L'ATTUALE RUOLO DEL PROVIDER NELLA SOCIETA' DIGITALE: MODELLI DI RESPONSABILITA' PENALE

di Gaia Fiorinelli
(Assegnista di ricerca- Scuola Superiore Sant'Anna, Pisa)

SOMMARIO: 1. Premessa. 2. Lo "stato dell'arte" della responsabilità penale del *provider*. – 3. La (nuova) disciplina europea per la *platform economy*. – 4. La posizione del *provider* in alcuni ordinamenti nazionali: ricerca di traiettorie comuni. – 5. Nuovi modelli di responsabilità (penale) per gli attori della rivoluzione digitale – 5.1. *Business* – 5.2. *Rete*. – 5.3. *Infrastruttura*. – 6. Conclusioni.

1. Lo studio delle intersezioni tra evoluzione tecnologica e diritto (penale) costituisce ormai una costante nella riflessione giuridica contemporanea[1]: la ragione di tale interesse – mai sopito e anzi sempre crescente nell'attuale era della c.d. "rivoluzione digitale" [2] – può immediatamente cogliersi, in termini volutamente generali, sol che si pensi alla presenza sempre più pervasiva della tecnologia nei più disparati settori della vita economica e sociale; un fenomeno, quest'ultimo, di proporzioni tali da aver talora imposto anche alla scienza penalistica il superamento di «vecchi modelli d'intervento giuridico» per l'elaborazione di un «nuovo diritto penale» adeguato a rispondere alle inedite questioni poste dalla «civiltà tecnologica»[3].

Un ambito paradigmatico di tale intersezione è indubbiamente rappresentato dal c.d. «diritto penale dell'informatica»[4], alludendo con ciò alla congerie di disposizioni introdotte nell'ordinamento in conseguenza del percepito «svilupparsi di una "nuova" forma di criminalità strettamente connessa all'uso degli elaboratori elettronici» [5]:

[1] In termini generali, sui rapporti tra tecnologia e diritto, nell'ambito di una letteratura sterminata, si possono richiamare, per una prospettiva metodologica, A. Cockfield, *Towards a Law and Technology Theory*, in *MLJ* 2007, 30, 3, 383 ss.; W. Hoffmann-Riem, *Digitale Disruption und Transformation. Herausforderungen für Recht und Rechtswissenschaft*, in *Digitale Disruption und Recht*, a cura di M. Eifert, Baden Baden 2020, 143 ss. Sulle intersezioni tra l'evoluzione tecnologica e il concetto di *responsabilità*, cfr. essenzialmente H. Jonas, *Il principio responsabilità. Un'etica per la civiltà tecnologica* (*Das Prinzip Verantwortung: Versuch einer Ethik für die technologische Zivilisation*), trad. it., Torino 2009, ma anche P. T. Durbin (a cura di), *Technology and responsibility*, Dordercht 1987.

[2] Per cui cfr., *ex multis*, L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano 2017.

[3] Cfr. in questi termini F. Stella, *Giustizia e modernità. La protezione dell'innocente e la tutela delle vittime*[2], Milano 2002, 516.

[4] Per cui cfr. essenzialmente L. Picotti, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in *Cybercrime*, diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano 2019, 33 ss.

[5] Al riguardo è indicativo rinviare a F. Mucciarelli, *Computer (disciplina giuridica del) nel diritto penale*, in

com'è noto, infatti, il legislatore italiano è intervenuto in maniera organica nell'ambito della criminalità informatica con la l. 23.12.1993 n. 547[6] e poi con la successiva l. 18.3.2008 n. 48[7], introducendo nuove fattispecie di reato per far fronte a quelle «nuove forme di aggressione» che, pur rivolgendosi «ai beni giuridici (patrimonio, fede pubblica, eccetera) già oggetto di tutela nelle diverse parti del corpo del codice»[8], risultavano tuttavia caratterizzate dall'utilizzo di un peculiare *mezzo informatico*, ovvero da un inedito *oggetto materiale informatico*.

Con la successiva evoluzione tecnologica dal *computer* al *web* – ovverosia, dalla informatizzazione di singoli apparati all'interconnessione di questi in un'unica rete – la riflessione penalistica ha dovuto fronteggiare ulteriori e nuove esigenze di assestamento: ciò che si è tradotto, ad esempio, nell'introduzione di un'apposita disciplina per il caso in cui determinati delitti fossero commessi «mediante l'utilizzo della rete internet» [9], ovvero nell'interpretazione dinamica da parte della giurisprudenza delle nozioni di «luogo pubblico o aperto al pubblico»[10] o di «mezzo di pubblicità»[11].

Soprattutto, con l'avvento di internet si è dovuto prendere atto dell'irruzione sulla scena di un nuovo *attore*, l'*internet service provider*, ovverosia il soggetto la cui attività (imprenditoriale) consiste nella fornitura di servizi internet e che risulta perciò (potenziale, quanto spesso unico) titolare di poteri di controllo e di intervento su ciò che accade *online* [12]. In tale direzione, dunque, tanto la dottrina quanto la

DigDPen, II, 1988, 373 ss.: l'A. analizza le molteplici «tipologie dei *computer crimes*», operandone un'articolata classificazione nell'ambito del panorama legislativo precedente rispetto all'introduzione dei primi reati informatici con la l. 547/1993, per poi constatare che «dar forma e contenuto a simili esigenze di tutela è cosa senz'altro non agevole».

[6] Rubricata «*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*».

[7] Rubricata «*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*».

[8] Cfr. in questi termini la *Relazione del Disegno di legge* n. 2773, «Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica» (XI Legislatura, divenuto Legge 23.12.1993, n. 547), in www.penale.it, nonché C. Pecorella, *Il diritto penale dell'informatica*, Padova 2006.

[9] Si può citare, ad esempio, la dicitura di cui all'art. 600-*quater* Cp, ovvero all'art. 609-*undecies* Cp.

[10] Si allude alla qualificazione giurisprudenziale del *social network* quale «agorà virtuale» o «piazza immateriale», ai fini dell'applicazione dell'art. 660 Cp, per cui *cfr.* Cass. 11.7.2014 n. 37596, in *DPP* 2014, 10, 1175 ss. Cfr. in proposito G. Checcacci, *Facebook come un luogo pubblico: un caso di "analogia digitale" in malam partem*, in *Crim* 2014, 503 ss.

[11] Cfr. ad es. Cass. 10.12.2021 n.10762, in *GD* 2022, 17, che stabilisce che la «diffusione di un messaggio diffamatorio attraverso l'uso di una bacheca "*Facebook*" integra un'ipotesi di diffamazione aggravata ai sensi dell'art. 595 Cp, comma 3, sotto il profilo dell'offesa arrecata "con qualsiasi altro mezzo di pubblicità" diverso dalla stampa, poiché la condotta in tal modo realizzata è potenzialmente capace di raggiungere un numero indeterminato, o comunque quantitativamente apprezzabile, di persone».

[12] In tal senso D. S. Wall, *Crime, Security, and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and its Implications for Regulation and Policing*, in *The Oxford Handbook of Law, Regulation and Technology*, a cura di R. Brownsword, E. Scotford, K. Yeung, Oxford 2016, 1092 ss., individua per l'appunto negli attori privati della rete i «*capable guardians*». In generale, cfr. U. Sieber, *Criminal Liability for the Transfer of Data in International Networks. New Challenges for the Internet. Part I,* in *Comp. Law & Sec. Report,* 1997, 13, 3, 151 ss.; Id., *Criminal Liability for the Transfer of Data in International Networks. New Challenges for the*

giurisprudenza si sono interrogate sulla configurabilità in capo al *provider* di profili di responsabilità penale per gli illeciti commessi dagli utenti avvalendosi delle infrastrutture e delle piattaforme di condivisione che il *provider* stesso gestisce e rende disponibili, così ritenendolo (od istituendolo) *garante* della "legalità" in rete.

Tale questione teorica – la cui (avvertita) urgenza pratica è dipesa anche dalle difficoltà di accertamento e di *enforcement* sovente incontrate dalle autorità pubbliche, là dove si trattasse di perseguire un reato realizzato *online*[13] – è stata oggetto nel ristretto giro di qualche anno di una copiosa riflessione dottrinale e di alcune pronunce giurisprudenziali[14]. Nondimeno, essa parrebbe ora aver perso l'iniziale centralità, tanto che persino in occasione della recente introduzione di fattispecie penali per reprimere fenomeni che hanno tipicamente luogo *online* (si pensi, ad esempio, all'art. 612-*ter* Cp)[15], la figura del *provider* è rimasta del tutto in ombra.

