilità di doveri generalizzati di controllo e filtraggio preventivi: a tacer d'altro, una simile soluzione comporterebbe un'inammissibile limitazione della libertà di comunicazione e informazione degli utenti. Escluso dunque che l'*ISP* possa essere punito per non avere impedito all'internauta di pubblicare un materiale antiggiuridico, l'indagine si sposta sulla possibilità di chiamare i gestori delle piattaforme sociali a rispondere del suo mantenimento nella rete. A questo proposito occorre ricordare che, *de iure condito*, la direttiva 2000/31/CE subordina la responsabilità del fornitore di servizi *internet* alla conoscenza effettiva dell'antigiuridicità del contenuto, mentre il d. lgs. n. 70 del 2003 stabilisce che l'*host provider* debba attivarsi in seguito alla richiesta dell'autorità giudiziaria.

Tale ultima previsione non consente però di assicurare una tempestiva rimozione del materiale antiggiuridico presente nella rete; pertanto, una parte della giurisprudenza e della dottrina ha preso ad affermare che il *SN* risponde della sua mancata attivazione già in seguito alla segnalazione di un privato. Per giungere a questo risultato, un primo orientamento sostiene la configurabilità di una responsabilità per omesso impedimento della protrazione dell'altrui reato¹⁴, mentre un secondo afferma la qualificazione del *provider* alla stregua di un produttore di contenuti, autonomamente punibile per l'illicita diffusione del materiale precedentemente pubblicato dall'utente¹⁵. Il presupposto di entrambe le ricostruzioni è che il *SN* offre un servizio non "neutrale" e per questa ragione non può godere dei *safe harbour* previsti dalla su richiamata Direttiva¹⁶.

Quanto alla prima soluzione, va considerato però che la maggior parte dei reati di manifestazione del pensiero ha carattere istantaneo¹⁷; per tale ragione, il mantenimento

¹⁴ Così Cass., sez. V, 14 luglio 2016, n. 54946, con nota critica di R. Carbone, *Responsabilità del blogger: parziale revirement della Cassazione?*, in *Cass. pen.*, 7-8, 2017, 2782 ss.; aperture verso la soluzione proposta dalla Cassazione si rinviengono, invece, in R. Bartoli, *Brevi considerazioni sulla responsabilità penale dell'internet service provider*, in *Dir. pen. proc.*, 5, 2013, 606.

¹⁵ In questi termini Cass., sez. V, 8 novembre 2018, n. 12546; in dottrina P. Lasalvia, *La diffamazione via web nell'epoca dei social network*, in *Cybercrime*, cit., 356 s. Su questa sentenza e su quella citata nella nota che precede B. Panattoni, *I riflessi penali del perdurare nel tempo dei contenuti illeciti nel cyberspace*, in *Sist. pen.*, 5, 2020, 310 ss.; in merito sia consentito rinviare anche a S. Braschi, *Social media e responsabilità penale dell'Internet Service Provider*, in *questa Rivista*, 3, 2020, 163 ss.

¹⁶ Chiaro il riferimento alla figura dell' "*host provider* attivo", a proposito della quale vd. *retro*, nt. 9.

¹⁷ Sul punto S. Seminara, *La responsabilità penale degli operatori su internet*, in *Dir. inf.*, 4-5, 1998, 765; diversamente L. Picotti, *Diritto penale e tecnologie informatiche*, cit., 89 ss. Si segnala che all'interno della

nella rete del contenuto antigiuridico dà luogo a una condotta susseguente, che gioco-forza fuoriesce dallo schema del concorso di persone. Inoltre, poiché nell'attuale sistema normativo non è possibile affermare che, in linea generale, i SN sono titolari di una posizione di garanzia¹⁸, la punibilità per omesso impedimento dell'altrui violazione può trovare spazio solamente in una prospettiva di politica criminale. Osservazioni non dissimili valgono per l'orientamento che afferma la configurabilità di un'autonoma responsabilità del *provider*: in effetti, in assenza di un obbligo di rimozione, non è agevole comprendere come mai l'automatico, ininterrotto funzionamento dei meccanismi di diffusione dei dati nella rete dovrebbe acquisire un'autonoma tipicità penale; se poi si considera che le piattaforme sociali affidano l'organizzazione delle informazioni a sistemi di intelligenza artificiale, sembra impossibile affermare che il *provider* ha il dolo richiesto per la punibilità delle singole violazioni¹⁹. Infine, nel silenzio del legislatore, le due ricostruzioni affidano il giudizio sulla neutralità della piattaforma sociale all'interprete e una simile impostazione cozza con le esigenze di certezza del diritto e prevedibilità della sanzione.

