Social media e responsabilità penale dell'*Internet Service Provider*[*]

Sofia Braschi

Abstract

Il saggio affronta il tema della responsabilità penale dell'*Internet Service Provider*, approfondendo il ruolo dei *social media* nel contrasto ai reati commessi nella rete. Dopo avere dato conto delle caratteristiche essenziali del *Web 2.0*, l'Autrice analizza i più recenti orientamenti della giurisprudenza italiana relativi alla responsabilità dell'amministratore del *blog*, per passare poi a considerare i contenuti della *Netzwerkdurchsetzungsgesetz*, entrata in vigore in Germania il 1° ottobre 2017, e i progetti di legge in discussione in questo paese, che mirano a sanzionare i gestori delle piattaforme attive nel *dark web*. L'indagine evidenzia il progressivo superamento del modello di disciplina delineato dalla direttiva 2000/31/CE e suggerisce alcune riflessioni conclusive intorno alla necessità di adeguare la normativa vigente all'attuale realtà economico-sociale.

The paper addresses the criminal liability of the Internet Service Provider, focusing on the role of social media in tackling cybercrime. After considering the main features of Web 2.0, the Author examines the most recent Italian judgments on the liability of the blog administrator. The essay then explores the contents of the Netzwerkdurchsetzungsgesetz, which came into force in Germany on 1 October 2017, as well as the recent German bills aimed at punishing providers operating on the dark web. The study highlights the constant overcoming of the rules defined by Directive 2000/31/EC and suggests some final reflections, whose aim is to adapt the current legislation to the economic and social reality.

Sommario

[*] L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio a doppio cieco

Keywords

responsabilità penale dell'*internet service provider* - *social media* - diffamazione - *Netzwerkdurchsetzungsgesetz* - *dark web.*

1. Premessa.

Alcuni recenti orientamenti legislativi e giurisprudenziali suggeriscono di tornare a riflettere sul ruolo dell'*Internet Service Provider* (di seguito ISP) nel contrasto ai reati commessi all'interno del *web*.

Con riferimento al versante legislativo, possiamo menzionare l'esempio offerto dalla Germania, ove il *Bundestag* ha introdotto a carico dei gestori di *social network* di grandi dimensioni una serie di obblighi volta ad assicurare l'efficace funzionamento dei meccanismi di segnalazione e rimozione dei contenuti illeciti immessi nella rete[1]; sempre in questo paese sono inoltre in discussione due proposte di legge che mirano a sanzionare gli amministratori delle piattaforme *online* in cui si svolgono traffici criminali[2].

Quanto invece alla giurisprudenza, è sufficiente osservare che all'interno del nostro sistema va consolidandosi un'interpretazione vieppiù restrittiva del d. lgs. 9 aprile 2003, n. 70, di attuazione della direttiva 2000/31/CE, con una conseguente contrazione delle aree di impunità tradizionalmente riservate agli ISP.

Se indubbiamente questi indirizzi segnano un passo in avanti rispetto alla disciplina eurounitaria, va peraltro evidenziato che essi riflettono una più generale tendenza alla responsabilizzazione dei prestatori di servizi nella rete. In effetti, malgrado la mancata revisione della summenzionata direttiva sul commercio elettronico, la Commissione Europea ha affermato la necessità che le piattaforme *online* siano «proattive nell'eliminazione dei contenuti illegali»[3] e, in linea con questa impostazione, la recente direttiva 2019/790/UE sulla protezione del diritto d'autore ha sensibilmente incrementato i doveri di collaborazione dei *provider*[4]. In maniera ancor più netta, la Corte Europea

[1] È opportuno evidenziare che anche nel nostro paese sono state avanzate proposte di legge intese a implementare la tutela degli utenti delle reti sociali: in questa prospettiva si consideri il d.d.l. n. 3001, comunicato alla Presidenza il 14 dicembre 2017, il quale replicava il modello di disciplina frattanto adottato in Germania (*Atti parlamentari (Senato della Repubblica), XVII legislatura, Disegni di leggi e relazioni*, stampato n. 3001), e il d.d.l. n. 2688, comunicato alla Presidenza il 7 febbraio 2017, il quale proponeva invece l'introduzione di due nuove fattispecie incentrate sulla diffusione di notizie false e stabiliva alcuni obblighi in capo ai gestori delle piattaforme sociali, come quello di rettifica delle false informazioni e di rimozione dei contenuti diffamatori circolanti nella rete (*Atti parlamentari (Senato della Repubblica), XVII legislatura, Disegni di leggi e relazioni*, stampato n. 2688). Infine, sottolineiamo che nel senso di una maggiore responsabilizzazione dei gestori dei *social network* si è orientato anche il legislatore francese con la *loi n° 2018-1202* del 22 dicembre 2018.

[2] Si allude ai disegni di legge BR-Drs. 33/19 e IT-SiG 2.0, a proposito dei quali *infra*, § 7.

[3] Così si legge nella COM (2017) 555 (*Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni* "*Lotta ai contenuti illeciti online. Verso una maggiore responsabilizzazione delle piattaforme online*"), 21.

[4] L'art. 17 della direttiva 2019/790/UE del 17 aprile 2019 stabilisce infatti che le piattaforme di *file-sharing* non beneficiano delle esenzioni stabilite dalla direttiva sul commercio elettronico. La responsabilità per la condivisione non autorizzata di materiali protetti da diritto d'autore è comunque esclusa se il gestore

dei Diritti dell'Uomo ha ripetutamente censurato la creazione di aree di impunità in favore dei prestatori di servizi nella rete, così addirittura sollecitando un ripensamento generale del diritto dell'Unione[5].

Dinanzi al quadro tratteggiato, sembra utile fare il punto sulle attuali tendenze relative alla responsabilità degli ISP e cercare di delineare i possibili sviluppi della materia. Nelle pagine che seguono approfondiremo dunque il ruolo dei gestori dei *social media* nel contrasto ai reati commessi nella rete: inizieremo richiamando alcuni profili generali della responsabilità dei fornitori di servizi *internet* nell'ambito del c.d. *Web 2.0*[6]; quindi esamineremo gli orientamenti emersi nella nostra giurisprudenza penale con riferimento alla punibilità dei *blogger* per gli illeciti realizzati dagli utenti, per passare poi a considerare il modello di disciplina proposto dalla "legge per il miglioramento della tutela dei diritti sui *social networks*" (*Netzwerkdurchsetzungsgesetz*), entrata in vigore in Germania il 1° ottobre 2017. Per finire, faremo alcuni cenni alle problematiche inerenti ai *provider* che svolgono un'attività essenzialmente criminale; i risultati dell'indagine costituiranno la base per una breve riflessione intorno alle linee evolutive della materia.

2. La responsabilità dell'ISP nell'era del *Web 2.0*: inquadramento del tema.

Che l'assetto normativo disegnato dalla direttiva sul commercio elettronico sia stato superato dall'evoluzione tecnologica è un dato oramai ampiamente acquisito all'interno della comunità giuridica. È infatti noto che con l'avvento del c.d. *Web 2.0* l'attività svolta dai *provider* è andata incontro a una profonda mutazione, di talché solo in parte essa può attualmente essere descritta ricorrendo alle categorie – *mere conduit*, *hosting* e

del sito dimostra 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 [abbia] ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti»; in ogni caso, il *provider* non risponde se prova «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». Va peraltro precisato che, a norma dell'art. 2, n. 6, 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».

[5] Di particolare importanza è la sentenza della Grande Camera nel caso *Delfi c. Estonia*, ric. 64569/09 (2015), con la quale i giudici di Strasburgo hanno affermato la compatibilità con l'art. 10 CEDU, relativo alla libertà di espressione, della condanna al risarcimento del danno emessa nei confronti di un portale d'informazione per la mancata rimozione dei contenuti illeciti pubblicati dagli utenti; sulla sentenza e sui successivi orientamenti della Corte EDU R. Petruso, *Responsablità delle piattaforme* online, *oscuramento di siti* web *e libertà d'espressione nella giurisprudenza della Corte Europea dei Diritti dell'Uomo*, in *Dir. inf.*, 5, 2018, 520 ss.

[6] Con questa espressione s'intende «un sistema di interconnettività ove gli utenti non sono più solamente destinatari di contenuti, ma possono interagire immettendo essi stessi materiali in forma di testi, video, musica o immagini, con dinamiche comunicative» (S. Seminara, Internet, in *Enc. dir.*, 2014, Ann. VII, 568).

caching – utilizzate dal legislatore dei primi anni duemila[7]. Mentre l'espansione della "mediasfera"[8], derivante dalla comparsa nel mercato di nuovi strumenti tecnologici (*smartphone*, *tablet*) e dalla capillare diffusione di quelli più tradizionali, ha determinato il venir meno delle esigenze economico-sociali che avevano giustificato l'adozione di quella disciplina[9].

Ciò nondimeno, il Parlamento Europeo non è ancora approdato a una revisione organica della normativa; il dibattito all'interno dell'Unione si è concentrato invece sulla soddisfazione di specifici bisogni di protezione, essenzialmente collegati all'utilizzo delle reti sociali[10]. Si è invero osservato che, nei *social network*, la possibilità per l'utente di nascondere la propria identità personale, unita alla facoltà di scegliere la propria rete di connessioni, agisce da detonatore rispetto a fenomeni che attingono beni personali d'importanza primaria (si allude soprattutto alla realtà dei cosiddetti "discorsi d'odio", ma la considerazione vale anche per i più tradizionali reati di opinione[11]). Mentre il sempre maggiore ricorso ai *social media* come strumenti di informazione aumenta il rischio di diffusione di notizie false (le c.d. *fake news*), con notevoli ricadute sulla tenuta democratica delle istituzioni[12]. Donde l'assunzione di iniziative volte a contrastare le forme più aggressive o menzognere di comunicazione nella rete[13].

---

[7] Così, *ex multis*, L. Picotti, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. Cadoppi-S. Canestrari-A. Manna-M. Papa (diretto da), Cybercrime, Torino, 2019, 87; S. Seminara, Internet, cit., 601; R. Flor, Social networks *e violazioni penali dei diritti d'autore. Quali prospettive per la responsabilità dei fornitori del servizio?*, in *Riv. trim. dir. pen. ec.*, 3, 2012, 673 ss.