Ebbene, il presente contributo muove invece dalla premessa che la riflessione sulla responsabilità del *provider* (da intendersi non soltanto come il fornitore di servizi internet, ma anche e soprattutto come il fornitore di servizi digitali *online*[16]) costituisca un tema di estrema attualità, non soltanto perché si tratta di una figura centrale nel paradigma tecno-economico della c.d. «società dell'informazione»[17], oramai da riguardare come un «qualsiasi altro settore industriale maturo»[18], ma anche perché, com'è stato osservato, «molto recentemente il progresso e il benessere dell'umanità hanno iniziato a essere, non soltanto *collegati* a, ma soprattutto *dipendenti* dall'efficace ed efficiente gestione»[19] dei servizi informatici e digitali, così ampliandosi anche le possibili proiezioni offensive dei reati realizzati *online*.

Dopo una preliminare ricognizione dello "stato dell'arte" sulla responsabilità del *provider* (cui è dedicato il par. 2), la riflessione si concentrerà sulla più recente disciplina degli obblighi e delle responsabilità dei fornitori di servizi digitali e delle c.d. "piattaforme" elaborata in ambito euro-unitario (par. 3) e in alcuni altri ordinamenti nazionali (par. 4), sul presupposto che una riflessione *attuale* sul ruolo del *provider*

Internet. Part V: Causation and Summary, in *Comp. Law & Sec. Report,* 1998, 14, 1, 22 ss.; T. Gillespie, *Custodians of the internet. Platforms, content moderation, and the hidden decisions that shape social media*, New Haven 2018.

[13] In ordine alla sussistenza di un tale rapporto di causa-effetto cfr. ad es. C. Pecorella, *Il diritto penale dell'informatica*, cit., 34.

[14] Per cui v. più ampiamente *infra*, par. 2.

[15] Per cui cfr. ad es. N. Amore, *La tutela penale della riservatezza sessuale nella società digitale. Contesto e contenuto del nuovo cybercrime disciplinato dall'art. 612-ter c.p.*, in www.lalegislazionepenale.eu, 20.1.2020.

[16] Cfr. C. Klein, *Online Service Providing — Challenges in the Mass Medium Internet*, in *Media Management*, a cura di A. Vizjak, M. Ringlstetter, Berlin-Heidelberg 2003, 83 ss., che evidenziava l'evoluzione «*from Internet Service Provider to Online Service Provider*», atteso che i primi si limitavano a fornire *tecnicamente* l'accesso a internet, mentre i secondi hanno iniziato ad aggiungere anche l'autonoma offerta di contenuti e servizi agli utenti.

[17] In questi termini cfr. C. Freeman, *Preface to Part II*, in *Technical Change and Economic Theory*, a cura di C. Freeman, R. Nelson, G. Silverberg, L. Soete, London-New York 1988, 10.

[18] Cfr. Clusit, *Rapporto sulla sicurezza ICT in Italia*, 2019, su www.clusit.it, ottobre 2019, 17.

[19] L. Floridi, *op. cit.*, 3.

non possa prescindere da un preliminare "aggiornamento" della stessa nozione presa a riferimento, al fine di mettere meglio a fuoco gli attuali protagonisti della c.d. *platform economy*[20]*;* per poi, infine, tirare le fila dell'analisi, delineando alcuni possibili modelli di responsabilità (penale) per i nuovi attori della rivoluzione digitale (par. 5).

2. A partire da tali premesse, è anzitutto necessario verificare come, *de iure condito*, sia stata risolta nell'ordinamento interno la questione relativa alla possibile attribuzione ai fornitori di servizi digitali di responsabilità penali, in forma attiva od omissiva, per fatti di reato *da altri* realizzati su internet[21].

2.1. Com'è noto, in assenza di un'apposita disciplina che prevedesse un «generalizzato obbligo di controllo preventivo da parte dei fornitori di accesso e servizi di rete»[22], i primi interpreti avevano ipotizzato il possibile coinvolgimento del *provider* negli illeciti commessi dagli utenti secondo due direttrici alternative: per un verso, a titolo di concorso secondo il modello generale dell'art. 110 Cp, individuando proprio nel «collegamento in rete» e nella messa a disposizione di *software* e strumenti per la condivisione di contenuti un rilevante contributo concorsuale, di natura causale o agevolatrice rispetto a eventuali condotte illecite di comunicazione, divulgazione o diffusione realizzate dagli utenti; per altro verso, a titolo di omesso impedimento del reato altrui ai sensi dell'art. 40 cpv Cp, facendo perno, ad esempio, sulle posizioni di garanzia previste dalla legge in materia di tutela dei dati personali e così assumendo che sul *provider* incombesse un obbligo di "controllo" sulla fonte di pericolo rappresentata «dall'esercizio di attività di comunicazione e diffusione di dati ed informazioni»[23]. Il tutto a condizione, beninteso, che il *provider* si fosse in entrambi i casi concretamente rappresentato il fatto illecito dell'utente.

Ancora, il tema della responsabilità del *provider* era stato da altri declinato ricorrendo a una sorta di associazione figurativa, ravvisando cioè nel ruolo dei fornitori di servizi internet le "sembianze" del direttore di periodico e così prospettando l'applicazione della disciplina prevista dall'art. 57 Cp[24]; una soluzione che, tuttavia, si

[20] Per una panoramica generale, cfr. ad es. M. Staglianò, *Gigacapitalisti*, Torino 2022.

[21] Cfr. ad es. S. Seminara, *La responsabilità penale degli operatori su* internet, in *DInf* 1998, 4-5, 745 ss.., e in part. 747, ove l'A. sottolinea come sia parso sin da subito evidente che, rispetto a condotte formulate nei termini di "*chi distribuisce, divulga, diffonde, trasmette o cede a terzi*" contenuti illeciti, le relative disposizioni penali potessero almeno astrattamente applicarsi anche ai *provider*.

[22] Cfr. L. Picotti, *La responsabilità penale dei* service-providers *in Italia*, in *DPP* 1999, 501 ss.

[23] Cfr. ancora per tali prospettive L. Picotti, *La responsabilità penale dei* service-providers *in Italia*, cit., 504.

[24] In argomento, *cfr.* L. Picotti, *Fondamento e limiti della responsabilità penale dei* service-providers *in* internet, in *DPP* 1999, 379 ss.; V. Zeno-Zencovich, *La pretesa estensione alla telematica del regime della stampa: note critiche*, in *DInf* 1998, 15 ss.; Id., *I rapporti fra responsabilità civile e responsabilità penale nelle comunicazioni su* internet *(riflessioni preliminari)*, in *DInf* 1999, 1049 ss.; D. R. Johnson, K. A. Marks, *Mapping Electronic Data Communications Onto Existing Legal Metaphors: Should we let our conscience (and our contracts) be our guide*, in *VLR* 1993, 38, 487 ss., e in part. 491. Anche la Corte di Cassazione tendenzialmente maneggia in modo piuttosto

è sin dall'origine scontrata con il divieto di analogia in materia penale e, comunque, con la sostanziale diversità *tecnica* tra telematica e stampa[25].

Mentre nell'ordinamento interno si tentava poi d'intervenire sul punto con una prima proposta di legge, la quale prevedeva d'inserire un'apposita disposizione che avrebbe testualmente previsto che «il titolare ed il responsabile delle reti telematiche (...) non sono responsabili per quanto da altri comunicato attraverso le reti da essi gestite od ivi immesso, salvo l'obbligo di denunziare ad autorità dotata di potere di polizia giudiziaria ogni e qualsiasi violazione di cui essi siano venuti a conoscenza perpetrata in danno o per mezzo delle reti da essi gestite»[26], è intervenuta a dissolvere dubbi e congetture la Direttiva n. 2000/31/CE («Direttiva sul commercio elettronico»), recepita in Italia con il d. lgs. 9.4.2003, n. 70.

Tale regime distingue tra diverse tipologie di *provider* – in virtù dell'attività in concreto prestata e del grado di ingerenza nell'elaborazione e nella diffusione delle informazioni caricate dagli utenti – e ne differenzia di conseguenza le relative responsabilità[27]. Soprattutto, per quanto ora interessa, completa tale regime generale l'espressa previsione di carattere generale (di cui all'art. 17 d. lgs. 70/2003) secondo la quale il *provider*, a prescindere dalla tipologia di servizio prestato, non è assoggettato a un «obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite», fermi restando gli obblighi di informare «senza indugio» l'autorità competente nel caso di presunte attività o informazioni illecite e di fornire

prudente l'analogia con la stampa, ad es. là dove si è affermato che soltanto al giornale telematico (e non, invece, agli altri mezzi digitali di condivisione di contenuti) sia applicabile la normativa sulla stampa, perché l'unico «*ontologicamente e funzionalmente* assimilabile alla pubblicazione cartacea» (Cass. 23.10.2018 n. 1275, in *CEDCass,* m. 274385-01, che evidenzia come il giornale telematico presenti infatti «una sua organizzazione redazionale e un direttore responsabile (spesso coincidenti con quelli della pubblicazione cartacea)»).