Il vero è che, al fine di ottenere una maggiore responsabilizzazione dei gestori delle piattaforme sociali, risulta imprescindibile un intervento del legislatore; assunta questa prospettiva, però, restano da chiarire il fondamento e l'ampiezza della punibilità del *provider*. In proposito, si è già osservato che il fornitore del servizio di *social networking* non ha un legame con l'utente-produttore del contenuto, che giustifichi una responsabilità di tipo editoriale; aggiungiamo che, considerata l'enorme quantità di dati presenti nella rete, nemmeno sembra sensato addebitare al gestore del sito la *volontaria* diffusione di un materiale antigiuridico. La mia opinione è che, più ragionevolmente, al SN possa essere rimproverata la mancata assunzione di misure volte a contenere il rischio della circolazione dei contenuti illeciti pubblicati dagli utenti; il significato di questa affermazione risulterà più chiaro dopo una breve digressione sul funzionamento delle

giurisprudenza civile ricorre l'affermazione del carattere permanente dei reati commessi nella rete: così, *ex multis*, Cass. civ., sez. I, 21 febbraio 2019, n. 7708, in *Riv. dir. ind.*, 4-5, 2019, II, 201.

¹⁸ Invero, tralasciando la possibilità di ricavare, nell'ambito delle normative di settore, degli specifici doveri di protezione, la dottrina e la giurisprudenza maggioritarie ritengono che il d. lgs. n. 70 del 2003 costituisca la fonte di obblighi di attivazione, che solo nel caso di una richiesta d'intervento della competente autorità amministrativa o giudiziaria possono dare luogo a un'autonoma responsabilità penale: così spec. Cass. pen., sez. III, 17 dicembre 2013, n. 5107, in *Riv. pen.*, 5, 2014, 495; in dottrina, *ex multis*, A. Ingrassia, *Responsabilità penale degli internet service provider: attualità e prospettive*, in *Dir. pen. proc.*, 12, 2017, 1626 s.; S. Seminara, *Internet*, cit., 597 s. Sostiene, invece, l'esistenza di una posizione di garanzia in capo al gestore di una piattaforma di *video-sharing* F. Sgubbi, *Parere pro veritate*, in *Dir. inf.*, 4-5, 2009, 745 ss.; cfr., con riferimento al settore della pedopornografia, L. Picotti, *Art. 600-ter, III comma c.p.*, in A. Cadoppi (a cura di), *Commentario delle norme contro la violenza sessuale e contro la pedofilia*, Padova, 2006, 210 ss., e, rispetto a quello del diritto d'autore, R. Flor, *Social network e violazioni penali dei diritti d'autore. Quali prospettive per la responsabilità del fornitore del servizio?*, in *Riv. trim. dir. pen. ec.*, 3, 2012, 681 s.

¹⁹ Per alcune considerazioni critiche intorno a questa soluzione B. Panattoni, *I riflessi penali*, cit., 316 ss.; evidenzia la difficoltà di rinvenire una «concreta rimproverabilità», anche una volta risolto il problema della tipicità oggettiva dell'illecito addebitato al *provider* C. Melzi d'Eril, *Fake news e responsabilità: paradigmi classici e tendenze incriminatrici*, in *questa Rivista*, 1, 2017, 66. In generale, sulle implicazioni a livello costituzionale dell'assimilazione delle piattaforme sociali ai *content provider*, O. Pollicino, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet Service Provider*, in *Consulta Online*, 3 febbraio 2014, 18 ss.