[8] L'uso di questa espressione per individuare «un ambiente […] in cui i media elettronici in rete giocano un ruolo fondamentale» è mutuato da R. De Simone, *Presi nella rete. La mente ai tempi del* web, Milano, 2012, 11, secondo il quale «la fase attuale è caratterizzata da un'ubiquità dei media che non ha precedenti nella storia. […] Siamo immersi in permanenza nella mediasfera».

[9] Nella dottrina penalistica, per tutti, L. Picotti, *Diritto penale e tecnologie*, cit., 87; nella letteratura civilistica, per un'analoga considerazione e una sintetica esposizione delle ragioni ispiratrici della direttiva 2000/31/CE R. Panetta, *Il ruolo dell'*internet service provider *e i profili di responsabilità civile*, in *Resp. civ. e prev.*, 3, 2019, 1019 ss.; in tema vd. anche M. Montanari, *La responsabilità delle piattaforme* on-line *(il caso di Rosanna Cantone)*, in *Dir. inf.*, 2, 2017, 256-257.

[10] Va detto che questo approccio trova riscontro all'interno della giurisprudenza della Corte Europea dei Diritti dell'Uomo, la quale, in ossequio al principio di proporzione, diversifica i criteri di responsabilità dei *provider* in relazione ai singoli fenomeni criminali: su questa base, ad esempio, accoglie soluzioni maggiormente responsabilizzanti ogniqualvolta viene in rilievo il fenomeno dell'incitamento all'odio e alla violenza (sul punto R. Petruso, *Responsabilità delle piattaforme* online*,* cit., 534-535).

[11] In argomento A. Spena, *La parola(-)odio*, in *Criminalia*, 2016, 579-580; da ult. V. Nardi, *I discorsi d'odio nell'era digitale: quale ruolo per l'*internet service provider?, in *Dir. pen. cont.*, 7 marzo 2019, 6-7. In aggiunta alle considerazioni riportate nel testo, si può evidenziare che l'avvento delle reti sociali sembra avere favorito anche la crescita dei movimenti negazionisti: in tema G. Ziccardi, *Il negazionismo in* Internet*, nel* deep web *e sui* social network*: evoluzione e strumenti di contrasto*, in *notizie di Politeia*, 2017, 108 ss.

[12] Secondo un'impostazione piuttosto diffusa, riconducibile alla letteratura nordamericana, le *fake news* consistono in «articoli recanti notizie che sono intenzionalmente e verificabilmente false e potrebbero trarre in inganno i lettori»; sul punto e per approfondimenti relativi alle ricadute costituzionali di questo fenomeno G. Pitruzzella, *La libertà di informazione nell'era di* Internet, in *Parole e potere. Libertà di espressione,* hate-speech *e* fake-news, Milano, 2017, ora in *questa Rivista*, 1, 2018, 13 ss. Per un inquadramento del tema nella prospettiva penale, invece, T. Guerini, *La tutela penale della libertà di manifestazione del pensiero nell'epoca delle* fake news *e delle infodemie*, in *disCrimen*, 15 giugno 2020, 11 ss.

[13] A tal proposito si segnala che la Commissione Europa ha promosso, in collaborazione con alcuni colossi del *web* e del *social networking*, la redazione e applicazione di un codice di condotta (*Code of conduct countering illegal hate speech online*) volto a contrastare il fenomeno dei discorsi d'odio. Maggiori dettagli

Di fronte dell'inerzia del legislatore, il nostro diritto pretorio ha preso dunque ad allargare l'ambito di responsabilità dei *provider*. Valorizzando le indicazioni provenienti dalle Corti superiori, la giurisprudenza dapprima ha ricondotto i portali di informazione *online* entro il perimetro dell'art. 57 c.p.[14], quindi – ed è questo il problema che c'interessa adesso analizzare – ha incominciato a delineare criteri di imputazione affatto originali per gli illeciti commessi nelle reti sociali. È chiaro, peraltro, che una simile operazione deve fare i conti con i limiti posti dal diritto positivo; pertanto, occorre verificare la fondatezza a livello sistematico di queste soluzioni e la loro compatibilità con i principi stabiliti dalla direttiva 2000/31/CE. Prima di procedere in tale direzione, è opportuno però precisare le nozioni di *social network* e riepilogare i tratti salienti della disciplina vigente, di cui occorre tenere conto per inquadrare l'attività di questi *provider*; senza trascurare inoltre che nella giurisprudenza civile va consolidandosi un'interpretazione evolutiva del d. lgs. 70/2003.

Iniziando dal concetto di *social network*, in un'accezione più lata l'espressione viene utilizzata come sinonimo di *social media*, per individuare tutti i siti la cui caratteristica principale consiste nell'offerta di uno spazio virtuale, all'interno del quale gli utenti hanno la possibilità di comunicare e condividere contenuti[15]. È bene precisare che, sotto questo profilo, reti come *Facebook* e *Twitter* non si differenziano da altri *user content aggregator service provider*, quali piattaforme di *video-sharing* o *blog* che contengono aree a disposizione per i commenti dei lettori; rispetto a tali figure, essi si contraddistinguono essenzialmente per la possibilità riconosciuta al singolo fruitore di creare un'identità personale e una rete di contatti con la quale condividere le proprie connessioni[16]. Data l'ampiezza della nozione, non sorprende che alla denominazione di *social network* possano essere ricondotti siti che variano notevolmente per i temi oggetto della comunicazione così come per il regolamento economico-contrattuale. Sotto il primo profilo, occorre invero considerare che mentre alcune piattaforme hanno un contenuto generalistico (ad esempio *Facebook*), altre mettono in collegamento i membri di una comunità definita (si pensi ad *Academia.edu*) ovvero toccano specifici ambiti della vita sociale (come quello professionale: così *LinkedIn*); non mancano nemmeno *network*

possono essere rinvenuti alla pagina *The EU Code of conduct on countering illegal hate speech online*; per un quadro più completo delle iniziative assunte all'interno dell'Unione nella lotta all'*hate speech* V. Nardi, *I discorsi d'odio*, cit., 8-9. Infine, con riferimento alle proposte di regolamentazione volte a contrastare il fenomeno delle *fake news* nel quadro europeo, E. Lehner, Fake-news *e democrazia*, in *questa Rivista*, 1, 2019, 98 ss.

[14] Questo filone giurisprudenziale è stato inaugurato da Cass. pen., 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. Per un commento critico sul tema 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.

[15] Alcuni autori utilizzano in questo senso solo l'espressione *social media*: per una simile e più opportuna soluzione, C. Fuchs, *La politica economica dei* social media, in *Sociologia della comunicazione*, 43, 2012, 62; la definizione proposta nel testo si trova ad esempio in S. Martinelli, *L'autorità privata del* provider, in P. Sirena-P. Zoppini (a cura di), *I poteri privati e il diritto della regolazione*, Roma, 2018, 556 s.

[16] Sul punto e per una panoramica dell'evoluzione storica delle reti sociali G. Riva, *I* social network, in *Manuale di informatica giuridica e diritto delle nuove tencologie*, a cura di M. Durante-U. Pagallo, Torino, 2012, 467 ss.; la definizione richiamata nel testo è accolta anche da E. Rosati-G. Sartor, Social networks *e responsabilità del* provider, in *EUI working papers*, LAW 2012/05, 1-2. Nella dottrina penalistica vd. L. Picotti, *I diritti fondamentali nell'uso ed abuso dei* social network. *Aspetti penali*, in *Giur. mer.*, 12, 2012, 2523B.

focalizzati sulla vendita di beni o servizi (ad esempio, *Airbnb*) ovvero sullo scambio di determinate tipologie di contenuti (come fotografie – *Instagram* – e materiali audiovisivi – *TikTok*). A livello economico, invece, accanto a *social network* che offrono un servizio gratuito e traggono utilità dalla profilazione degli utenti e dalla vendita delle relative informazioni (è il caso di *Facebook*), vi sono piattaforme che guadagnano dall'attività pubblicitaria (ad esempio *Youtube*) ovvero mettono in comunicazione i soggetti interessati alla vendita e all'acquisto di un bene, ottenendo un profitto dalle singole transazioni (si pensi ad *Airbnb*).

Venendo adesso al quadro normativo, bisogna anzitutto premettere che l'attività del fornitore di servizi di *social networking* può essere ricondotta all'interno del d. lgs. n. 70/2003; è noto che tale normativa si basa sul principio di neutralità del *provider* e in maniera coerente con questo presupposto esclude la responsabilità del fornitore di servizi per la memorizzazione prolungata o temporanea di contenuti illeciti. Più nel dettaglio, premessa la mancanza di un «obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza», il d. lgs. 70/2003 all'art. 16 stabilisce che il prestatore di servizi della società dell'informazione 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[17].

Tuttavia, dinanzi alla obsolescenza della vigente disciplina, la giurisprudenza civile ha preso ad elaborare diversi criteri di imputazione[18]. Invero, alcune sentenze hanno recepito la nozione di "*host provider* attivo" elaborata dalla Corte di Giustizia dell'Unione Europea per individuare le situazioni in cui il *provider* agisce sui dati memorizzati al fine di ottimizzarne la fruizione[19], concludendo che i gestori delle piattaforme di

[17] È opportuno precisare che l'art. 14, c. 1, lett. *b)* della direttiva 2000/31/CE stabilisce invece che il *provider* non è responsabile delle informazioni memorizzate, sempreché, una volta al corrente del fatto che l'attività o l'informazione è illecita, egli «agisca immediatamente per rimuovere le informazioni o disabilitarne l'accesso».

[18] Per una breve panoramica di questi orientamenti R. Bocchini, *La responsabilità civile plurisoggettiva, successiva ed eventuale dell'ISP*, in *Giur. it.*, 12, 2019, 2607-2608. È opportuno evidenziare che il modello di responsabilità del *provider* elaborato dalla giurisprudenza viene generalmente condiviso, sia pur con diverse sfumature, dalla dottrina: oltre all'Autore appena citato (2610 ss.), vd., *ex multis*, R. Panetta, *Il ruolo dell'*internet service provider, cit., 1019 ss.