[25] Per cui cfr. V. Zeno-Zencovich, *La pretesa estensione alla telematica del regime della stampa: note critiche*, cit., 15 ss., il quale osserva come per "telematica" debba intendersi la «la trasmissione/ricezione di messaggi in forma elettronica da un soggetto ad un altro soggetto o ad altri soggetti determinati o indeterminati attraverso una rete di telecomunicazioni»: una realtà, dunque, «assolutamente diversa» rispetto alla nozione di stampa.

[26] Si fa riferimento alla Proposta di legge n. 3530, presentata il 4.4.1997 d'iniziativa del deputato Stagno d'Alcontres, recante «*Disciplina delle reti telematiche ad accesso variabile in connessione sovranazionale*», in www.leg13.camera.it. Per una prospettiva critica cfr. ancora S. Seminara, *op. cit.*, 7458, il quale essenzialmente rileva la «singolarità di un dovere di denuncia posto a carico di imprenditori privati».

[27] Nello specifico, si è operata una distinzione tra (i) il prestatore che svolga un'attività di *mere conduit* («semplice trasporto») , il quale non può ritenersi responsabile delle informazioni trasmesse, salvo che egli non sia a qualsiasi titolo intervenuto attivamente nell'elaborazione o nella diffusione delle informazioni medesime; (ii) il prestatore che si occupi di attività di *caching* («memorizzazione temporanea») , il quale non è responsabile delle informazioni memorizzate, a condizione che non ne modifichi il contenuto e ne gestisca le condizioni di accesso e di aggiornamento in conformità alle richieste degli utenti o dell'autorità; infine, (iii) il prestazione di servizi di *hosting* («memorizzazione») , il quale è esonerato da responsabilità, a condizione che non sia effettivamente consapevole dell'illiceità delle informazioni o delle attività memorizzate e che, non appena a conoscenza di tali fatti, agisca immediatamente su comunicazione delle autorità competenti per rimuovere le informazioni o per disabilitarne l'accesso.

alle autorità medesime qualsiasi informazione rilevante per l'identificazione dei soggetti che vi sono coinvolti.

Tale disciplina – dedicata alla responsabilità *civile* del *provider* ma rilevante altresì per delimitarne la posizione di garanzia ai fini dell'applicazione della legge penale – escludeva, dunque, la sussistenza di poteri-doveri di sorveglianza in capo al prestatore di servizi informatici, tenuto a rimuovere i contenuti illeciti e a informare le autorità competenti soltanto in occasione della (incidentale e non doverosa) conoscenza di presunte attività o informazioni illecite, con la conseguente impossibilità di configurare, a partire da tali obblighi, un meccanismo imputativo per omesso impedimento di reati altrui, ai sensi dell'art. 40 cpv. Cp.

La disciplina generale dettata dalla Direttiva 2000/31/CE non esaurisce, peraltro, il novero delle disposizioni o delle impostazioni teoriche che si sono nel tempo stratificate attorno alla figura del *provider* e che sono state classificate in modo particolarmente efficace da quella dottrina che, dieci anni or sono, le ha ricomprese entro i «tre distinti paradigmi idealtipici»[28] del *cittadino*, del *controllore* e del *tutore dell'ordine*.

In particolare, il primo di tali paradigmi si limita all'attribuzione all'*internet service provider* del ruolo di un «comune cittadino» e si connota per l'assenza di doveri di controllo, obblighi di denuncia o oneri di cooperazione con le autorità pubbliche; su tale presupposto, eventuali responsabilità penali per illeciti commessi in rete possono, dunque, essergli ascritte soltanto nelle «ipotesi di autorìa e di concorso commissivo doloso»: predicando, cioè, l'esclusiva applicazione del diritto penale "comune".

Il secondo modello di incriminazione articola, invece, le responsabilità del *provider* secondo il *tipo* del "controllore", nel senso che impone (indirettamente) a quest'ultimo obblighi di censura dei contenuti da altri immessi in rete mediante l'imputazione di un rimprovero per l'omesso impedimento dei reati altrui, secondo lo schema del reato omissivo improprio: un'ipotesi la cui praticabilità è stata, tuttavia, tendenzialmente esclusa, proprio in ragione dell'insussistenza di un obbligo generale di sorveglianza[29].

Infine, il terzo paradigma di responsabilizzazione – corrispondente al modello del "*tutore dell'ordine*" e rinvenibile nel d. lgs. 70/2003, ma anche in altre disposizioni

[28] Cfr. A. Ingrassia, *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine? Risposte attuali e scenari futuribili di una responsabilità penale dei provider nell'ordinamento italiano*, in www.penalecontemporaneo.it, 8.11.2012, nonché in *Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, a cura di L. Luparia, Milano 2012.

[29] Deve al riguardo segnalarsi come il DDL S. 2688, presentato il 7.2.2017, in tema di contrasto alle c.d. *fake news*, all'art. 7 (rubricato «Disposizioni concernenti la responsabilità dei gestori delle piattaforme informatiche in caso di pubblicazione o diffusione di notizie non attendibili o non veritiere») proponesse di stabilire che i «gestori delle piattaforme informatiche» siano «tenuti ad effettuare un costante monitoraggio dei contenuti diffusi attraverso le stesse», dovendo valutarne l'attendibilità e la veridicità, soprattutto qualora gli utenti manifestino un'attenzione «diffusa» e «improvvisa».

settoriali[30] – si distingue per il coinvolgimento soltanto *ex post* del *provider* nelle strategie di repressione degli illeciti commessi su internet, mediante la previsione, ad esempio, di obblighi di denuncia dei reati di cui sia venuto a conoscenza e obblighi di cooperazione con l'autorità nell'individuazione degli autori o nella rimozione o blocco dei contenuti, al cui inadempimento potrà tutt'al più seguire un rimprovero nella forma del reato omissivo proprio[31].

2.2. Così ricostruita la natura e la latitudine degli obblighi effettivamente configurabili in capo all'*internet service provider* nell'ipotesi di attività illecite commesse dagli utenti, deve rilevarsi come alla declinazione delle varie possibili forme del concorso del *provider* nei delitti commessi *online* abbia contribuito in sensibile misura l'interpretazione della giurisprudenza di legittimità: per vero, in assenza di una cornice normativa che facesse ricadere sul fornitore di servizi digitali precisi obblighi *impeditivi* (o meglio, in presenza di una disciplina che espressamente escludeva la sussistenza di generale dovere di sorveglianza o di garanzia), la stessa si è a più riprese misurata con il tentativo di ricavare *aliunde* modelli di incriminazione che fossero riferibili anche al *provider*.

In un primo filone d'indagine si collocano le numerose pronunce nelle quali è stato proprio il paradigma concorsuale di cui all'art. 110 Cp a fondare (o ad escludere) l'ascrizione di responsabilità al *provider* per reati (da altri) realizzati.

Tra le ipotesi più frequenti sottoposte all'attenzione della Corte di Cassazione rientra, ad esempio, il caso del soggetto che gestisca un sito internet contenente raccolte di inserzioni pubblicitarie, tra le quali figurino anche (ma non solo) annunci relativi ad attività di prostituzione[32]: fattispecie nella quale s'impone, per l'appunto, di verificare l'applicabilità anche al gestore del sito delle sanzioni penali previste dall'art. 3 della l. 20.2.1958, n. 75, per le ipotesi di induzione e favoreggiamento della prostituzione. Ebbene, la questione è stata risolta dalla giurisprudenza di legittimità riguardando essenzialmente le *modalità* della condotta del gestore stesso, escludendo la responsabilità di quest'ultimo là dove la sua condotta si fosse estrinsecata in un mero «servizio in favore della persona» e risultando, per converso, pienamente integrata la

[30] A quest'ultimo paradigma delineato sono, ad esempio, riconducibili – come osserva A. Ingrassia, *Il ruolo dell'ISP nel ciberspazio*, cit., 35 – gli «Obblighi per fornitori dei servizi della società dell'informazione resi attraverso reti di comunicazione elettronica» previsti dall'art. 14-*ter* della l. 269/1998, ove si prescrive la necessaria segnalazione al Centro nazionale per il contrasto alla pedopornografia su Internet da parte dei *provider*, «qualora ne vengano a conoscenza», delle imprese o dei soggetti che, a qualunque titolo, diffondono, distribuiscono o fanno commercio, anche in via telematica, di materiale pedopornografico, comunicando altresì ogni informazione rilevante e soggiacendo, nel caso di inadempimento, a una sanzione amministrativa pecuniaria di un importo compreso tra 50 mila e 250 mila euro.

[31] Tale ricostruzione è ripresa (così come tutti i virgolettati) da A. Ingrassia, *Il ruolo dell'ISP nel ciberspazio*, cit., 5 ss.