“procedure di segnalazione e rimozione” (*notice and action procedure*).

5. Le prospettive di sviluppo della materia: le “*notice and action procedure*”

Con l’espressione “*notice and action procedure*” o “*notice and take down procedure*” s’intende un meccanismo di controllo successivo, caratterizzato per l’eliminazione da parte del gestore della piattaforma sociale dei contenuti illeciti segnalati dagli utenti; sorte sul terreno del diritto d’autore e progressivamente estese alla repressione dei discorsi d’odio, siffatte “procedure di segnalazione e rimozione” stanno acquisendo un’importanza sempre maggiore all’interno del continente europeo²⁰.

In primo luogo, infatti, non si può trascurare che, in una prospettiva di parziale superamento della direttiva 2000/31/CE, lo scorso 15 dicembre 2020 la Commissione Europea ha presentato una proposta di Regolamento (*Digital Services Act*, di seguito *DSA*), che mira a subordinare l’esonero dalla responsabilità per la memorizzazione dei contenuti illeciti generati dagli utenti all’adozione, da parte degli *hosting provider*, di procedure di segnalazione e rimozione. Si prevede che i fornitori di servizi di memorizzazione debbano mettere in atto meccanismi trasparenti e facilmente accessibili, che consentano a qualsiasi persona di segnalare la presenza di specifici contenuti illegali (art. 14)²¹. Quindi, si chiarisce che, nel caso di segnalazione sufficientemente precisa e motivata, il gestore della piattaforma digitale ha una “conoscenza effettiva” della violazione commessa dall’utente; donde la sua responsabilità nel caso di mancata rimozione del contenuto oggetto di memorizzazione²². Tale innovazione non sorprende, ove solo si consideri che in un’analoga direzione si era già orientata la direttiva (UE) 2019/790 del 17 aprile 2019, in tema di *copyright*: dopo avere stabilito che le piattaforme di *file-sharing*

²⁰ Sulle origini delle procedure di segnalazione e rimozione, anche in ottica comparata, B. Panattoni, *Il sistema di controllo successivo: obbligo di rimozione dell’ISP e meccanismi di notice and take down*, in *Dir. pen. cont.*, 5, 2018, 256 ss. Per completezza, va ricordato che nel 2016 la Commissione europea, in collaborazione con alcune piattaforme digitali, ha promosso la redazione del *Code of conduct countering illegal hate speech online*, il quale fra l’altro stabilisce che «le aziende informatiche predispongono procedure chiare ed efficaci per esaminare le segnalazioni riguardanti forme illegali di incitamento all’odio nei servizi da loro offerti, in modo da poter rimuovere tali contenuti o disabilitarne l’accesso»; l’importanza delle suddette procedure è stata ribadita anche dalla Raccomandazione n. 2018/334, del 1° marzo 2018.

²¹ Per maggiori dettagli, vd. il testo della *Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE*.

²² Va evidenziato che le *online platform* di medie e grandi dimensioni devono altresì adottare un sistema interno di reclamo e comunicare ai competenti organi di polizia le informazioni di cui siano venuti a conoscenza, dalle quali sia possibile ricavare il sospetto che è stato commesso o è in corso un grave reato, il quale comporti un pericolo per la vita e l’incolumità fisica della persona; la definizione di *online platform* si rinviene all’art. 2, lett. h («un prestatore di servizi di *hosting* che, su richiesta di un destinatario del servizio, memorizza e diffonde al pubblico informazioni, tranne qualora tale attività sia una funzione minore e puramente accessoria di un altro servizio»), mentre l’art. 16 chiarisce che sono esentati dagli obblighi previsti dalla sezione le *online platform* che rientrino nella nozione di *micro or small enterprise* ai sensi della Raccomandazione 2003/361/EC. Per completezza, segnaliamo infine che il *DSA* prevede ulteriori doveri per le *very large platform*, fra i quali rientrano l’adozione di misure di valutazione e mitigazione dei rischi di diffusione di contenuti antiggiuridici e obblighi di trasparenza e rendicontazione (art. 25 ss.).