[19] La nozione di "*host provider* attivo" è stata accolta da Cass. civ., sez. I, 21 febbraio 2019, n. 7708, in *Riv. dir. ind.*, 4-5, 2019, II, 201; fra i giudici di merito Trib. Roma, sez. XVII, 12 luglio 2019, n. 14757, in *Guida dir.*, 41, 2019, 49. Con riferimento invece alla giurisprudenza della Corte di Lussemburgo, vd. spec. CGUE, C-324/09, *L'Oréal SA e a. c. eBay Inernational AG e a.* (2011); è opportuno segnalare che l'orientamento secondo cui l'art. 14 della direttiva sul commercio elettronico si applica solo agli "*host provider* passivi" è stato recentemente avallato pure dalla Commissione europea, nella citata COM (2017) 555. Per completare il quadro, ricordiamo infine che il ridimensionamento del principio di neutralità del prestatore di servizi nella rete ha interessato anche l'attività dei motori di ricerca: nella nota pronuncia CGUE, C-131/2012, *Marjo Costela Gonzalez e AEPD c. Google Spain e Google Inc.* (2014), la Corte di Giustizia dell'Unione Europea ha riconosciuto in capo al *provider* l'obbligo, a determinate condizioni, di procedere alla cancellazione dei dati personali del richiedente, osservando che, «nella misura in cui l'attività di un motore di ricerca può incidere [...] sui diritti fondamentali alla vita privata e alla protezione dei dati personali, il gestore di tale motore di ricerca […] deve assicurare, nell'ambito delle sue responsabilità, delle sue competenze e delle sue possibilità, che detta attività soddisfi le prescrizioni della direttiva 95/46». Questo principio è stato peraltro recepito dal regolamento UE 2016/679, che all'art. 17 disciplina il cosiddetto "diritto all'oblio".

social networking non possono beneficiare dei *safe harbours* previsti dalla direttiva[20]. Nella medesima prospettiva, ma in maniera meno radicale, un più recente indirizzo giurisprudenziale afferma che, a prescindere dalla sua natura, il *provider* ha l'obbligo di rimuovere i contenuti illeciti di cui sia venuto a conoscenza, senza che sia necessaria una formale richiesta dell'autorità giudiziaria[21]. A questo proposito si è infatti evidenziato che l'assetto definito dal d. lgs. 70/2003 è incapace di apprestare una tutela efficace a interessi di natura personale, come l'immagine o la reputazione, con riferimento ai quali ogni protrazione dell'illecito rischia di determinare un danno irreparabile[22]; si è così asserito che la richiesta del privato va ritenuta sufficiente a far scattare l'obbligo del prestatore di eliminare i contenuti oggetto di segnalazione, e conseguentemente a determinare l'insorgere di una responsabilità civile nel caso di loro intempestiva rimozione.

3. Il ruolo dell'amministratore del *blog* nella giurisprudenza penale: vecchi problemi...

Sul versante penale, negli ultimi anni la questione del ruolo dei gestori delle reti sociali è stata affrontata con esiti innovativi all'interno di due sentenze relative alla responsabilità dell'amministratore del *blog* per la mancata rimozione dei contenuti illeciti pubblicati dagli utenti. Tali pronunce devono essere attentamente esaminate perché, sebbene siano relative a uno specifico mezzo di comunicazione (il *blog*), esse contengono principi teoricamente suscettibili di trovare applicazione anche agli altri *social media*. In via preliminare è opportuno rammentare che, esclusa l'applicabilità dell'art. 57 c.p., l'opinione prevalente in dottrina e in giurisprudenza riconduceva l'attività del gestore del diario virtuale entro l'ambito di applicazione del d. lgs. 70/2003; in maniera coerente con questa impostazione, la responsabilità del *blogger* era dunque limitata ai casi di partecipazione attiva agli illeciti commessi dagli utenti[23]. Superando questa impostazione, la Suprema Corte ha invece ritenuto punibile per diffamazione il titolare della piattaforma che mantiene in rete i commenti offensivi pubblicati dai lettori. Poiché, peraltro, per approdare a questa conclusione i giudici di legittimità hanno seguito percorsi differenti, è opportuno esaminare partitamente le due decisioni; iniziamo dun-

[20] Così Trib. Milano, 9 settembre 2011, n. 10893, in *Riv. dir. ind.*, 6, 2011, II, 364 ss. e 7 giugno 2011, n. 7680; più di recente App. Milano, 7 gennaio 2015, in *Riv. dir. ind.*, 1, 2017, II, 4 ss.

[21] Così Trib. Roma, sez. IX, 15 febbraio 2019, n. 3512, in *Riv. dir. ind.*, 4-5. 2019, II, 296; App. Firenze, sez. II, 11 aprile 2018, n. 862; Trib. Napoli Nord, 3 novembre 2016, in *Dir. inf.*, 2, 2017, 243 ss.; Trib. Roma, sez. IX, 27 aprile 2016, n. 8437; Trib. Milano, 7 giugno 2011, n. 7680.

[22] Sul punto Trib. Napoli Nord, 3 novembre 2016, cit., ove si afferma che, «venendo in rilievo diritti della personalità (quali l'immagine, il decoro, la reputazione, la riservatezza), appare irrazionale dover attendere un ordine dell'autorità, il quale potrebbe intervenire quando oramai i diritti in questione sono irrimediabilmente pregiudicati e non più suscettibili di reintegrazione».

[23] In dottrina 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 s.; 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, 1076-1077; in giurisprudenza vd. invece Cass. pen., sez. V, 16 luglio 2010, n. 35511, in *Riv. it. dir. proc. pen.*, 4, 1604 ss.; cfr. Cass. pen., sez. V, 19 febbraio 2018, n. 16751, in *Cass. pen.*, 11, 2018, 3743 ss.

que trattando della prima e rimandiamo al paragrafo che segue l'esame della soluzione più recente.

Al fine di affermare la responsabilità dell'amministratore del *blog*, la Corte di Cassazione (Cass. pen., sez. V, 14 luglio 2016, n. 54946) nel suo primo arresto ha ritenuto decisiva la mancata adozione delle iniziative necessarie ad evitare la protrazione dell'altrui reato di diffamazione. Partendo dal presupposto che, una volta venuto a conoscenza del carattere illecito della pubblicazione, il gestore del sito sia obbligato a porre fine alla violazione, si è concluso che questi risponde come concorrente nell'altrui reato.

Una simile ricostruzione presta però il fianco a molteplici obiezioni. Anzitutto, infatti, la punibilità *ex* art. 110 c.p. si infrange dinanzi alla istantaneità del reato di diffamazione: fissata la consumazione nella immissione in rete del contenuto lesivo, il suo mantenimento nel *web* da parte del gestore del sito costituisce una condotta susseguente, che giocoforza fuoriesce dallo schema del concorso di persone[24]. Inoltre, la configurazione di una responsabilità per omesso impedimento del reato cozza con l'impossibilità di affermare l'esistenza nel nostro sistema di una posizione di garanzia in capo al *provider*: tralasciando la possibilità di ricavare, nell'ambito delle normative di settore, degli specifici obblighi di protezione[25], il d. lgs. 70/2003 da un lato esclude un generale dovere di controllo del prestatore di servizi nella rete, dall'altro costituisce 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[26].

Per la verità, alla prima annotazione si potrebbe opporre che nella diffamazione a mezzo *internet* non è del tutto infondato parlare di permanenza della violazione, dal momento che, in casi come quello in esame, il reo mantiene il dominio sul fatto anche dopo la pubblicazione del contenuto lesivo dell'onore[27]. Del resto, sulla scorta di un'analoga considerazione, un'autorevole dottrina ha in passato argomentato il prolungamento della consumazione nelle ipotesi di cosiddetta diffamazione "per espo-

[24] Così già S. Seminara, *La responsabilità penale degli operatori* su internet, in *Dir. inf.*, 4-5, 1998, 765 s.; più di recente A. Ingrassia, *Responsabilità penale degli* internet service provider*: attualità e prospettive*, in *Dir. pen. proc.*, 12, 2017, 1625. Aperture nei confronti della configurabilità di una responsabilità «per omesso impedimento di protrazione *ex post*» del reato in R. Bartoli, *Brevi considerazioni sulla responsabilità penale dell'*internet service provider, in *Dir. pen. proc.*, 5, 2013, 606.

[25] Sul punto R. Flor, Social networks *e violazioni penali*, cit., 679, secondo il quale «a fronte dell'assenza di un obbligo generale di sorveglianza o di controllo "preventivo", sono state introdotte nuove norme in settori specifici, come nella lotta alla pedopornografia *on-line*, che prevedono puntuali doveri in capo al *service provider*, suscettibili di essere posti a fondamento di una responsabilità omissiva, sia autonoma, *ex* art. 40 cpv. c.p., che concorsuale, *ex* art. 110 c.p.».

[26] Escludono l'esistenza di una posizione di garanzia in capo al *provider*, *ex multis*, A. Ingrassia, *Responsabilità penale degli* internet service provider, cit., 1626 s.; Id., *Il ruolo dell'ISP nel cyberspazio: cittadino, controllore o tutore dell'ordine?*, in *Dir. pen. cont.*, 8 novembre 2012, 26 ss.; S. Seminara, Internet, cit., 597-598; R. Bartoli, *Brevi considerazioni*, cit., 602-603. Diversamente F. Sgubbi, *Parere* pro veritate, in *Dir. inf.*, 4-5, 2009, 746; L. Picotti, *Art. 600*-ter, *III comma c.p.*, in Cadoppi (a cura di), *Commentario delle norme contro la violenza sessuale e contro la pedofilia*, Padova, 2006, 210 ss.

[27] Va peraltro evidenziato che la ricostruzione accolta dalla sentenza in esame è ambigua, giacché la Suprema Corte non afferma il carattere permanente del reato, bensì radica la responsabilità sull'«aver l'imputato mantenuto consapevolmente l'articolo sul sito, consentendo che lo stesso esercitasse l'efficacia diffamatoria»; sottolinea questo aspetto A. Ingrassia, *Responsabilità penale degli* internet service provider, cit., 1625 ss.

sizione"[28]; pertanto, si potrebbe sostenere che l'internauta risponde di diffamazione per tutto il tempo in cui non rimuove il *post* illecito pubblicato sul *blog*. Senonché una simile ricostruzione trascurerebbe di considerare che un'interpretazione estensiva del "dominio sul fatto" risulta poco aderente alla realtà della comunicazione digitale, in cui è già la stessa nozione di autore a perdere di consistenza[29]; soprattutto, l'idea della permanenza del reato, unita alla mancanza di finitezza spazio-temporale della rete, è in grado di determinare un completo stravolgimento degli istituti collegati alla consumazione[30]. In effetti, è sufficiente riflettere sulle conseguenze derivanti con riferimento al diritto di querela e alla prescrizione per rendersi conto della natura dirompente di tale soluzione[31]; in definitiva, bisogna ammettere che è preferibile l'interpretazione che fissa il disvalore del reato nella diffusione del contenuto lesivo e conseguentemente afferma la natura istantanea della violazione[32].