[32] Per cui cfr. da ultimo Cass. 30.5.2018 n. 39404, su www.online.leggiditalia.it. Ulteriori esempi sono riportati da A. Ingrassia, *Il ruolo dell'ISP nel ciberspazio*, cit., 11 ss.

fattispecie incriminatrice qualora alla pubblicazione degli annunci si fossero collegate ulteriori forme di cooperazione funzionali a rendere più allettante l'offerta e facilitare il contatto con un numero maggiore di utenti[33].

In altre parole, sottesa a tale giurisprudenza vi è l'idea che, mentre risulta pienamente lecita (e, dunque, *estranea* al perimetro del contributo materiale rilevante ai sensi dell'art. 110 Cp) la prestazione da parte del *provider* di servizi «ordinari», che si riducano alla predisposizione di una piattaforma per la condivisione e pubblicazione di annunci, la condotta del fornitore è invece ritenuta idonea a integrare *in forma commissiva* la fattispecie contestata qualora a ciò si accompagni la prestazione a favore degli utenti di servizi «aggiuntivi», «personalizzati», «ulteriori», tali da costituire una forma di «collaborazione organizzativa» tra il *provider* e l'utente, oppure qualora i servizi pubblicitari siano prestati applicando tariffe dissimili da quelle ordinariamente applicate per le restanti attività offerte dal sito[34].

Simili soluzioni giurisprudenziali parrebbero implicitamente richiamare, in tale contesto settoriale, la risalente questione dogmatica inerente alla controversa (individuazione e) rilevanza penale delle c.d. condotte (o azioni) «neutrali»[35]: vale a dire, di quelle condotte che, pur risultando «causalmente efficienti rispetto alla perpetrazione di un reato da parte di altri», possano al contempo predicarsi «neutrali» in ragione della loro natura di prestazioni professionali tendenzialmente «"standardizzate" o fungibili»[36], la cui riconduzione entro il paradigma concorsuale si tradurrebbe (sia pur indirettamente) nell'elevare il fornitore del servizio a "garante" dell'«evenienza di uso illecito del bene o del servizio ceduti ad opera di un terzo, per finalità criminose»[37].

Un'intuizione, quest'ultima, che troverebbe conferma nella più recente categoria, di elaborazione pretoria, del c.d. «*hosting provider* attivo»[38], congegnata con il preciso

[33] In argomento, cfr. Cass. 18.3.2009 n. 26343, in *CEDCass* 2009; Cass. 12.1.2012 n. 4443, in *CEDCass,* m. 251971; Cass. 29.1.2013 n. 20384, in *CEDCass*, m. 255426; Cass. 21.10.2014 n. 48981, in *CEDCass,* m. 261209.

[34] Cfr. ancora Cass. 30.5.2018 n. 39404, cit. In termini parzialmente sovrapponibili, la giurisprudenza di legittimità ha poi ricondotto entro l'ambito applicativo del delitto di favoreggiamento della prostituzione la condotta del gestore (c.d. «*webmaster*») di un sito internet «finalizzato a favorire l'incontro e la conoscenza tra utilizzatori della rete mediante accesso alle chat ed a servizi di videoconferenza» , la cui «neutralità» risultava esclusa dalla predisposizione di aree dedicate alla visualizzazione di «materiale pornografico immesso in rete in diretta o registrato» e al collegamento diretto tra «intrattenitori» e «utenti», nonché – soprattutto – dalla retribuzione diretta dei singoli intrattenitori da parte del sito, «mediante la corresponsione di una percentuale delle somme ricavate grazie alla loro attività», per cui cfr. Cass. 22.4.2004 n. 25464, in *CEDCass*, m. 228692.

[35] Al riguardo non può che rinviarsi all'analisi di E. Basile, *Consiglio tecnico e responsabilità penale. Il concorso del professionista tramite azioni «neutrali»*, Torino 2018; in part. 83 ss., il quale colloca per l'appunto il tema al crocevia tra «(legittimo) svolgimento di attività professionali e partecipazione punibile».

[36] Cfr. ancora E. Basile, *op. cit.,* 83-84.

[37] Cfr. ancora E. Basile, *op. cit.,* 85.

[38] Ricostruisce l'evoluzione di tale paradigma G. P. Accinni, *Profili di responsabilità penale dell'hosting provider "attivo"*, in www.archiviopenale.it, 23.5.2017, 2. In argomento, v. anche Cass. civ. 19.3.2019 n.7708, in *GI*, 2019, 12, 2604 ss. e n. e 7709, in *CorrGiur* 2020, 2, 177 ss.: «La giurisprudenza recente della Corte di giustizia dell'Unione Europea ha accolto la nozione di "hosting provider attivo", riferita a tutti quei casi che esulano da un'"attività dei

fine di distinguere, all'interno dell'indistinta nozione di *internet service provider*, quei fornitori che non si limitino a un intervento meramente «tecnico, automatico e passivo» (per rammentare il tenore testuale della Direttiva 2000/31), ma anzi rielaborino le informazioni, i dati e i contenuti inseriti dagli utenti, al fine di sfruttarne commercialmente la disponibilità sul proprio sito; così non presentando più quei tratti di *neutralità* e *passività* che ne giustificavano un giudizio di estraneità rispetto alle condotte poste in essere dagli utenti.

Così, ad esempio, dovendo definire la posizione dei gestori della piattaforma *thepiratebay.org*, indagati per il delitto di cui all'art. 171-*ter* l. 22.4.1941 n. 633 in ragione della messa in circolazione nella rete internet di opere protette dal diritto d'autore[39], la Corte di Cassazione ha osservato – limitando l'analisi al solo tema del concorso del *provider* – come il nodo essenziale della questione risieda, per l'appunto, nella *natura* del contributo fornito dal titolare del sito: il quale sarà senz'altro estraneo al reato qualora si limiti a mettere a disposizione degli utenti un protocollo di comunicazione. Al contrario, là dove il titolare del sito effettui «qualcosa di più» – ad esempio, indicizzando le informazioni e i contenuti caricati dagli utenti, così rendendole più facilmente reperibili, anche mediante un motore di ricerca – egli cesserà di «essere un mero "corriere" che organizza il trasporto dei dati», ma avrà anzi posto in essere un contributo concorsuale «che ben può essere inquadrato nella partecipazione imputabile a titolo di concorso di persone ex art. 110 Cp»[40].

Su un primo versante, dunque, la giurisprudenza di legittimità ha in più casi circoscritto l'applicazione delle esenzioni da responsabilità previste dal d. lgs. 70/2003, valorizzando il ruolo talora marcatamente *attivo* dei fornitori di servizi digitali, e in particolare dei gestori di siti *web*, rispetto all'organizzazione dei contenuti caricati dagli utenti.

Sicuramente meno nutrito è, invece, il secondo possibile filone d'indagine, relativo alla responsabilità concorsuale "per omissione" del *provider*: un tema che è stato essenzialmente affrontato nell'ambito della nota vicenda giudiziaria c.d. *Google-Vivi Down*, nella quale si trattava, in particolare, di valutare la configurabilità in capo agli imputati (nella specie, due amministratori delegati e il responsabile *privacy* di *Google Italy s.r.l.*) di un rimprovero a titolo di *omesso impedimento* dei delitti di diffamazione

prestatori di servizi della società dell'informazione (che) sia di ordine meramente tecnico, automatico e passivo, con la conseguenza che detti prestatori non conoscono né controllano le informazioni trasmesse o memorizzate dalle persone alle quali forniscono i loro servizi", mentre "(p)er contro, tali limitazioni di responsabilità non sono applicabili nel caso in cui un prestatore di servizi della società dell'informazione svolga un ruolo attivo».

[39] Cfr. Cass. 29.9.2009, n.49437, in *DPP* 2010, 3, 290 ss.; in argomento, V. Spinosa, *Nella Baia dei Pirati: l'arrembaggio al diritto d'autore su internet*, in *La giustizia penale nella "rete". Le nuove sfide della società dell'informazione nell'epoca di Internet*, a cura di R. Flor, D. Falcinelli, S. Marcolini, Milano 2014, 59 ss.

[40] Cfr. ancora Cass. 29.9.2009, n.49437, cit.

e trattamento illecito di dati personali realizzati da un utente mediante l'*upload* (e, dunque, la pubblicazione) di un video sulla piattaforma *www.video.google.it*[41].

Orbene, con un percorso argomentativo che non ha poi superato il vaglio della Corte d'Appello[42] e, soprattutto, della Corte di Cassazione[43], il Giudice di prime cure aveva ritenuto configurabile il concorso omissivo gli imputati nei delitti realizzati dall'utente, sul presupposto che, pur in assenza di un obbligo di controllo *preventivo* sui dati immessi sulla rete, il proprietario o il gestore di un sito *web* sarebbero purtuttavia responsabili di garantire che il servizio fornito si adegui e rispetti le normative vigenti (nello specifico, le norme in tema di *privacy*).