non beneficiano delle esenzioni stabilite dalla Direttiva sul commercio elettronico, l'art. 17 da un lato ha affermato la responsabilità del *provider* per la messa a disposizione del materiale protetto da diritto d'autore, dall'altro ha stabilito che il gestore del sito non risponde nel caso in cui dimostri «di aver agito tempestivamente, dopo aver ricevuto una segnalazione sufficientemente motivata dai titolari dei diritti, per disabilitare l'accesso o rimuovere [dal sito] *web* le opere o altri materiali oggetto di segnalazione e aver compiuto i massimi sforzi per impedirne il caricamento in futuro»²³.

Analoghe soluzioni sono state già sperimentate nell'ambito delle legislazioni nazionali. Anzitutto, va rammentato che nel 2017 la Germania si è dotata di una «legge per il miglioramento della tutela dei diritti sui social network» (*Netzwerkdurchsetzungsgesetz*, di seguito NetzDG), la quale prevede che i SN con più di due milioni di utenti registrati all'interno dello stato tedesco siano tenuti ad adottare procedure trasparenti ed efficaci per la rimozione del materiale antigiuridico²⁴. Senza entrare nel dettaglio della normativa, è bene sottolineare che la NetzDG impone termini stringenti per la rimozione dei contenuti oggetto di segnalazione (ventiquattro ore nelle ipotesi di illiceità manifesta, sette giorni negli altri casi), stabilendo peraltro che, per la soluzione dei casi più controversi, il SN abbia la possibilità di interpellare un organo di autoregolamentazione indipendente appositamente creato; commina inoltre onerose sanzioni pecuniarie per l'ipotesi della sua mancata attuazione (fino a cinque milioni di euro nei casi più gravi, § 4). Nella medesima direzione sembra volersi orientare anche l'ordinamento austriaco²⁵, mentre in Francia il *Conseil Constitutionnel* ha censurato la *LOI n° 2020-766, du 24 juin 2020*, che imponeva alle piattaforme digitali l'adozione di misure di *notice and action*, minacciando gravi sanzioni in caso di inadempimento: partendo dal presupposto che la previsione di doveri di controllo e di rimozione da attuare entro termini stringenti incentivi l'assunzione da parte degli *ISP* di atteggiamenti censori, la Corte ha ritenuto

²³ È opportuno precisare che la Direttiva si applica al «prestatore di servizi della società dell'informazione il cui scopo principale o uno dei principali scopi è quello di memorizzare e dare accesso al pubblico a grandi quantità di opere protette dal diritto d'autore o altri materiali protetti caricati dai suoi utenti, che il servizio organizza e promuove a scopo di lucro» (art. 2, n. 6). Se, in linea generale, «i prestatori di servizi di condivisione di contenuti *online* sono responsabili per atti non autorizzati di comunicazione al pubblico, compresa la messa a disposizione», la loro responsabilità è però esclusa – oltretutto nei casi indicati nel testo – se dimostrano di «aver compiuto i massimi sforzi per ottenere un'autorizzazione» ovvero di «aver compiuto, secondo elevati standard di diligenza professionale di settore, i massimi sforzi per assicurare che non siano disponibili opere e altri materiali specifici per i quali [abbiano] ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti» (art. 17).

²⁴ BT-Drucksache 18/12356; il testo in italiano della legge può essere consultato in *Dir. inf.*, 4-5, 2017, 723 ss. (trad. a cura di G. Codiglione). Sui contenuti del provvedimento e sulle ragioni alla base della sua adozione vd. S. Müller-Franken, *Netzwerkdurchsetzungsgesetz: Selbstbehauptung des Rechts oder erster Schritt in die selbstregulierte Vorzensur? – Verfassungsrechtliche Fragen*, in *Archiv für Presserecht*, 2018, 1 ss. e, nella dottrina italiana, T. Guerini, *Fake news e diritto penale*, cit., 79 ss. Si evidenzia che la NetzDG, se da un lato adotta una nozione ampia di SN, dall'altro dà rilevanza alla finalità di profitto dell'attività svolta da questi operatori; siffatta soluzione, che per la verità sembra un ragionevole tentativo di limitare l'operatività degli obblighi ai soggetti dotati dei mezzi economici necessari alla loro implementazione, è invece criticata da M. Bassini – G. E. Vigevari, *Primi appunti su fake news e dintorni*, in *questa Rivista*, 1, 2017, 19, secondo i quali l'«approccio tedesco (basato sul *follow the money*) appare problematico in quanto presuppone che la capacità di ottenere profitti da parte di una piattaforma significhi un suo maggiore coinvolgimento (o quantomeno l'esigibilità di una condotta attiva) nella rimozione dei contenuti».