Concludendo, la configurabilità di una responsabilità a titolo di concorso di persone va rifiutata alla luce della impossibilità di ricavare dal diritto positivo un generale obbligo di protezione in capo al *provider*; anche sotto questo profilo, non è dunque possibile sostenere che l'amministratore del *blog* risponde per omesso impedimento dell'altrui reato di diffamazione.

4. (*segue*) ...e nuove soluzioni.

Alla luce delle considerazioni che precedono non sorprende che, tornando sul tema, la Suprema Corte abbia da ultimo accolto una diversa soluzione: in un recente arresto

[28] Si allude alla distinzione fra pubblicazione "per distribuzione" e "per esposizione" enucleata da T. Padovani, *Il momento consumativo nei reati commessi col mezzo della stampa*, in *Riv. it. dir. proc. pen.,* 1971, 800 ss.; in generale, nel senso della configurabilità in forma permanente del reato di diffamazione, A. Pecoraro Albani, *Del reato permanente*, in *Riv. it. dir. proc. pen*., 1960, 421, il quale fa l'esempio di colui che ha cura di «mantenere esposto per lungo tempo sul balcone, al fine di ingiuriare il suo dirimpettaio, un bel paio di corna». Si evidenzia inoltre che nella giurisprudenza civile è diffusa l'idea del carattere permanente degli illeciti commessi nella rete (così, *ex multis*, Cass. civ., sez. I, 21 febbraio 2019, n. 7708, cit.); tale interpretazione riflette però la confusione fra permanenza del reato e delle sue conseguenze.

[29] In generale, sulla dissoluzione del testo nell'era della comunicazione digitale R. De Simone, *Presi nella rete*, cit., 114.

[30] Il rapporto fra il concetto di consumazione e il reato commesso nel *cyberspace* è approfondito soprattutto da L. Picotti, *Diritto penale e tecnologie*, cit., 89 ss., il quale però giunge a un'opposta conclusione: premessa l'opportunità di ricorrere alla distinzione fra perfezione e consumazione/esaurimento del reato, l'Autore conclude che «il reato cibernetico non può dirsi "esaurito" nel periodo intermedio anche assai lungo che può intercorrere fra i due momenti, in cui "permane" e si approfondisce l'offesa». Per ulteriori riflessioni intorno alla consumazione del reato di diffamazione a mezzo *Internet* sia consentito rinviare a S. Braschi, *La consumazione del reato. Fondamenti dogmatici ed esigenze di politica criminale*, Milano, 2020, 259 ss.

[31] Va infatti considerato che, secondo la giurisprudenza, il diritto di querela può essere esercitato fino alla cessazione della permanenza (sul punto, per tutti, C. Mazzucato, *Art. 124*, in G. Forti-S. Seminara-G. Zuccalà (a cura di), *Commentario breve al codice penale*, Milano, 2017, 557); in ogni caso, nell'ipotesi di scoperta tardiva del reato, si potrebbe giungere al risultato paradossale di punire una diffamazione anche a molti anni di distanza dalla pubblicazione nella rete del *post* illecito.

[32] Sul punto, per tutti, S. Seminara, *La responsabilità penale*, cit., 765, secondo cui "i reati (di condotta) fondati su verbi modali come diffondere, divulgare ecc. si consumano nel momento in cui i contenuti illeciti sono resi accessibili da parte del loro autore».

(Cass. pen., sez. V, 8 novembre 2018, n. 12546) è stato affermato che l'amministratore del *blog*, il quale non elimina i commenti offensivi pubblicati dagli utenti, risponde di un autonomo reato di diffamazione.

Ad avviso dei giudici di legittimità, creando e gestendo una piattaforma di comunicazione, l'amministratore del *blog* tiene un comportamento positivo, che contribuisce alla circolazione del contenuto prodotto dall'utente; ne deriva che, nel caso in cui venga informato dalla natura illecita della pubblicazione, il gestore del sito può essere considerato responsabile di un nuovo reato di diffamazione. Rispetto alla precedente ricostruzione, la novità consiste dunque nell'inquadramento della condotta del *blogger* all'interno della responsabilità commissiva e nell'attribuzione ad essa di un'autonoma rilevanza penale; in questo modo si ritiene possibile aggirare l'obiezione secondo cui il diritto vigente non pone in capo al *provider* nessun obbligo di protezione, che giustifichi la configurazione di una responsabilità a titolo di concorso di persone.

Per la verità, la qualificazione in termini autonomi del comportamento dell'amministratore del sito, che non rimuove i contenuti pubblicati dagli utenti, non rappresenta un'assoluta novità; al contrario, essa trova un importante precedente giurisprudenziale nella sentenza relativa al caso noto come *Google vs Vividown*[33]. In quell'occasione, infatti, i giudici di legittimità sostennero che, una volta informato della illiceità dei contenuti ospitati sul proprio portale, il gestore della piattaforma di *video-sharing* acquisisce la qualifica di "responsabile del trattamento" e per questa ragione risponde del reato previsto dall'art. 167 d. lgs. 30 giugno 2006, n. 196. Peraltro, una simile ricostruzione sembra oggi confortata dal disposto dell'art. 17 della direttiva (UE) 2019/790, a norma del quale la condotta del *provider* che ospita un contenuto sul proprio portale deve essere trattata alla stregua di «un atto [positivo] di condivisione al pubblico»[34].

Nemmeno questa soluzione risulta però convincente.

Anzitutto si potrebbe obiettare che, dal punto di vista sistematico, non trova conferma l'obbligo dell'ISP di rimuovere i contenuti lesivi dell'onore, che siano oggetto di segnalazione da parte dell'utente. Per comprendere il significato di questa osservazione occorre considerare che gli artt. 14-*ter* e -*quater* l. 3 agosto 1998, n. 269, e l'art. 1, c. 2, d.l. 18 febbraio 2015, n. 7, stabiliscono che i siti contenenti materiale pedopornografico ovvero implicati nella commissione di reati di terrorismo siano inseriti in un apposito elenco presso il Ministero degli interni e oscurati su richiesta dell'autorità giudiziaria. Sembra dunque del tutto irragionevole che, proprio nei casi di diffamazione, in cui si rende necessario contemperare interessi di rango costituzionale, spetti invece interamente al gestore della piattaforma di comunicazione verificare l'esistenza del reato[35].

---

[33] Si tratta di Cass. pen., sez. III, 17 dicembre 2013, n. 5107, in *Riv. pen.*, 5, 2014, 495; va peraltro precisato che in quest'ultimo caso, a differenza che nella vicenda in esame, la Suprema Corte affermò la configurabilità di una responsabilità penale in capo al *provider* per la sua mancata attivazione, sul presupposto di una previa comunicazione da parte dell'autorità competente. Sul punto, per alcune brevi considerazioni, A. Ingrassia, *Responsabilità penale degli* internet service provider*,* cit., 1623 s.

[34] I contenuti essenziali della direttiva sono riportati *retro*, nt. 4.

[35] Invero, l'impostazione accolta dal d. lgs. 70/2003, che, come visto sopra, all'art. 16 subordina l'obbligo di attivazione del *provider* alla richiesta dell'autorità amministrativa o giudiziaria, risponde «allo scopo di rafforzare la determinatezza della fattispecie, evitando al *provider* l'onere di autonome iniziative con i connessi rischi di una responsabilità risarcitoria» (S. Seminara, Internet, cit., 603).

In secondo luogo, il ragionamento seguito dalla Corte di Cassazione appare fragile: non è infatti chiaro come mai, in assenza di un obbligo di rimozione, l'automatico, ininterrotto funzionamento dei meccanismi di diffusione dei dati nella rete possa acquisire un'autonoma tipicità penale[36]. A tacer del fatto che una simile ricostruzione svuota di significato il concetto di azione[37], essa è contraddetta dalla circostanza che, come visto, per sanzionare la mancata rimozione dei contenuti illeciti già oggetto di memorizzazione, il legislatore abbia avvertito la necessità di introdurre un apposito obbligo di attivazione (art. 16, c. 1, lett. *b)*, d. lgs. 70/2003). La verità è che la ricostruzione proposta dai giudici di legittimità costituisce un *escamotage* volto ad aggirare il principio secondo cui il dovere d'intervento del *provider* presuppone una comunicazione dell'autorità giudiziaria: in altri termini, la Suprema Corte ha cercato di trasferire sul piano penale l'orientamento accolto dalla giurisprudenza civile, secondo cui è sufficiente la segnalazione del privato perché scatti l'obbligo di eliminare le informazioni illecite memorizzate[38]. È chiaro, però, che una simile operazione cozza con l'art. 25 Cost., configurando una forma di responsabilità priva di fondamento legale; per questo motivo, la soluzione proposta dalla Cassazione non può essere accettata.

Giunti a questo punto, per completare il quadro sembra opportuna una breve riflessione sulla figura dell'"*host provider* attivo"; si è visto sopra che questa nozione viene utilizzata per individuare i fornitori di servizi nella rete che non svolgono attività meramente automatiche e passive e che perciò dovrebbero rimanere estranei all'ambito di applicazione del d. lgs. 70/2003. A tal proposito va premesso che lo scopo della costruzione è quello di ovviare ai limiti della disciplina vigente, adattando il modello di allocazione dei rischi connessi all'utilizzo di *internet* all'attuale realtà delle reti sociali: poiché, infatti, questi *provider* traggono profitto dalla elaborazione delle informazioni prodotte dagli utenti[39], si ritiene che essi siano tenuti anche a sostenere i costi derivanti dalla realizzazione di fatti pregiudizievoli per i fruitori[40]. Fatta questa precisazione,

[36] A tal proposito, la S.C. si limita ad affermare che «se […] il gestore del sito apprende che sono stati pubblicati da terzi contenuti obiettivamente denigratori e non si attiva tempestivamente a rimuovere tali contenuti, finisce per farli propri e quindi per porre in essere ulteriori condotte di diffamazione, che si sostanziano nell'aver consentito, proprio utilizzando il suo *web-log*, l'ulteriore divulgazione delle stesse notizie diffamatorie».