Peraltro, osservando ad esempio che «non è la scritta sul muro che costituisce reato per il proprietario del muro, ma il suo sfruttamento commerciale può esserlo, in determinati casi ed in presenza di determinate circostanze», il Tribunale di Milano aveva attribuito un particolare rilievo «all'interesse economico» del *provider* nella prestazione del servizio, per il perseguimento del quale gli imputati avrebbero accettato consapevolmente il «rischio concreto di inserimento e divulgazione di dati, anche e soprattutto sensibili, che avrebbero dovuto essere oggetto di particolare tutela»[44]: quello dell'interesse economico del *provider* nell'attività prestata è, allora, un profilo che, seppur mai autonomamente tematizzato, tuttavia traluce frequentemente nell'analisi della giurisprudenza (e che sarà poi più ampiamente sviluppato *infra*, par. 5.1). Ad ogni modo, tale pronuncia rimane sostanzialmente un *unicum* per quanto attiene all'applicazione del paradigma del reato omissivo improprio al fornitore di servizi internet.

In un terzo filone giurisprudenziale si può collocare, infine, un recente orientamento interpretativo, sviluppato dalla giurisprudenza di legittimità che si è pronunciata sulla configurabilità di una responsabilità *concorsuale* in capo al gestore

[41] La ricostruzione precisa della vicenda si ritrova in T. Milano 24.2.2010 n. 1972, su www.dejure.it.

[42] La Corte d'Appello di Milano (cfr. App. Milano 21.12.2012 n. 8611, in www.penalecontemporaneo.it, 4.3.2013) ha assolto gli imputati da tutti i reati loro ascritti, rilevando come l'assenza di una rilevante posizione di garanzia, l'impossibilità di estendere al *provider* il regime di cui all'art. 57 Cp, nonché l'impossibilità di ricostruire in capo al *provider* una posizione di garanzia rispetto al trattamento dei dati coinvolti nel video, per il quale è unicamente responsabile l'*uploader*.

[43] Cass. 17.12.2013 n. 5107, in *FI* 2014, II, 336 ss., con nota di F. Di Ciommo; in *CP* 2014, 2052 ss., con nota di P. Troncone, *Il caso* Google *(e non solo), il trattamento dei dati personali e i controversi requisiti di rilevanza penale del fatto*; in *DInf* 2014, 225 ss., con nota di F. Resta.
Analogamente, in una diversa fattispecie, la Corte di Cassazione ha escluso che possa ad esempio configurarsi in capo al gestore di un sito di incontri un «dovere giuridico di accertamento prodromico alla pubblicazione dell'annuncio», in ordine all'età degli utenti, funzionale alla prevenzione dei reati contro la libertà sessuale dei minorenni; un siffatto dovere, infatti, non è previsto dalla legge, né può ritenersi "volontariamente assunto" da parte del *provider* che, nelle "condizioni di utilizzo" del sito, preveda sanzioni applicabili agli iscritti in caso di mendacio, e ciò soprattutto in considerazione del «carattere eminentemente privato del contesto nel quale le informazioni si offrono» (cfr. Cass. 16.12.2020 n. 9081, reperibile su www.online.leggiditalia.it, che ha per l'appunto escluso la sussistenza di un dovere di «verifica della veridicità di quanto affermato dai partecipanti in sede di registrazione»).

[44] Cfr. ancora T. Milano 24.2.2010 n. 1972, cit.

del sito o del *blog* sul quale siano stati pubblicati contenuti a carattere diffamatorio, qualora questi non li abbia prontamente rimossi all'esito di una segnalazione. In tale contesto, facendo seguito a una prima pronuncia[45], nella cui motivazione non era stato compiutamente esplicitato il fondamento normativo legittimante l'ascrizione di responsabilità al *provider*, la Corte di Cassazione è tornata su tale questione in un caso sostanzialmente analogo[46], soffermandosi con considerazioni di ampio respiro su quello che è ritenuto «il vero problema della responsabilità del *provider*», ovverosia «il caso in cui questo debba rispondere del fatto illecito altrui», posto in essere avvalendosi delle infrastrutture, del server, del sito, dei servizi o delle pagine resi disponibili da detto *provider*.

Orbene, dopo aver rilevato «l'assenza di un obbligo generale di sorveglianza *ex ante*», nonché di un «obbligo di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite», in virtù della Direttiva 2000/31/CE e dal relativo decreto di recepimento d. lgs. 70/2003, la Corte ha tuttavia sottolineato come il regime di responsabilità delineato dalla Direttiva debba intendersi limitato – in forza del *considerando* n. 42 – ai soli casi nei quali il *provider* presti un'attività «di ordine meramente tecnico, automatico e passivo, [...] non conosce(ndo) né controlla(ndo) le informazioni trasmesse o memorizzate»[47], risultando vieppiù «inadeguato alla materia che si prefigge di regolare», specie in considerazione delle più recenti frontiere dell'evoluzione tecnologica di internet.

Di conseguenza, ad avviso della Corte una siffatta esenzione non sarebbe applicabile al *blogger*, ovverosia a colui che metta «a disposizione degli utenti una piattaforma sulla quale poter interagire attraverso la pubblicazione di contenuti e commenti»[48]. Benché, infatti, il *blogger* non possa essere ritenuto responsabile «per tutto quanto scritto sul proprio sito anche da altri soggetti» – ciò che ne amplierebbe indiscriminatamente i doveri di vigilanza –, ritiene tuttavia la Corte, testualmente, che là dove il *blog* sia stato dotato di «filtri nella pubblicazione di contenuti» o di meccanismi alternativi di segnalazione, il gestore sia di conseguenza «tenuto a vigilare ed approvare i commenti prima che questi siano pubblicati», «per evitare conseguenze penali»; soprattutto, questi dovrà «rispondere dei contenuti denigratori pubblicati sul suo diario da terzi quando, presa cognizione della lesività di tali contenuti, li mantenga consapevolmente»[49].

[45] Cfr. Cass. 12.7.2016 n. 54946, in *FI* 2017, II, 251 ss., con nota di F. Di Ciommo; in *CP* 2017, 2781 ss., con nota di R. Carbone, *Responsabilità del* blogger*: parziale* revirement *della Cassazione?*; in *RCivPrev* 2017, 1646 ss., con nota di C. Curreli, *La controversa responsabilità del gestore di un sito* web*, in caso di diffamazione commessa da terzi*.
[46] Cfr. Cass. 8.11.2018 n. 12546, in *GD* 2019, 20, 84 ss.
[47] Cfr. ancora Cass. 8.11.2018 n. 12546, cit.
[48] Cfr. ancora Cass. 8.11.2018 n. 12546, cit.
[49] Cfr. ancora Cass. 8.11.2018 n. 12546, cit.

In altri termini, premesso che la (problematica) *fonte* della responsabilità del *blogger* viene fatta dipendere dall'aver questi (volontariamente) adottato un sistema di *filtro* del contenuti [50], ad avviso della Corte l'omessa attivazione al fine di rimuovere contenuti illeciti pubblicati da terzi si traduce automaticamente nella «consapevole condivisione del contenuto lesivo», e ciò sul presupposto 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» [51]: con l'effetto, dunque, di configurare un ulteriore, quanto problematico modello di responsabilità del *provider* per «omesso impedimento *degli effetti* di un reato altrui» [52].

Tali ultime torsioni dogmatiche – sebbene non condivisibili negli esiti raggiunti – segnalano nondimeno la perdurante attualità del tema delle responsabilità penali degli "attori" della società digitale: non più, come si anticipava, *meri internet service provider*, ma attivi gestori dello spazio virtuale.

3. Come si anticipava, se l'intento del presente lavoro di ricerca è quello di "aggiornare" la riflessione relativa alla figura del *provider*, è in ambito europeo che si registrano le novità più significative in relazione ai modelli di prevenzione dell'uso illecito di tecnologie digitali [53]: in tale contesto si assiste, in effetti, a uno spostamento del "fuoco" dell'intervento regolatorio su paradigmi di stampo preventivo – che si inscrivono nella più ampia strategia elaborata dall'Unione Europea per la disciplina del Mercato Unico Digitale –, i quali risultano di sicura rilevanza anche per la presente indagine.