²⁵ Si allude alla *Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen (Kommunikationsplattformen-gesetz-KoPi-G.*

la suddetta legge lesiva della libertà di comunicazione e informazione degli utenti²⁶. Quanto, infine, al nostro sistema, alle procedure di segnalazione e rimozione dei contenuti fa riferimento la l. 29 maggio 2017, n. 71, in tema di *cyberbullismo*: l'art. 2 prevede che il minore ultraquattordicenne, nonché il genitore o esercente la responsabilità del minore che abbia subito atti di *cyberbullismo* possono chiedere l'oscuramento di qualsiasi dato personale della vittima al titolare della piattaforma sociale. La legge non contempla alcuna sanzione per l'ipotesi in cui il *provider* ometta di dare un riscontro tempestivo; tuttavia, stabilisce che, in questa eventualità, l'utente abbia la possibilità di adire il Garante della *privacy* al fine di ottenere la pronta rimozione del contenuto illecito oggetto della segnalazione. Infine, verso l'introduzione di procedure obbligatorie di segnalazione e rimozione si orientava anche il d.d.l. n. 3001, del 14 dicembre 2017, c.d. d.d.l. Zanda-Filippin, il quale presentava contenuti affini alla su menzionata NetzDG; tale proposta, però, non ha mai avviato l'*iter* parlamentare²⁷. Sintetizzando, si può affermare che sul versante legislativo si registra una comune tendenza ad attribuire alle piattaforme sociali doveri di controllo successivo, eventualmente sanzionandole per la loro mancata implementazione: in tal modo, si ritiene possibile limitare i danni derivanti dalla pubblicazione di materiali antigiuridici, senza peraltro gravare gli *ISP* di obblighi eccessivamente onerosi né attuare una sorveglianza generalizzata delle comunicazioni.

6. Considerazioni finali

A questo punto, è possibile svolgere alcune considerazioni conclusive intorno ai possibili sviluppi della materia. Abbiamo visto che, in linea generale, si fa strada l'idea secondo cui, per minimizzare il rischio della circolazione di materiali antigiuridici nella rete, è opportuno incentivare l'adozione da parte delle piattaforme sociali di meccanismi di controllo successivo, attivabili su richiesta dell'utente e finalizzati alla rimozione dei contenuti illeciti. Questa evoluzione, se da un lato riflette condivisibili esigenze di tutela, dall'altro consente di ovviare alla inadeguatezza dei modelli di responsabilità già sperimentati con riferimento ai *media* più tradizionali: a tacer d'altro, la loro estensione ai *SN* è ostacolata dalle caratteristiche della comunicazione digitale e dall'ampiezza dei dati presenti nella rete. Dal confronto fra le disposizioni che abbiamo prima menziona-

²⁶ Va però segnalato che nel 2018 la Francia si è dotata di due leggi (*Loi organique n° 2018-1201 e n° 2018-1202, du 22 décembre 2018*), che prevedono alcuni obblighi di trasparenza in capo ai *provider* e stabiliscono la possibilità, durante il periodo elettorale, di ricorrere agli organi giudiziari per ottenere entro 48 ore la rimozione di notizie false diffuse nella rete; tali previsioni sono state giudicate compatibili con la Costituzione dal *Conseil Constitutionnel* con la *Décision n° 2018-773, du 20 décembre 2018*. Per approfondimenti sui contenuti della legge e sulla decisione T. Guerini, *Fake news e diritto penale*, cit., 75 ss.; C. Magnani, *Libertà d'informazione on-line e fake-news: vera emergenza? Appunti sul contrasto alla disinformazione tra legislatori statali e politiche europee*, in *forumcostituzionale.it*, 18 aprile 2019, 16 ss.