[37] Sul tema vd. le considerazioni di S. Seminara, Internet, cit., 570, secondo cui «la nozione di condotta […] richiede sempre un dominio dell'agente sul fatto, che preclude ogni sua dilatazione diretta a comprendere ulteriori effetti collegati al funzionamento di *Internet* e all'operato di ulteriori *server* o all'attività degli utenti».

[38] Considerazioni analoghe, con riferimento però alla sentenza esaminata nel paragrafo che precede, si rinvengono in R. Carbone, *Responsabilità del* blogger: *parziale* revirement *della Cassazione?*, in *Cass. pen.*, 7-8, 2017, 2787 s.

[39] Fermo restando quanto abbiamo evidenziato *supra* con riferimento alla estrema varietà dei *social network*, vd., per approfondimenti sul meccanismo di sfruttamento economico dei dati degli utenti da parte di siti come *Facebook*, S. Sica-G. Giannone Codiglione, Social network sites *e il "labirinto" delle responsabilità*, in *Giur. mer.*, 12, 2012, 2716 ss.; più in generale, per un'analisi critica del modello economico caratteristico del c.d. capitalismo dell'informazione C. Fuchs, *La politica economica dei* social media, cit., 74 ss.

[40] Così, sostanzialmente, R. Bocchini, *La responsabilità civile plurisoggettiva*, cit., 2608 ss.; sul punto, ampiamente, F. Di Ciommo, *Programmi-filtro e criteri di imputazione/esonero della responsabilità* on-line. *A proposito della sentenza Google/Vividown*, in *Dir. inf.*, 6, 2010, 853, secondo cui «in una situazione legislativa in cui ai *provider* non si chiede un controllo sui contenuti veicolati in *Internet* […] nessuno è incentivato

va evidenziato che un ragionamento non dissimile potrebbe trovare spazio anche in campo penale: poiché, infatti, la finalizzazione delle piattaforme sociali a uno scopo di profitto può porre queste in conflitto con le esigenze di protezione degli interessi degli utenti[41], appare tutt'altro che irragionevole imporre ai gestori dei siti obblighi di attivazione eventualmente presidiati dalla sanzione penale. Tuttavia, è chiaro che un simile discorso si inscrive in un orizzonte di politica criminale, mentre il ricorso alla nozione di "*host provider* attivo" non può giustificare l'applicazione di criteri d'imputazione *de iure condito* privi di fondamento legale: in mancanza di un intervento del legislatore, resta dunque necessario fare riferimento alle comuni regole in tema di concorso di persone, verificando alla luce della struttura della piattaforma sociale il contributo effettivamente apportato alla commissione del reato.

In conclusione, la ricostruzione offerta dalla Suprema Corte non può essere condivisa, giacché si pone in contrasto col diritto positivo, in base al quale il *provider* è tenuto a rimuovere i contenuti illeciti immessi nella rete previa richiesta dell'autorità giudiziaria. Fissato questo punto, occorre peraltro riconoscere che l'attuale sviluppo delle piattaforme sociali suggerisce di meditare sulla opportunità di riformare la disciplina vigente; come anticipato, in questa direzione si è già mosso il legislatore tedesco, approdando a una soluzione affatto originale, che è opportuno adesso esaminare.

5. Un possibile modello di disciplina? I contenuti della *Netzwerkdurch-setzungsgesetz*

Come accennato in apertura del lavoro, il tema del contrasto ai reati commessi nelle reti sociali è stato al centro di un recente intervento del legislatore tedesco, sfociato nell'adozione della *Netzwerkdurchsetzungsgesetz* (di seguito NetzDG). Scopo dichiarato della disciplina è quello di implementare la corretta interazione degli utenti nei *social network*, contrastando le forme più aggressive di comunicazione ovvero la diffusione di *fake news*[42]; la legge presenta però un ben più ampio raggio d'azione[43].

Procedendo a una sommaria esposizione dei suoi contenuti, bisogna anzitutto dire che la NetzDG trova applicazione ai *social network* con più di due milioni di utenti registrati

ad investire in *software* o strategie aziendali in grado, se non proprio di eliminare, di limitare il rischio costituito da illeciti commessi da utenti rimasti anonimi. […] Tutto ciò aumenta certamente le possibilità che in rete vengano commessi illeciti senza che nessuno risponda del relativo danno e, dunque, contribuisce ad aumentare la sensazione di deresponsabilizzazione che l'utente provoca mentre naviga».

[41] Esemplare in questo senso è la vicenda di Tiziana Cantone, giovane donna ritratta in alcuni video pornografici amatoriali successivamente diffusi nella rete: per ottenere la rimozione delle pagine che la rigurdavano, frattanto diventate di grande successo nella rete, la ragazza dovette affrontare una dura battaglia legale contro *Facebook*, la quale fu portata a termine dalla madre dopo il suo suicidio. Per un breve resoconto della storia e dei suoi risvolti a livello penale G. M. Caletti, *"Revenge porn" e tutela penale*, in *Dir. pen. cont.- Riv. trim.*, 3, 2018, 65 ss.

[42] BT-Drucksache 18/12356, 11 s. Per una panoramica del contesto nel quale si inscrive l'intervento normativo, per tutti, S. Müller-Franken, *Netzwerkdurchsetzungsgesetz: Selbstbehauptung des Rechts oder erster Schritt in die selbstregulierte Vorzensur? – Verfassungsrectliche Fragen*, in *Archiv für Presserecht*, 1, 2018, 1 ss.

[43] Per questa annotazione, con accento critico, vd. già le osservazioni della *Deutsche Gesellschaft für Recht und Informatik* (*Stellungnahme der DGRI zum Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG)*, in *Computer und Recht*, 2017, 311).

in Germania; è bene inoltre precisare che la legge accoglie una definizione ampia di *social network*, riferendosi ai «fornitori di servizi di telecomunicazione che per scopo di profitto gestiscono piattaforme *internet* progettate per permettere agli utenti di condividere qualunque tipo di contenuto o di renderlo accessibile al pubblico» (§ 1 NetzDG)[44].
A carico di questi *provider* vengono posti due obblighi fondamentali: da un lato, essi sono chiamati a svolgere un resoconto semestrale sull'attività di gestione delle segnalazioni effettuate dagli utenti con riferimento alla presenza di contenuti antigiuridici nella rete; dall'altro, devono adottare procedure trasparenti ed efficaci per la rimozione di tale materiale. Per individuare la nozione di "contenuti antigiuridici", la legge fa rimando ad alcune disposizioni del codice penale: senza pretesa di esaustività si possono ricordare i §§ 86 e 86a, relativi all'utilizzo di simboli e propaganda politica vietata, il § 111, che incrimina il pubblico incitamento alla violenza, i §§ 184b e 184d concernenti la pubblicazione e la detenzione di materiale pedopornografico, e i §§ 185-187, in tema di ingiuria e diffamazione. La violazione degli obblighi menzionati configura un illecito amministrativo punito con una sanzione pecuniaria, che nei casi più gravi può raggiungere l'importo di cinque milioni di euro; la legge trova applicazione anche agli illeciti commessi all'estero (§ 4 NetzDG)[45].
La scelta del legislatore tedesco è stata dunque quella di rendere obbligatoria l'adozione di misure di *notice and take down*, a tale scopo indicando alcuni principi generali che devono essere seguiti dai *provider*. Invero, la NetzDG stabilisce che i gestori delle reti sociali devono predisporre procedure di segnalazione e rimozione facilmente accessibili e tempestive; soffermandoci su quest'ultimo punto, la legge impone termini stringenti per la rimozione dei materiali oggetto di segnalazione: ventiquattro ore nelle ipotesi di illiceità manifesta, sette giorni negli altri casi. Essa inoltre stabilisce che, ogniqualvolta la liceità del contenuto dipende dalla veridicità di una dichiarazione, il *social network* può sollecitare la replica dell'autore (§ 3 NetzDG); per la soluzione dei casi più controversi la legge prevede infine che venga interpellato un organo di autoregolamentazione indipendente appositamente creato[46].
Come si vede, la NetzDG non interviene sulla responsabilità penale del gestore della rete sociale, la cui punibilità rimane dunque circoscritta ai casi di consapevole mancata rimozione dei contenuti illeciti oggetto di segnalazione, secondo quanto previsto dalla *Telemediengesetz*[47]; né essa intacca il principio secondo cui il *provider* non è tenuto ad effet-

[44] Vengono dunque esclusi i quotidiani *online* (per i quali vige un più severo regime di responsabilità penale) e le piattaforme di comunicazione individuale (si pensi a *Whatsapp*), mentre sono ricompresi, ad esempio, siti di *e-commerce* come *eBay*; sul punto G. Nolte, *Hate-Speech, Fake-News, das «Netzwerkdurchsetzungsgesetz» und Vielfaltsicherung durch Suchmaschinen*, in *Zeitschrif für Medienwissenschaft*, 2017, 555, il quale peraltro evidenzia la scarsa determinatezza della disposizione e il suo difetto di corrispondenza col linguaggio comune, presso il quale la nozione di *social network* assume un significato più circoscritto (sul punto *retro*, § 2).

[45] Con riferimento alle sanzioni occorre inoltre considerare che il § 30, c. 2, *Ordnungswidrigkeitengesetz* consente di aumentare fino a dieci volte l'importo massimo della sanzione pecuniaria prevista dalla legge.

[46] Sul punto vd. il § 3, c. 3, lett. *b)* e c. 6, ove sono specificati i requisiti necessari per l'accreditamento dell'organo di autoregolamentazione.