In particolare, già nella *Comunicazione della Commissione europea* «Le piattaforme online e il mercato unico digitale» [54] si propone – per quanto strettamente inerente all'oggetto della presente ricerca – l'introduzione a livello europeo di obblighi funzionali a «garantire la condotta responsabile delle piattaforme *online*», superando su taluni versanti il regime di responsabilità (limitata) definito nella citata Direttiva

[50] Con il paradossale effetto, dunque, di *dissuadere* gli altri soggetti operanti nel medesimo ambito dall'adozione di un siffatto meccanismo di controllo: invero, trattandosi di valutare gli estremi del concorso (necessariamente doloso) del *blogger* nel delitto (doloso) realizzato dall'utente, il sistema di filtro produce l'effetto di *attualizzare* la conoscenza del *blogger* circa la presenza di contenuti illeciti, mentre dall'omessa adozione di tale sistema di filtraggio non può scaturire alcuna conseguenza (non trattandosi di fattispecie di reato generalmente rilevanti nella forma *colposa*).

[51] Cfr. ancora Cass. 8.11.2018 n. 12546, cit.

[52] Cfr. A. Ingrassia, *Responsabilità penale degli internet service provider: attualità e prospettive,* in *DPP* 2017, 12, 1621 ss., in part, 1625, nonché R. Bartoli, *Brevi considerazioni sulla responsabilità penale dell'Internet Service Provider*, in *DPP* 2013, 5, 600 ss.

[53] Su questo tema cfr. ad es. T. Tropina, C. Callanan, *Self- and Coregulation in Cybercrime, Cybersecurity and National Security*, Berlin 2015.

[54] Cfr. Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato Delle Regioni, *Le piattaforme online e il mercato unico digitale: Opportunità e sfide per l'Europa* (COM(2016) 288 final), in www.eur-lex.europa.eu.

2000/31/CEE. Benché, infatti, le esenzioni ivi previste abbiano agevolato lo sviluppo dei servizi nella società dell'informazione nella fase iniziale della "rivoluzione digitale", la proliferazione di attività e contenuti illegali su internet impone, ad avviso della Commissione, un mutamento del regime di responsabilità del *provider*, quantomeno in relazione ad alcune fenomenologie criminose, ritenute di particolare gravità: tra queste, la «condivisione di video *online* con contenuti nocivi per i minori e istigazioni all'odio»; «l'uso dei contenuti protetti dal diritto d'autore», soprattutto se impiegati illecitamente a fini di profitto; e, infine, le ipotesi di «incitamento al terrorismo, abusi sessuali sui minori e discorsi di incitamento all'odio», contro le quali *tutte* le piattaforme *online* dovrebbero «essere incoraggiate a intervenire direttamente su base volontaria e in modo più efficace, per ridurre l'esposizione a contenuti illeciti o nocivi».

Nella medesima ottica preventiva, anche nella successiva *Raccomandazione*[55] sulle misure per contrastare efficacemente i contenuti illegali *online*, la Commissione europea propone di affiancare ai più tradizionali meccanismi di rimozione fondati sulle segnalazioni degli utenti (Capo II, nn. 5-6) anche l'eventuale adozione da parte dei *provider* di «misure proattive opportune, proporzionate e specifiche in relazione ai contenuti illegali», tra le quali ad esempio «strumenti automatizzati» che rilevino tali medesimi contenuti (Capo II, n. 18).

Così, anche nel quasi contestuale «Codice di condotta per lottare contro le forme illegali di incitamento all'odio online»[56], sottoscritto d'intesa tra la Commissione europea e quattro (tra le più importanti) piattaforme digitali, queste ultime hanno assunto pubblicamente l'impegno – sia pur ai soli fini di contrastare l'incitamento all'odio *online* – di predisporre meccanismi di segnalazione e rimozione dei contenuti illeciti idonei ad assicurare la rapidità dell'intervento (entro 24 ore). Oltretutto, tra gli obiettivi del codice di condotta rientrano altresì la definizione di *best practices* da estendere anche ad altri fornitori di servizi digitali, nonché la predisposizione da parte dei *provider* di programmi di formazione e sensibilizzazione, l'istituzione di meccanismi di cooperazione con le autorità degli Stati membri e la definizione di "codici di comportamento" per gli utenti, che vietino a questi ultimi – anche indipendentemente dalle legislazioni nazionali – la «promozione dell'istigazione alla violenza e a comportamenti improntati all'odio».

Un approccio sostanzialmente analogo si rinviene – per fornire un ulteriore spunto – nel Regolamento europeo 2021/784[57], in vigore dal 7 giugno 2022, specificamente dedicato al contrasto della diffusione di contenuti terroristici *online* e, per l'appunto,

[55] Cfr. Raccomandazione (UE) 2018/334 della Commissione dell'1.3.2018 sulle misure per contrastare efficacemente i contenuti illegali *online*, in www.eur-lex.europa.eu.

[56] Cfr. il Codice di condotta per lottare contro le forme illegali di incitamento all'odio online, in www.ec.europa.eu.

[57] Cfr. Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio del 29.4.2021.

predisposto con l'intento di «garantire il buon funzionamento del mercato unico digitale», «contrastando l'uso improprio dei servizi di *hosting* a fini terroristici», così da rafforzare al contempo la fiducia degli utenti e garantire ai fornitori una maggiore certezza del diritto (cons. 1). Nel testo del Regolamento si afferma espressamente che il contrasto dei contenuti illegali *online* richieda una «combinazione di misure legislative, non legislative e volontarie basate sulla collaborazione tra le autorità e i prestatori di servizi di *hosting*», cui si attribuisce un ruolo essenziale nell'attuale economia (e società) digitale; in particolare, proprio «in considerazione dell'importanza del ruolo che svolgono nonché delle capacità e dei mezzi tecnologici associati ai servizi che forniscono», si afferma nel Regolamento che i *provider* debbano ritenersi titolari di «particolari responsabilità nei confronti della società», per quanto attiene alla «protezione dei loro servizi dall'uso improprio» che potrebbero farne gli utenti (e, nella specie, i terroristi)[58].

Traducendo tali indicazioni di principio in previsioni concrete, il Regolamento 2021/784 non si limita, dunque, a prevedere che i prestatori servizi destinatari di un ordine di rimozione (proveniente dall'autorità competente) debbano adempiervi «entro un'ora»[59], rimuovendo i contenuti terroristici o disabilitando l'accesso, ma aggiunge anche che un prestatore di servizi di *hosting* «esposto a contenuti terroristici» debba adottare «misure specifiche» (la cui individuazione compete al *provider*) per *proteggere* i propri servizi dalla diffusione al pubblico di siffatti contenuti[60]: con ciò segnando l'esplicito ingresso, nella materia che ci occupa, del (familiare) paradigma di prevenzione mediante auto-organizzazione, ora però rivolto a « contrastare la disponibilità di contenuti terroristici nei [...] servizi» forniti e, dunque, alla *protezione* della propria attività da reati commessi da *terzi*.

Un simile paradigma ritorna, a ben vedere, anche nella Direttiva 2018/1808 sui servizi audiovisivi[61] (attuata con d. lgs. 8.11.2021 n. 208) e nella Direttiva 2019/790[62] (attuata con d. lgs. 8.11.2021 n. 177). Senza che, beninteso, in questa sede ci si possa soffermare sul contenuto di dettaglio di entrambi i testi normativi, interessa piuttosto sottolineare, quanto alla *prima*, come sia stata introdotta all'art. 42 d. lgs. 208/2021 la previsione che, fatti salvi gli artt. 14-17 d. lgs. 70/2003, i fornitori di piattaforme per la

[58] Cfr., in particolare, i cons. nn. 3, 4, 5 del Regolamento (UE) 2021/784.
[59] Cfr. art. 3 Regolamento (UE) 2021/784.
[60] Cfr. art. 5 Regolamento (UE) 2021/784, anche per la definizione di prestatore "esposto a contenuti terroristici". Quanto alle misure che il *provider* può adottare, il Regolamento elenca «personale o mezzi tecnici adeguati per individuare e rimuovere rapidamente o disabilitare l'accesso a contenuti terroristici», cui si aggiungono meccanismi di segnalazione, di sensibilizzazione e di moderazione.
[61] Cfr. Direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14.11.2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato.
[62] Cfr. la Direttiva (UE) 2019/790 del Parlamento Europeo e del Consiglio del 17.4.2019 sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE.

condivisione di video debbano adottare misure adeguate a tutelare (a) i minori da contenuti nocivi, anche generati dagli utenti e (b) il pubblico, più in generale, da contenuti, anche generati dagli utenti, che istighino alla violenza o all'odio o (c) la cui diffusione costituisce reato; quanto alla *seconda*, il d. lgs. 70/2003 interviene sulla l. 633/1941 in tema di diritto d'autore, prevedendo che i prestatori di servizi di condivisione di contenuti *online*, quando concedono l'accesso al pubblico a opere protette dal diritto d'autore o ad altri materiali protetti *caricati dai loro utenti*, compiono essi stessi un atto di comunicazione al pubblico o un atto di messa a disposizione del pubblico, che non è coperto dalla limitazione di cui all'art. 16 d. lgs. 70/2003 e per il quale il prestatore è, dunque, responsabile, a meno che non dimostri – in buona sostanza – di aver compiuto «i massimi sforzi», secondo «elevati *standard* di diligenza professionale del settore» per evitarlo e di aver tempestivamente disabilitato l'accesso o rimosso dai propri siti web il contenuto illecito, non appena ricevuta una segnalazione, nonché di aver compiuto i medesimi sforzi «per impedirne il caricamento in futuro» (artt. 102-*sexies* e 102-*septies* l. 633/1941).