²⁷ Sul contenuto della proposta e per alcune considerazioni critiche T. Guerini, *Fake news e diritto penale*, cit., 173 ss.; F. De Simone, "Fake news", "post truth", "hate speech": nuovi fenomeni sociali alla prova del diritto penale, in *Arch. pen.*, 2 aprile 2018, 17 ss.; dal punto di vista del diritto costituzionale, M. Monti, *La proposta del d.d.l. Zanda-Filippin sul contrasto alle fake news sui social network: profili problematici*, in *diritticomparati.it*, 7 dicembre 2017, spec. 3 ss.

to emerge però che la valorizzazione delle misure di *notice and action* solleva due fondamentali interrogativi: il primo involge l'ampiezza dei poteri che possono essere delegati alle piattaforme digitali, il secondo riguarda invece il riflesso delle suddette procedure sulla responsabilità del fornitore di servizi nella rete. Esaminiamoli brevemente.

Con riferimento alla prima questione, si è visto che l'attribuzione al *SN* del compito di stabilire la liceità di una pubblicazione solleva perplessità che attengono al rispetto della libertà di espressione e informazione degli internauti. In effetti, il *provider* non è un soggetto imparziale, sicché il conferimento ad esso di funzioni di controllo non sembra offrire sufficienti rassicurazioni contro il pericolo di decisioni arbitrarie²⁸; peraltro, il *SN* a differenza di un editore ha uno scarso interesse alla singola pubblicazione e per questo motivo è portato a eliminare i contenuti oggetto di segnalazione, così ulteriormente comprimendo la libera circolazione delle opinioni nella rete (c.d. *chilling effect*)²⁹. Infine, non si possono trascurare i costi derivanti dalla necessità di soddisfare gli obblighi di controllo imposti dal legislatore, i quali rischiano di pregiudicare i siti di piccole dimensioni e conseguentemente intaccare il pluralismo dell'informazione.

Sebbene dotate di fondamento, queste osservazioni non sembrano però decisive. Per non pregiudicare la funzione sociale delle piattaforme digitali, una parte della dottrina ha invero proposto di affiancare i *provider* nelle singole decisioni, mediante l'istituzione di appositi organi statali³⁰: questa soluzione consentirebbe di assicurare il controllo sull'operato del *SN* e al contempo arginare l'adozione di atteggiamenti censori, volti a ridurre il rischio di incappare nella responsabilità civile e penale. Nella medesima direzione si muove anche il *DSA*, il quale, se da un lato impone alle medio-grandi piat-

²⁸ Sul punto M. Monti, *Privatizzazione della censura*, cit., 37 ss.; il problema era stato già sollevato, con riferimento però al motore di ricerca *Google*, da O. Pollicino, *Google rischia di "vestire" un ruolo para-costituzionale*, in *Il Sole 24 ore*, 14 maggio 2014. È chiaro, peraltro, che il rischio di decisioni arbitrarie si manifesta soprattutto allorché si rende necessario bilanciare esigenze di tutela e libertà costituzionali, come nei tradizionali reati di opinione, ovvero in presenza di illeciti politicamente più sensibili (cfr. però, con riferimento ai reati di parola collegati al terrorismo internazionale di matrice islamica F. Fasani, *Le "parole preparatorie". I reati antiterrorismo di parola nell'era dei new media*, in *Dir. pen. cont. – Riv. trim.*, 1, 2019, 117 ss.).