[47] Così chiaramente G. Nolte, *Hate-Speech*, cit., 553. Bisogna ricordare che l'attività del gestore del *social network* ricade all'interno del § 10 *Telemediengesetz*, il quale limita la punibilità dell'*host provider* ai casi

tuare alcun controllo preventivo sui contenuti pubblicati dagli utenti. La legge rafforza invece i doveri di intervento *ex post* dei gestori delle reti sociali, spostandoli dal campo dell'autoregolamentazione a quello della responsabilità amministrativa[48]; la notevole severità della sanzione dovrebbe assicurare il rispetto da parte dei *provider* delle prescrizioni stabilite dalla normativa.

Vero ciò, va peraltro considerato che, non di rado, la violazione degli obblighi che abbiamo riferito potrà emergere in occasione dei giudizi civili o penali concernenti i "contenuti antigiuridici" oggetto di segnalazione. Sotto questo profilo, il modello di responsabilità introdotto dalla NetzDG potrebbe essere accostato a quello previsto per gli enti dal § 30 *Ordnungswidrigkeitengesetz* (di seguito OWiG)[49]: anche nel caso in esame, infatti, la responsabilità amministrativa si salda con quella della persona fisica derivante dalla commissione di un reato. Inoltre, sul piano politico-criminale, si è già evidenziato che l'assoggettamento a sanzione dei gestori della rete sociale si fonda sulla considerazione che questi *provider* traggono profitto dall'attività svolta dai fruitori[50]; né si può trascurare che l'adozione di *policy* maggiormente restrittive nella rimozione dei contenuti illeciti è in grado, se non di eliminare, quantomeno di limitare significativamente le offese prodotte con le singole violazioni. Poiché, però, la responsabilità amministrativa regolata dal § 30 OWiG, a differenza di quella prevista dalla NetzDG, necessariamente presuppone la commissione di un reato e uno stretto collegamento fra la società e il suo autore, mentre un simile legame manca tra il fornitore del servizio di *social networking* e il singolo utente della rete, non è possibile spingere oltre il parallelismo fra i due meccanismi di imputazione.

6. (*segue*) e le sue criticità

Passando a valutare la bontà della disciplina che abbiamo illustrato, va detto che sin dalla presentazione del relativo progetto di legge, la NetzDG ha sollevato molteplici perplessità, essenzialmente dipendenti dalla sua asserita incompatibilità col diritto eurounitario e costituzionale[51].

in cui la mancata tempestiva rimozione del contenuto illecito è sorretta da dolo diretto; a differenza che nel nostro sistema, per la responsabilità del fornitore di servizi nella rete non è peraltro necessaria una segnalazione istituzionale della illiceità del contenuto. Per una panoramica sui presupposti della responsabilità dell'*host provider* in Germania, per tutti, J. Eisele, *vor § 184*, in A. Schönke-H. Schröder (a cura di), *Strafgesetzbuch Kommentar*, München, 2019, 1876 s., *Rn.* 84 ss.

[48] Evidenzia questo aspetto G. Nolte, *Hate-Speech, Fake-News*, cit., 555, secondo il quale sarebbe stato più opportuno intervenire rimanendo nel campo dell'autoregolamentazione. Con specifico riferimento al rapporto fra NetzDG e responsabilità civile del *provider* cfr. K. N. Peifer, *Fake News und Providerhaftung. Warum das NetzDG von Fake News die falschen Instrumente liefert*, in *Computer und Recht*, 12, 2017, 811 s.

[49] Per una sintetica illustrazione del sistema di responsabilità amministrativa degli enti in Germania e per ampi riferimenti bibliografici G. Heine/B. Weißer, *Vorbem. §§ 25 ff.*, in A. Schönke-H. Schröder, *Strafgesetzbuch Kommentar*, cit., 513 ss., *Rn.* 121 ss.; nella letteratura italiana V. Mongillo, *La responsabilità penale tra individuo ed ente collettivo*, Torino, 2018, 243 ss.

[50] Cfr., sul duplice scopo «preventivo-repressivo» e «di riequilibrio economico» del modello punitivo delineato dal § 30 OWiG, V. Mongillo, *La responsabilità penale*, cit., 246-247.

[51] Una panoramica completa dei profili di ritenuta illegittimità della NetzDG si rinviene in V. Claussen, Fake-news*, pluralismo informativo e responsabilità in rete*, in *questa Rivista*, 3, 2018, 119 ss.

Sotto il primo profilo, si è infatti sostenuto che la legge sarebbe contraria al principio della libera circolazione dei prestatori dei servizi dell'informazione, stabilito dall'art. 3 della direttiva 2000/31/CE; si è poi argomentato che la NetzDG contrasterebbe con l'art. 17 della stessa direttiva, secondo cui l'obbligo di rimozione presuppone una "conoscenza effettiva" della illiceità della comunicazione; infine, si è affermato che, individuando termini perentori per la rimozione dei contenuti, la nuova normativa violerebbe la regola secondo cui l'azione del *provider* è illecita (solo) se intempestiva[52].
Ancora più articolate le obiezioni relative alla conformità della normativa alla Costituzione, a proposito delle quali ci limitiamo ad alcuni brevi cenni. Le critiche principali riguardano il pericolo di una eccessiva compressione alla libertà di manifestazione del pensiero: si osserva infatti che la previsione di termini stringenti, unita alla prospettiva di incorrere in responsabilità per la mancata rimozione dei contenuti illeciti, non potrebbe che avere l'effetto di sollecitare l'adozione da parte dei *provider* di atteggiamenti fortemente censori[53]; inoltre, il sistema delineato dalla legge sarebbe discutibile anche sotto il profilo della cessione a soggetti privati del potere, di natura tipicamente pubblicistica, di accertare la liceità di una determinata comunicazione[54].
Iniziando dai dubbi relativi al diritto eurounitario, le obiezioni che abbiamo sinteticamente riferito sembrano superate alla luce degli orientamenti assunti dalla Commissione Europea, che con la raccomandazione approvata il 1° marzo 2018 ha invitato gli Stati membri e i *provider* a cooperare per l'adozione di procedure di *notice and take down* efficaci e trasparenti[55]; sotto questo profilo, si potrebbe persino affermare che la normativa tedesca si candida a rappresentare un modello per gli altri paesi dell'Unione.
Più delicata è, invece, la questione relativa ai rischi di un'eccessiva limitazione della libertà di espressione. Alle obiezioni che abbiamo riferito si potrebbe invero controbattere che la legge fonda la responsabilità del *social network* sulla mancata adozione di procedure efficaci e tempestive di segnalazione e rimozione dei contenuti antigiuridici, mentre prescinde dal giudizio relativo alla correttezza delle singole statuizioni; per questo motivo, non vi sarebbe alcun pericolo di un controllo pervasivo sulle comunicazioni[56]. Quanto poi all'attribuzione ai *provider* di prerogative tipiche del potere giudi-

[52] Per queste obiezioni vd. G. Spindler, *Internet Intermediary Liability Reloaded. The New German Act on Responsibility of Social Networks and its (In-)Compatibility with European Law*, in *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2, 2017, 167 ss.

[53] S. Müller-Franken, *Netzwerkdurchsetzungsgesetz*, cit., 7 ss.; l'Autore punta il dito, fra l'altro, sul c.d. "*overblocking*", cioè sul possibile oscuramento di contenuti leciti, volto a minimizzare il rischio di incorrere in responsabilità. Per meglio comprendere le preoccupazioni alla base di queste obiezioni, possono riportarsi le considerazioni di E. Rosati - G. Sartor, Social networks *e responsabilità del* provider, cit., 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». Ampie considerazioni critiche in merito ai rischi di una eccessiva limitazione della libertà di manifestazione del pensiero si trovano anche in G. Nolte, *Hate-Speech, Fake-News*, cit., 557 ss.

[54] In proposito, per tutti, S. Müller-Franken, *Netzwerkdurchsetzungsgesetz*, cit., 5 ss.

[55] *Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online*, art. 1.

[56] A. Lang, *Netzwerkdurchsetzungsgesetz und Meinungsfreiheit. Zur Regulierung privater Internet-Intermediäre bei der Bekämpfung von Hassrede*, in *Archiv des Öffentlichen Recht*, 2, 2018, 227 ss., secondo cui la NetzDG realizza un bilanciamento ragionevole fra l'esigenza di assicurare la libertà d'espressione e quella di

ziario, la legge si limiterebbe a recepire un sistema oramai radicato nel mondo delle reti sociali, all'interno delle quali sono già da tempo operativi meccanismi di monitoraggio e rimozione dei contenuti pubblicati dagli utenti[57]; oltretutto, nel procedere in questa direzione, la NetzDG si sarebbe preoccupata di assicurare l'intervento dello Stato, prevedendo l'istituzione di un'apposita autorità indipendente chiamata a dirimere i casi più controversi.

Tali osservazioni sono indubbiamente ragionevoli. Vero ciò, va peraltro riconosciuto che la questione del ruolo dei *provider* nella individuazione della liceità delle comunicazioni "non manifestamente antigiuridiche" e in specie di quelle afferenti all'area della pubblica informazione chiama in causa problemi estremamente delicati di tutela dell'ordinamento democratico. Data la complessità della materia, a proposito della quale si registra una notevole diversità di opinioni anche presso la nostra letteratura costituzionale [58], è opportuno astenerci dal prendere una posizione sul punto. Volendo nondimeno stilare un bilancio conclusivo, si può affermare che la NetzDG sembra in grado di assicurare una tutela più effettiva dei diritti degli utenti della rete; quantomeno con riferimento alle ipotesi di manifesta antigiuridicità del contenuto, essa configura dunque un modello di disciplina meritevole di essere preso in considerazione anche nel nostro paese[59].

7. Cenni al fenomeno del *dark web* e le sue possibili implicazioni in campo penale

Prima di svolgere alcune riflessioni conclusive, per completare la nostra analisi intorno alla responsabilità dei *provider* sembra utile aprire una breve parentesi relativa al fenomeno del c.d. *dark web*. Invero, l'affermazione del *Web 2.0* sembra avere avuto come conseguenza collaterale l'espansione di quest'area della rete: l'avversione nei confronti del modello economico-sociale delle grandi piattaforme di *social networking*, unito all'insofferenza verso le relative *policy* in tema di trattamento dei dati personali, ha spinto molti utenti ad abbandonare il lato più "superficiale" del *web*[60]. A ciò si aggiunge che, al

tutelare i beni giuridici eventualmente aggrediti nella rete.