Last but not least, a "rivoluzionare" il tema della responsabilità del *provider* è da ultimo intervenuto il *Digital Services Act*, ovverosia il Regolamento UE 2022/2065 del 19.10.2022, relativo al mercato unico dei servizi digitali, che – per quanto ora interessa – modifica anche la direttiva 2000/31. Nello specifico, il Regolamento, nel riconfermare l'assenza di obblighi generali di sorveglianza o di accertamento attivo dei fatti (art. 8) in capo ai prestatori di servizi intermediari e al contempo la possibilità per le autorità nazionali di rivolgere ai *provider* ordini "di contrastare i contenuti illegali" (art. 9) o di "fornire informazioni" (art. 10), introduce nondimeno un regime più rigoroso per i prestatori di servizi di memorizzazione di informazioni, comprese le piattaforme *online* (Capo III, Sez. 2), prevedendo l'obbligo di adottare un meccanismo di *notice and action* per la segnalazione e la tempestiva rimozione dei contenuti illegali (art. 16), ma anche un inedito obbligo di denuncia alle autorità dello Stato membro («qualora venga a conoscenza di informazioni che fanno sospettare che sia stato commesso, si stia commettendo o probabilmente sarà commesso un reato che comporta una minaccia per la vita o la sicurezza di una o più persone», come previsto dall'art. 17). Infine, l'art. 33 del Regolamento demanda alle piattaforme *online* di dimensioni «molto grandi» l'individuazione, l'analisi e la valutazione di eventuali «rischi sistemici nell'Unione derivanti dalla progettazione o dal funzionamento del loro servizio e dei suoi relativi sistemi, compresi i sistemi algoritmici, o dall'uso dei loro servizi» e ricomprende espressamente tra i rischi sistemici rilevanti anche la «diffusione di contenuti illegali tramite i loro servizi», avverso il quale rischio le piattaforme sono tenute ad adottare misure di «attenuazione ragionevoli, proporzionate ed efficaci» (art. 34).

Volendo delineare alcune considerazioni di sintesi, il mutamento pare *copernicano*. Progressivamente s'impongono, infatti, in capo ai *provider* doveri di diligenza e obblighi "cautelari" di prevenzione e gestione del rischio di commissione di illeciti *da parte di terzi*, i quali contribuiscono a modellare un nuovo paradigma di responsabilità[63]: un tempo fondata su una struttura normativa «condizionale» (in quanto vincolata alla sussistenza dei requisiti, positivi e negativi, di cui agli artt. 14 ss. d. lgs. 70/2003), ora invece la responsabilità del *provider* tende verso una forma di prevenzione «organizzativa»[64], sul modello della *self-regulation*, che potrà produrre ripercussioni di tutto rilievo, nella prospettiva che ci occupa, nella misura in cui essa rappresenta la nuova cornice per la costruzione di una (possibile) posizione di garanzia in capo al *provider*.

Deve, del resto, sottolinearsi come una simile evoluzione risulti muoversi in parallelo con il mutamento del baricentro della disciplina, ora non più costituito dal generico prestatore di servizi quanto (nella più recente dizione testuale) dalla «piattaforma»[65], ovverosia l'«impresa» che si avvale della rete per la prestazione dei (più svariati) servizi[66] e che è, dunque, dotata di un inedito (quanto decisivo) potere socioeconomico nella dinamica del mercato europeo[67]. Tale evoluzione segnala, dunque, anche l'opportunità di distinguere, all'interno della generica nozione di *provider*, le diverse categorie di operatori che, in ragione delle dimensioni aziendali, o del *tipo* o del *settore* dell'attività prestata, possono in effetti necessitare di distinti regimi di responsabilità.

4. La particolare prospettiva assunta alla base dell'indagine suggerisce ora di spostare lo sguardo sui più recenti modelli di responsabilità, o di *responsabilizzazione*, del *provider* rinvenibili nel panorama comparatistico: in particolare, si concentrerà l'attenzione (i) sul paradigma della c.d. «autoregolamentazione regolata»[68] introdotto

[63] Cfr. M. L. Montagnani, *A New Liability Regime for Illegal Content in the Digital Single Market Strategy,* in *Oxford Handbook of Online Intermediary Liability*, a cura di G. Frosio, Oxford 2020, 309 ss.
[64] Cfr. ancora M. L. Montagnani, *op. cit.*, 311.
[65] In proposito, cfr. ad es. la ricostruzione di E. Bietti, *A genealogy of Digital Platform Regulation*, in www.ssrn.com, 4.6.2021, e soprattutto l'analisi di J. E. Cohen, *Law for the Platform Economy*, in *UCDLR* 2017, 51, 133 ss.
[66] La Commissione Europea ha definito la piattaforma come «*undertaking operating in two (or multi)-sided markets, which uses the Internet to enable interactions between two or more distinct but interdependent groups of users so as to generate value for at least one of the groups*» (cfr. Commissione europea, *Public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy*, 24.9.2015).
[67] Cfr. per una ricostruzione anche A. Bertolini, F. Episcopo, N. Cherciu, *Liability of Online Platforms*, in www.europarl.europa.eu, 5.2.2021; rimarcano le differenze esistenti nell'ambito dei servizi digitali anche J. M. Balkin, *How to Regulate (and Not Regulate) Social Media*, in *Knight Institute Occasional Paper Series* 2020, 1, nonché T. Gillespie, *op. cit.*, 40 ss., in ordine alla distinzione tra la nozione di *piattaforma* e quella di *intermediario*.
[68] Cfr. J. Rinceanu, *Verso una forma di polizia privata nello spazio digitale? L'inedito ruolo dei* provider *nella disciplina tedesca dei* social network, in www.sistemapenale.it, 11.3.2021; v. anche V. Claussen, *Fighting hate*

nell'ordinamento tedesco; (ii) sul modello analogo adottato nell'ordinamento francese; infine, (iii) sulle proposte di riforma della Sect. 230 CDA (in tema di responsabilità del *provider*) più di recente avanzate nell'ordinamento statunitense[69]. Tali disposizioni non hanno evidentemente, a differenza di quelle analizzate nel par. 3, una diretta rilevanza nell'ordinamento interno, ma forniscono nondimeno utili spunti nella prospettiva che ora ci occupa.

4.1. Un primo modello di intervento nel settore oggetto del presente contributo può rinvenirsi, come si anticipava, nel *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG)*, ispirato dall'intento (testualmente indicato nella rubrica) di migliorare l'applicazione della legge sui *social network*[70]: uno scopo che, a ben vedere, delimita anche l'ambito applicativo delle relative disposizioni, selezionando all'interno dell'ampia nozione di *provider* i soli fornitori digitali che gestiscono piattaforme di condivisione di contenuti tra gli utenti.

Entro tale cornice, e proprio al fine di superare i problemi di applicazione ed *enforcement* della legge sul *web*, nonché di impedire con maggiore effettività la diffusione su internet di contenuti illeciti, il legislatore tedesco ha appunto ritenuto che il "perno" sul quale debba far leva il potere statale sia lo stesso *provider*, al quale – in considerazione della funzione svolta – sono imposti obblighi di *compliance*, presidiati da sanzioni e funzionali a coinvolgere coattivamente i singoli fornitori nell'identificazione e nella rimozione dei contenuti illeciti dalla rete. L'applicazione di un simile regime è, tuttavia, condizionata al duplice presupposto che (i) il fornitore di servizi digitali gestisca a scopo di lucro una piattaforma su internet, destinata a consentire agli utenti di condividere e pubblicare contenuti (c.d. *social network*) e che (ii) lo stesso abbia almeno due milioni di utenti registrati in Germania; ne sono, invece, escluse tanto le piattaforme di stampo giornalistico-editoriale – nelle quali il fornitore è *direttamente* responsabile dei contenuti veicolati –, quanto le piattaforme destinate alla comunicazione individuale o alla diffusione di contenuti specifici.

In estrema sintesi, secondo il modello appena delineato sul fornitore ricade l'obbligo di adottare una procedura efficace e trasparente per la gestione delle segnalazioni relative a contenuti illegali, le cui caratteristiche sono in parte *direttamente* stabilite dallo stesso *NetzDG*, che ad esempio circoscrive l'ambito delle fattispecie penali di

speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation, in www.medialaws.eu, 24.10.2018, 3, 110 ss.