²⁹ Si tratta del fenomeno del c.d. *overblocking*: in merito vd. le considerazioni di E. Rosati – G. Sartor, *Social networks e responsabilità del provider*, in *EUI working papers*, LAW 5, 2012, 8: «Mentre l'editore del giornale ha un forte interesse alla pubblicazione degli articoli, ciascuno dei quali è importante elemento del giornale e concorre a determinarne il valore commerciale, il titolare di una piattaforma aperta per il *Web* ha scarso interesse alla presenza di un particolare contributo [...] e pertanto normalmente anziché difendere quel contributo di fronte alle rimostranze dei terzi, preferirà procedere alla sua rimozione». Condividono queste osservazioni, *ex multis*, M. Bassini – G. E. Vigevani, *Primi appunti*, cit., 20; C. Melzi d'Eril, *Fake news e responsabilità*, cit., 66. Con specifico riferimento all'impostazione accolta dalla *NetzDG*, cfr. G. Nolte, *Hate-Speech, Fake-News, das «Netzwerkdurchsetzungsgesetz» und Vielfaltsicherung durch Suchmaschinen*, in *Zeitschrift für Medienwissenschaft*, 2017, 556 ss. e A. Lang, *Netzwerkdurchsetzungsgesetz und Meinungsfreiheit. Zur Regulierung privater Internet-Intermediäre bei der Bekämpfung von Hassrede*, in *Archiv des Öffentlichen Recht*, 2, 2018, 232 ss.

³⁰ Così M. Monti, *Le Internet platforms, il discorso pubblico e la democrazia*, in *Quad. cost.*, 4, 2019, 826 s., il quale sostiene la necessità di affidare alla pubblica autorità il giudizio "in secondo grado" sulla liceità della pubblicazione; la necessità del coinvolgimento di organi statali è stata affermata per la prima volta da G. Pitruzzella, *La libertà di informazione*, cit., 26. Nella letteratura penalistica cfr. T. Guerini, *Fake news e diritto penale*, cit., 206 ss., il quale individua nella *NetzDG* un modello di disciplina esportabile anche nel nostro paese, ritenendo peraltro opportuno affidare a un'autorità amministrativa indipendente – nello specifico l'AGCOM – il ruolo di «intermediario tra chi propone il reclamo e il gestore del *social network*, chiamato a valutarne la fondatezza».

taforme di implementare sistemi interni di reclamo, dall'altro statuisce che i soggetti raggiunti da un provvedimento del *provider*, che abbia stabilito la rimozione di un contenuto o la disabilitazione del relativo *account* personale, abbiano la possibilità di rivolgersi ad appositi e riconosciuti organi stragiudiziali; in ogni caso, resta impregiudicato il diritto dell'utente alla tutela giurisdizionale³¹.

Più articolato – quantomeno nella prospettiva del cultore del diritto penale – è il discorso relativo all'incidenza delle procedure di *notice and action* sulla responsabilità del *provider*: a questo proposito occorre assicurare che il *SN* eserciti un controllo effettivo, senza peraltro sfociare in forme di responsabilità di posizione, che avrebbero, fra l'altro, la conseguenza di mortificare l'iniziativa economica degli operatori e la libertà di informazione degli utenti. Ciò precisato, abbiamo visto che la direttiva (UE) 2019/790 sembra individuare nella predisposizione di meccanismi di segnalazione e rimozione un'esimente per la responsabilità derivante dalla diffusione dei contenuti antigiuridici pubblicati dall'utente, mentre il sistema tedesco ha optato per la creazione di un autonomo illecito amministrativo, incentrato sulla mancata implementazione delle suddette procedure.

A livello strutturale, la prima soluzione ricalca la più tradizionale responsabilità di tipo editoriale, dalla quale si distingue però per il carattere successivo del controllo e per la maggiore specificazione del dovere di diligenza imposto alla piattaforma sociale: in buona sostanza, si tratta infatti di addebitare al *provider* la *colposa* diffusione del contenuto antigiuridico prodotto dall'utente³². La ricostruzione presta il fianco però a due obiezioni: anzitutto, si potrebbe osservare che ha poco senso applicare al *SN* la pena prevista per il fatto principale, atteso che la sua "colpa" consiste in un difetto di organizzazione; in secondo luogo, in assenza di una specifica previsione, il compito di verificare l'adeguatezza del sistema di segnalazione e rimozione spetta al giudice competente per il reato informatico e una simile impostazione potrebbe incidere negativamente sulla prevedibilità della sanzione³³. Sotto questo profilo, parrebbe dunque preferibile la soluzione accolta dalla NetzDG, che affida a un apposito ufficio il giudizio relativo alla congruità dei meccanismi di "*notice and action*"³⁴; parametrando la sanzione alle dimensioni del *SN*, questa legge sembra inoltre assicurare una maggiore effettività