57 A. Lang, *Netzwerkdurchsetzungsgesetz*, cit., 237 ss.

58 Propone l'introduzione di «Istituzioni specializzate, terze e indipendenti (giudici o autorità indipendenti) che, sulla base di principi predefiniti, intervengano successivamente, su richiesta di parte e in tempi rapidi, per far rimuovere dalla rete quei contenuti che sono palesemente falsi o llegali o lesivi dei diritti fondamentali e della dignità umana» G. Pitruzzella, *La libetà di informazione*, cit., 26; decisamente critico nei riguardi dell'idea di istituire autorità indipendenti competenti ad accertare la veridicità delle informazioni diffuse nelle reti sociali, invece, N. Zanon, Fake-news *e diffusione dei* social media*: abbiamo bisogno di un'"Autorità Pubblica della Verità"?*, in *questa Rivista*, 2, 2018, 13 ss.

59 Ritiene che la NetzDG sia in grado di funzionare con riferimento ai reati d'odio e a fattispecie come la pornografia minorile, meglio di quanto non possa fare a proposito delle *fake news* K. N. Peifer, *Fake News und Providerhaftung*, cit., 811.

60 Così sostanzialmente R. Gehl, *Power/freedom on the dark web: a digital ethnography of the dark Web social Network*, in *New media & society*, 18, 2016, 3 ss. Sul punto vd. anche il *reportage* realizzato da C. Frediani, Deep web. *La rete oltre Google. Personaggi, storie, luoghi dell'*internet profonda, Genova, 2014, 56. L'Autrice intervista gli amministratori di alcune piattaforme attive nel *deep web*; fra le varie testimonianze, si segnala quella riportata nelle pp. 55-56, ove l'intervistato afferma: «È come tornare a prima dell'*internet* per idioti.

fine di contrastare i traffici illegali situati nel *dark web*, in Germania sono state avanzate due proposte di legge incentrate sulla incriminazione dei gestori delle piattaforme che operano in questa parte della rete; anche sotto il profilo politico-criminale, il tema appare dunque collegato all'oggetto delle nostre riflessioni.

In via preliminare sono opportune alcune informazioni tecniche relative al fenomeno di cui parliamo. Con l'espressione *dark web* s'intende usualmente indicare il complesso di siti presenti nel *deep web*, che sono utilizzati per la realizzazione di attività criminali; a sua volta il *deep web* corrisponde alla parte di *internet* che non può essere raggiunta con i comuni motori di ricerca, bensì tramite *browser* – il più famoso dei quali è TOR ("*The Onion Router*") – che assicurano il pieno anonimato degli utenti[61]. TOR consente infatti di nascondere l'identità di tutti i soggetti coinvolti nella comunicazione, criptando i relativi indirizzi IP; nella rete TOR non operano inoltre i comuni programmi di indicizzazione, sicché l'unico modo per raggiungere un determinato sito è quello di essere indirizzati dagli utenti che ne conoscono la "collocazione". Poiché, infine, nel *dark web* le operazioni commerciali vengono usualmente svolte con *bitcoin* o altre criptovalute, non è possibile risalire all'identità degli internauti nemmeno ricostruendo i relativi movimenti finanziari[62].

Alla luce delle annotazioni che precedono, non sorprende che il *dark web* costituisca un habitat particolarmente favorevole per la proliferazione di attività criminali, come la vendita di armi o di stupefacenti, lo scambio di materiale pedopornografico o l'offerta di servizi di *hacking*[63]. A titolo esemplificativo, possiamo ricordare il caso di *Silk Road*, sito attivo dal 2011 al 2014 e specializzato nella vendita internazionale di droga[64]; ma anche nel nostro paese sono stati recentemente scoperti mercati illegali che hanno luogo negli ambiti più reconditi della rete[65]. Poiché, peraltro, il fenomeno del *dark web* costituisce un'assoluta novità, difetta ancora una piena consapevolezza delle sue possibili implicazioni in campo penale[66].

[…] Prima della bolla speculativa, del *web 2.0*, dei markettari, dei *social*. Qui non hai la pappa pronta con motori che ti dicono cosa cercare. […] La Rete doveva essere un posto di liberazione per tutti […] ma quell'ideale si è perso».

[61] Per una breve – ma esaustiva – panoramica del fenomeno L. Greco, *Strafbarkeit des Unterhaltens einer Handels- und Diskussionplattform insbesondere im sog. Darknet*, in *Zeitschrift für Internationale Strafrechtsdogmatik*, 9, 2019, 436 ss.; per approfondimenti sul funzionamento tecnico della rete TOR, invece, R. Dingledine-N. Mathewson-P. Syverson, *Tor:_The_Second-Generation_Onion_Router*, 1 ss.

[62] Sul punto M. Bachmann-N. Arslan, *"Darknet"-Handelsplätze für kriminelle Waren und Dienstleistungen: ein Fall für den Strafgesetzgeber?*, in *Neue Zeitschrift für Strafrecht*, 7, 2019, 242.

[63] È necessario rimarcare la complessità della realtà di cui parliamo, all'interno della quale si rinvengono infatti anche *forum* destinati allo scambio di informazioni e al dibattito politico (vd. la letteratura citata nella nt. 61); significativo, sotto questo punto di vista, è il fatto che, in tempi recenti, testate giornalistiche di fama internazionale abbiano scelto di utilizzare il *dark web* per la divulgazione delle proprie notizie: *The New York Times is Now Available as a Tor Onion Service*, 27 ottobre 2017.

[64] Per approfondimenti sulla storia di *Silk Road*, C. Frediani, Deep web, 14 ss.; in proposito vd. anche L. Trautman, *Virtual currencies, Bitcoin & What Now After Liberty Reserve, Silk Road and Mt. Gox?*, in *Richmond Journal of Law and Technology*, 20, 2014, 91 ss.

[65] A conferma di ciò *Armi, droga, documenti falsi: bloccato «Berlusconi market», l'emporio italiano del* dark web, in *Il Sole 24 ore*, 7 novembre 2019.

[66] Nel nostro sistema, l'utilizzo della rete TOR o di altri *browser* equivalenti sembra assumere una specifica rilevanza in sede di commisurazione della pena: l'art. 602-*ter* c. 9 c.p. stabilisce infatti che

Soffermandoci brevemente sul punto, abbiamo già accennato al fatto che in Germania sono stati presentati ben due progetti di legge, i quali prevedono specifiche incriminazioni volte a sanzionare l'organizzazione e gestione di piattaforme dirette all'agevolazione di traffici criminali[67]. Più nel dettaglio, mentre una prima proposta fa riferimento esclusivo all'offerta di servizi all'interno del *dark web* ed è circoscritta ai siti che agevolano la commissione di determinate fattispecie relative alla vendita di merci illegali, il secondo disegno di legge mira invece a sanzionare anche le piattaforme attive nel *surface web* e non contempla limitazioni basate sulla tipologia dei reati oggetto di agevolazione[68].

In entrambi i casi, il fondamento delle proposte consiste nell'asserita difficoltà di punire a titolo di concorso di persone l'amministratore del sito ove si svolgono le attività criminose; con specifico riferimento al *dark web*, si ritiene che l'assoluta impossibilità di risalire all'identità degli internauti e all'oggetto delle relative comunicazioni non consenta di affermare la ricorrenza del dolo di partecipazione in capo a chi gestisce la piattaforma sociale. A questa considerazione si aggiunge inoltre che la stessa creazione di siti in cui l'incontro fra le parti avviene con la massima garanzia dell'anonimato avrebbe come effetto quello di incentivare la commissione di reati; donde l'opportunità di svincolare la punibilità del *provider* dal concorso nella commissione di specifici illeciti[69].

Così ricostruiti i lineamenti essenziali delle proposte, possiamo osservare che la creazione di un'autonoma fattispecie offre indubbi vantaggi sul piano probatorio; a un esame più approfondito, però, non sembra che essa configuri una soluzione convincente. Invero, nei casi di piattaforme come *Silk Road*, specializzate nella vendita di determinate merci illegali, la direzione finalistica delle condotte poste in essere dall'amministratore del sito consente di ritenere integrati i presupposti della responsabilità concorsuale nel reato commesso dagli utenti, essendo irrilevante l'ignoranza degli specifici contenuti delle singole transazioni; ne discende che colui che crea o gestisce una piattaforma di comunicazione diretta allo svolgimento di traffici criminali potrà rispondere come agevolatore delle singole violazioni poste in essere dagli internauti (ad esempio, traffico di sostanze stupefacenti *ex* art. 73 d.p.r. 9 ottobre 1990, n. 309). Come si vede, dun-

le sanzioni previste per i reati in materia di prostituzione e pornografia minorili siano aumentate «in misura non eccedente i due terzi» se i fatti sono «compiuti con l'utilizzo di mezzi atti ad impedire l'identificazione dei dati di accesso alle reti telematiche». È peraltro evidente che i problemi connessi al *dark web* non attengono unicamente al piano della severità della risposta punitiva.

[67] Per una panoramica sul contesto nel quale si inseriscono le due proposte di legge, la cui presentazione è stata incentivata dalla scoperta, successiva all'attentato commesso nel 2016 a Monaco di Baviera, dei legami fra *dark web* e terrorismo internazionale, L. Greco, *Strafbarkeit des Unterhaltens*, cit., 435.

[68] Nel dettaglio, la prima proposta, di iniziativa parlamentare, prevede l'introduzione di un nuovo §126a, volto a sanzionare «colui che offre servizi *internet*, l'accesso o il raggiungimento dei quali avviene mediante particolari misure tecniche di sicurezza e il cui scopo o la cui attività sono diretti a rendere possibile o a rafforzare la commissione di fatti antigiuridici»; individua inoltre la nozione di «fatti antigiuridici» richiamandosi ad alcune fattispecie in tema di vendita di sostanze stupefacenti, medicinali, armi ed esplosivi. Il secondo disegno di legge, invece, presentato dal Ministero degli interni, prende in considerazione la condotta di chi «mette a disposizione di terzi un servizio su *internet* il cui scopo o la cui attività è diretta a consentire, promuovere o agevolare la commissione di atti illeciti». Per un confronto fra le due proposte vd. M.A. Zöller, *Strafbarkeit und Strafverfolgung des Betreibens internetbasierter Handelsplattformen für illegale Waren und Dienstleistungen*, in *Kriminalpolitische Zeitschrift*, 5, 2019, 277 ss.

[69] BR-Drs. 33/19, *Gesetzentwurf*, 4 ss.

que, in relazione a ipotesi come questa non è possibile affermare l'esistenza di lacune di tutela da colmare[70]. Le fattispecie contemplate nei summenzionati progetti di legge potrebbero assolvere invece a una vera e propria funzione di incriminazione nei casi in cui le piattaforme siano prive di una specifica connotazione criminale e nondimeno vengano utilizzate per la realizzazione di illeciti; poiché, però, con riferimento ai siti attivi nel *dark web* trovano applicazione i medesimi principi che governano la responsabilità dei *provider* che operano nella parte visibile della rete, non è possibile svincolare la punibilità dei gestori delle piattaforme dalla consapevole fornitura di un apporto attivo alla realizzazione di un reato[71]. In definitiva, la circostanza che un sito sia raggiungibile esclusivamente tramite TOR o altri programmi di criptazione dei dati, di per sé non giustifica l'applicazione di un diverso regime di responsabilità penale; deve dunque escludersi l'opportunità di fare propri i contenuti dei progetti di legge attualmente in discussione in Germania.

Concludendo, bisogna osservare che il fenomeno del *dark web* porta in primo piano un problema che, sebbene presente anche nella parte più visibile della rete[72], assume qua una portata decisiva: si tratta della estrema difficoltà di risalire all'identità dei responsabili delle singole violazioni[73]. A ben guardare, infatti, l'ineffettività della tutela penale non dipende tanto dall'esistenza di lacune sul piano del diritto sostanziale, bensì dalla mancanza di appropriati strumenti di indagine[74]. È chiaro, peraltro, che l'approfondimento di quest'ultimo tema comporterebbe una deviazione eccessiva dall'oggetto delle nostre riflessioni; pertanto, non resta adesso che chiudere la parentesi relativa al *dark*

---

[70] Così M. Bachmann-N. Arslan, *"Darknet"-Handelsplätze für kriminelle Waren*, 244; più ampiamente L. Greco, *Strafbarkeit des Unterhaltens*, cit., 443 ss. Una conferma di questa osservazione è offerta dai giudizi che hanno interessato i gestori delle piattaforme attive nel *dark web*, i quali si sono conclusi tutti con la pronuncia di sentenze di condanna (addirittura all'ergastolo, per il giovane creatore del sito *Silk Road*: *Ergastolo per il fondatore di* Silk Road*, il mercato nero del* web, in *la Repubblica*, 30 maggio 2015).

[71] Sul punto L. Greco, *Strafbarkeit des Unterhaltens*, cit., 440, il quale efficacemente nota: «offrire un'infrastruttura, nella quale acquirenti e venditori esercitano i loro commerci, non basta perché si possa parlare di complicità. Altrimenti anche il gestore di un club nel quale notoriamente si spaccia droga o di una stazione dove si esercita la prostituzione dovrebbe rispondere come concorrente».

[72] Il tema è troppo ampio per poter essere affrontato in questa sede. Sul punto ci limitiamo a osservare che alle criticità che generalmente affliggono la prova digitale (in proposito, per tutti, G. Di Paolo, *Prova informatica (diritto processuale penale)*, in *Enc. dir.*, Annali VI, 2013, 737 ss.), si aggiungono quelle derivanti dalla peculiare conformazione del mercato delle reti sociali: dal momento che i *server* dei grandi *provider* sono generalmente situati all'estero, il mezzo per ottenere i dati ivi contenuti consiste nella rogatoria internazionale; senonché il buon esito di questa procedura è condizionato dalla legislazione dello Stato in cui si trova il soggetto raggiunto dalla richiesta di informazioni e dal suo atteggiamento più o meno collaborativo. Sul punto e più in generale sulle indagini nell'ambito dei *social network*, C. Conti-M. Torre, *Spionaggio informatico nell'ambito dei* social network, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2014, 415 ss.

[73] Ad oggi, il modo più efficace per penetrare all'interno del *dark web* consiste nello svolgimento di indagini sotto copertura, a cui si aggiunge lo sfruttamento dei dati postali per localizzare i destinatari delle merci acquistate nei mercati illegali. Sul punto M. Bachmann-N. Arslan, *"Darknet"-Handelsplätze für kriminelle Waren*, cit., 244 s.; un resoconto delle indagini svolte dalla polizia americana nel caso *Silk Road* si trova invece in C. Frediani, Deep web, cit., 20 ss.

[74] Considerazioni analoghe in M. Bachmann-N. Arslan, *"Darknet"-Handelsplätze für kriminelle Waren*, cit., 246, secondo i quali le «parole-chiave» sono «personale specializzato, migliori attrezzature tecniche, formazione continua, cooperazione più forte a livello internazionale»; conf. M. A. Zöller, *Strafbarkeit und Strafverfolgung*, cit., 281.

web e passare ad abbozzare alcune riflessioni conclusive intorno al ruolo dei *provider* nell'ambito del *Web 2.0*.

8. Considerazioni conclusive

Volendo tracciare un bilancio conclusivo, bisogna anzitutto sottolineare che l'analisi svolta ha confermato il progressivo superamento dell'assetto normativo definito nei primi anni duemila: come efficacemente affermato da Rodotà, risulta oramai radicata l'idea secondo cui «il ricorso all'algoritmo non può divenire una forma di deresponsabilizzazione dei soggetti che lo adoperano»[75].

Più nel dettaglio, l'indagine ha consentito di fare luce sul cedimento nel nostro sistema del principio secondo cui l'*host provider* è tenuto a rimuovere le informazioni illecite solo in seguito alla comunicazione delle autorità competenti (art. 16 d. lgs. 70/2003)[76]; si è invero visto che la giurisprudenza civile e quella penale convergono nell'affermare la responsabilità del fornitore di servizi nella rete anche nei casi in cui ricorre la sola segnalazione del privato. Le ragioni alla base di questi orientamenti sono state illustrate: da un lato, l'enorme grado di diffusione della tecnologia digitale comporta che, a fronte della commissione di un illecito, sia essenziale un intervento tempestivo di rimozione dei materiali antigiuridici caricati nel *web*; dall'altro, la conformazione delle reti sociali, caratterizzate dallo sfruttamento economico dei contenuti prodotti dagli utenti, giustifica l'assegnazione in capo ad esse di più penetranti doveri di attivazione.

Al contempo, però, abbiamo osservato che una simile situazione rende imprescindibile un intervento del legislatore; a tacer d'altro, una volta che si riconosca la necessità di superare l'attuale disciplina, bisogna affrontare alcune importanti questioni. In primo luogo, infatti, occorre verificare se risulti ancora funzionale il tradizionale modello di imputazione incentrato sul paradigma partecipativo. Invero, la punibilità a titolo di concorso di persone deve fare i conti con la necessaria ricorrenza in capo al fornitore di servizi nella rete di requisiti di carattere soggettivo, il cui accertamento raramente è possibile nel caso dei grandi *provider* che operano in contesti essenzialmente legali; alla luce di tale considerazione, la soluzione, accolta dal legislatore tedesco, di fondare la responsabilità degli ISP sul mancato adempimento di obblighi strutturali aventi ad oggetto la predisposizione di procedure efficienti di segnalazione e rimozione dei contenuti illeciti pubblicati dagli utenti appare un'opzione tutt'altro che irragionevole.

Un secondo interrogativo riguarda la possibilità di una diversificazione della disciplina basata sulle finalità perseguite dalle singole piattaforme e sulle relative disponibilità economico-finanziarie[77]. Infine, bisogna stabilire se rimettere interamente al gestore

[75] S. Rodotà, *Il diritto di avere diritti*, Roma-Bari, 2012, 403.

[76] Si è già accennato al fatto che tale previsione riflette una scelta del legislatore nazionale, limitandosi l'art. 14, c. 1, lett. *b)* della direttiva 2000/31/CE a richiedere la conoscenza da parte del *provider* della illiceità delle informazioni; sul punto *retro*, nt. 17.

[77] Come visto, tale è stata la scelta del legislatore tedesco. Sottolinea la necessità di distinguere "piccoli" e "grandi *provider*" F. Di Ciommo, *Oltre la direttiva 2000/31/Ce, o forse no. La responsabilità dei* provider *di* Internet *nell'incerta giurisprudenza europea*, in *Foro it.*, 1, 2019, 2072; invece, sulla possibilità di operare «differenziazioni a seconda che l'attività sia svolta o no a fini di lucro» vd., in termini dubitativi, S.

della rete la valutazione relativa alla liceità dei contenuti oggetto di segnalazione ovvero adottare l'impostazione accolta dal legislatore tedesco, che come visto ha stabilito l'intervento di un'autorità indipendente per la soluzione dei casi più difficili[78].

Ciò precisato, due ulteriori considerazioni sono necessarie. La prima concerne il ruolo sussidiario della responsabilità del fornitore di servizi nella rete: bisogna infatti evidenziare che l'unico modo per assicurare l'effettività della tutela penale consiste nella individuazione e punizione dell'autore principale del reato commesso nel *web*. Sotto questo profilo, il tema della punibilità del *provider* appare collegato a quello relativo ai poteri dell'autorità giudiziaria e si manifesta l'importanza di una riflessione aggiornata sugli strumenti a disposizione per il contrasto ai reati commessi su *internet*.

La seconda considerazione attiene invece alla necessità di un ripensamento della disciplina relativa ai doveri degli ISP anche in chiave eurounitaria. Se la strategia fino ad ora seguita, di aumentare i doveri dei *provider* in funzione del contrasto a specifici fenomeni illeciti, presenta un'indubbia razionalità politico-criminale, va nondimeno ribadito che la direttiva 2000/31/CE è diventata oramai incapace di regolare il mercato digitale; il riconoscimento della sua obsolescenza deve costituire il primo passo verso un rinnovamento della disciplina, al fine di assicurare la tutela dei diritti fondamentali degli utenti della rete e – con specifico riferimento al "salto in avanti" compiuto dal legislatore tedesco – di salvaguardare le esigenze di certezza e di armonizzazione del diritto all'interno dell'Unione.

Seminara, Internet, cit., 604.

[78] In questo senso vd. gli artt. 14 s. della Raccomandazione del 1° marzo 2018.