³¹ In proposito vd. gli artt. 17 e 18. Il *DSA* prevede inoltre l'istituzione, all'interno di ciascuno stato membro, di un *Digital service coordinator* chiamato a vigilare sull'esatta attuazione del Regolamento; fra l'altro, questo soggetto deve certificare l'imparzialità e adeguatezza degli organismi di risoluzione delle controversie citati nel testo.

³² Sul modello di responsabilità disciplinato dall'art. 57 c.p., che secondo la dottrina più recente configura un autonomo reato proprio colposo dell'editore, vd. per tutti, F. Mantovani, *Manuale di diritto penale. Parte generale*, Milano, 2020, 429, e la letteratura ivi citata; è peraltro opportuno sottolineare ancora che il rapporto fra *SN* e produttore del contenuto è molto meno stretto di quello che lega editore e giornalista.

³³ È cioè evidente che l'illecito commesso dalla piattaforma sociale presenta un più marcato carattere economico; con riferimento alla seconda osservazione, parafrasando considerazioni sviluppate nel settore della responsabilità amministrativa degli enti, si potrebbe affermare che "alla certezza dei costi (di progettazione e implementazione del sistema di segnalazione e rimozione) si contrappone l'incertezza della valutazione di adeguatezza" (sul punto vd. ampiamente C. Piergallini, *Il modello organizzativo alla verifica della prassi*, in *Le Soc. Gli speciali*, 2011, 49 ss.).

³⁴ Per alcune considerazioni critiche sulla terzietà dei soggetti coinvolti nella valutazione dell'adeguatezza del sistema di *notice and action* C. Magnani, *Libertà d'informazione* on-line, cit., 15 s.

all'obbligo di implementare il sistema di segnalazione e rimozione. D'altra parte, però, occorre evidenziare che la disciplina tedesca si caratterizza per un notevole rigore punitivo, il quale trova scarsa giustificazione alla luce della posizione secondaria dell'*ISP* rispetto all'autore della violazione principale; se poi si considera che nel settore della comunicazione la previsione di sanzioni fortemente afflittive solleva delicati problemi in termini di legittimità costituzionale³⁵, prende forza l'idea della necessità di temperare le sanzioni applicabili alle piattaforme sociali.

Concludendo, segnaliamo che, al fine di assicurare l'attuazione del Regolamento, il *DSA* prevede che gli stati membri debbano adottare sanzioni «efficaci, proporzionate e dissuasive», senza peraltro superare limiti percentuali legati all'entità del fatturato del singolo intermediario digitale (art. 42): ove ve ne fosse bisogno, la previsione conferma che i *provider* sono destinati a ricoprire un ruolo sempre più importante nel contrasto ai reati commessi nella rete e suggerisce l'importanza di aggiornare la riflessione intorno allo statuto penale di questi operatori.

³⁵ In proposito, è sufficiente rammentare le numerose prese di posizione della Corte Europea dei Diritti dell'Uomo contro il ricorso alla pena detentiva per le violazioni commesse dai *media* più tradizionali e la conseguente questione di legittimità costituzionale avanzata nel nostro sistema per il delitto di diffamazione a mezzo stampa: sul punto, per tutti, M. C. Ubiali, *Diffamazione a mezzo stampa e pena detentiva: la Corte costituzionale dà un anno di tempo al Parlamento per trovare un punto di equilibrio tra libertà di espressione e tutela della reputazione individuale, in linea con i principi costituzionali e convenzionali*, in *Riv. it. dir. proc. pen.*, 3, 2020, 1476 ss.