[69] Per una panoramica generale cfr. anche T. Guerini, *Il Presidente e lo Sciamano. Riflessioni sul ruolo del diritto penale come elemento regolatore dell'*infosfera, in www.archiviopenale.it, 22.2.2021. I diversi modelli sono anche compendiati nello studio di A. De Streel et al., *Online Platforms' Moderation of Illegal Content Online. Law, Practices and Options for Reform*, in www.europarl.europa.eu, 23.6.2020.

[70] Cfr. «*Netzwerkdurchsetzungsgesetz vom 1. September 2017 (BGBl. I S. 3352)*».

rilievo [71] e definisce i tempi di rimozione, prevedendo che il *provider* debba (i) *immediatamente* prendere atto dei singoli reclami ed esaminarne il contenuto; (ii) rimuovere i contenuti "manifestamente illeciti" entro 24 ore dalla segnalazione, salvo che non sia stata concordata con l'autorità giudiziaria una diversa modalità e scadenza per la rimozione o il blocco del contenuto; (iii) decidere e provvedere sui contenuti non manifestamente illeciti entro un termine di sette giorni[72]. In parallelo, inoltre, e secondo un'impostazione *compliance-based*, si prevede la responsabilizzazione diretta e personale del *vertice* di ciascun *social network* per il monitoraggio sulla funzione di gestione dei reclami, la rimozione di eventuali carenze di stampo organizzativo e l'assicurazione di una adeguata formazione alle persone (fisiche) che materialmente si occupano di gestire i reclami, cosicché l'intero apparato risulta parte integrante dei processi di «*regulatory compliance*» [73] che i singoli *provider* sono tenuti a implementare. L'omesso adempimento di tali obblighi – *indifferentemente* per dolo o per colpa – comporta l'applicazione di una sanzione amministrativa pecuniaria[74].

Il *NetzDG* pare allora fondere il modello c.d. "economico" – limitando, cioè, l'applicazione della disciplina ai soli *provider* che superino determinati limiti dimensionali e che operino *a scopo di lucro* – con il modello di responsabilizzazione "intermedia" – nella parte in cui si fanno ricadere sul *provider* obblighi di rimozione e di cooperazione con l'autorità: con la sostanziale differenza, tuttavia, che – pur all'interno di un sistema co-regolato – l'*attualità* dell'obbligo di rimozione non discende da un ordine dell'autorità pubblica, ma deriva dalla ricezione della segnalazione di un contenuto (genericamente) illecito, rimettendo dunque al *provider* la (essenziale) valutazione circa la doverosità della rimozione.

Ne discende, in definitiva, come – pur trattandosi di sanzioni formalmente amministrative – l'ascrizione di responsabilità assuma la forma dell'omissione *propria*, nella misura in cui è affidata allo stesso destinatario della norma la valutazione circa la sussistenza (giuridica) del presupposto che faccia sorgere l'obbligo di *attivarsi*: così trasformando – come si è condivisibilmente osservato – i gestori di servizi internet in

[71] Si prevede, infatti, che rientrino nella nozione di «contenuti illegali» quelli che integrino gli estremi dei delitti di cui agli artt. 86, 86a, 89a, 91, 100a, 111, 126, da 129 a 129b, 130, 131, 140, 166, 184b, da 185 a 187, 201a, 241 o 269 StGB.

[72] Si prevede, inoltre, che sul *provider* incombano obblighi di natura "probatoria" – dovendo conservare i contenuti bloccati in conformità con la disciplina in tema di *data retention* – nonché "partecipativa", spettando sempre al *provider* l'obbligo di informare tanto il denunciante quanto l'utente del contenuto e dei motivi di ogni decisione. Ancora al *provider* spetta, inoltre, l'obbligo di prevedere una procedura per la revisione delle proprie decisioni, che può essere attivata tanto dall'utente, quanto dal denunciante e che deve necessariamente assicurare al richiedente un contatto diretto con la funzione aziendale responsabile della gestione delle segnalazioni e della rimozione dei contenuti illeciti. Infine, il modello della «autoregolamentazione regolata» trova, altresì, conferma nell'istituzione (§3, co. 6) di un ente, alla cui costituzione concorrono istituzioni e *social network*, competente per la "revisione" delle decisioni assunte dai *provider* o cui i singoli fornitori possono delegare la soluzione delle questioni che appaiano più complesse.

[73] Cfr. V. Claussen, *op. cit.*, 119.

[74] Di importo elevato: fino a 5 milioni di euro.

«sentinelle private» o in «ausiliari delle forze dell'ordine»[75], con un ruolo *attivo* e non meramente *esecutivo* di un provvedimento dell'autorità pubblica.

4.2. Un secondo modello generale di responsabilizzazione del *provider* può poi rinvenirsi nella *Loi visant à lutter contre la haine sur internet* (c.d. *Loi Avia*)[76], promulgata nell'ordinamento francese il 24 giugno 2020: mediante tale riforma si intendeva, in particolare, ampliare i doveri di cooperazione degli operatori di piattaforme *online* nella lotta contro i discorsi d'odio diffusi tramite internet, tanto nell'ottica della rimozione dei contenuti illeciti – mediante la previsione di obblighi (anche penalmente sanzionati) di rimuovere o rendere non accessibile, in conseguenza del ricevimento di una segnalazione, qualsiasi contenuto riconducibile alla definizione di "discorsi d'odio"–, quanto nelle fasi di accertamento e indagine dei reati, mediante obblighi di conservazione e di comunicazione di dati dall'autorità giudiziaria.

A prescindere dai contenuti di dettaglio di tale intervento, ciò che interessa ora sottolineare è, anzitutto, che il *Conseil d'État*, chiamato a rendere un parere preliminare sulla proposta di legge, ha ritenuto adeguato e ragionevole il regime di cooperazione previsto dalla *loi Avia* a carico degli operatori di servizi internet, riconoscendo che i *social network* e le piattaforme di condivisione di contenuti siano «nuovi attori», rispetto ai quali – «in quanto intermediari *attivi*» il cui ruolo non è più riducibile alla mera predisposizione dell'infrastruttura tecnica – risulta ormai inadeguata e "datata" la disciplina ispirata alla Direttiva 2000/31[77].

Cionondimeno, le novità introdotte con la *loi Avia* sono state censurate prima della loro promulgazione dal *Conseil constitutionnel*[78], che ha ritenuto, in termini generali, che le disposizioni di nuova introduzione realizzassero una limitazione alla libertà di espressione e comunicazione non appropriata, necessaria e proporzionata allo scopo perseguito. Più precisamente, il *Conseil constitutionnel* ha specificamente censurato la *loi Avia* nella parte in cui, imponendo sull'operatore un obbligo – penalmente sanzionato – di rimuovere i contenuti segnalati entro un termine di sole 24 ore, faceva sì che la "censura" di contenuti illeciti non presupponesse il preventivo intervento di un giudice, ma affidasse unicamente all'operatore il compito e la responsabilità di esaminare (oltremodo velocemente, per non rischiare di incorrere nelle sanzioni previste dal medesimo testo normativo) tutti i contenuti segnalati; e ciò a dispetto del fatto che nell'elenco dei reati che giustificavano la rimozione dei contenuti figurassero anche fattispecie composte da elementi costitutivi «giuridicamente complessi» o la cui

[75] J. Rinceanu, *op. cit.*, 10.
[76] Cfr. «*Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet*». Per alcune note di commento cfr. anche T. Guerini, *op. cit.*, 19 ss.
[77] Cfr. *Conseil d'État*, *Avis sur la proposition de loi visant à lutter contre la haine sur Internet*, 16.5.2019, consultabile *online* su www.assemblee-nationale.fr.
[78] Cfr. *Conseil constitutionnel*, 18.6.2020, n. 2020-801 DC, consultabile *online* su www.legifrance.gouv.fr.

illiceità poteva valutarsi soltanto soppesandone attentamente il significato alla luce del preciso contesto nel quale il contenuto in questione è stato diffuso[79]. Il *Conseil constitutionnel* ha, dunque, dichiarato numerose disposizioni della *loi Avia* contrarie alla Costituzione, perché il meccanismo creato non avrebbe fatto altro che «incoraggiare i gestori delle piattaforme *online* a rimuovere i contenuti loro segnalati, [fossero] essi manifestamente illeciti o meno»[80], così violando l'esercizio della libertà di espressione e di comunicazione in una misura non necessaria, appropriata e proporzionata.

Il *Conseil constitutionnel* è stato poi molto di recente chiamato a pronunciarsi nuovamente sul tema[81], in vista della promulgazione di una legge di adeguamento all'entrata in vigore del già citato Regolamento europeo n. 2021/784, con la quale si comminano sanzioni penali, a carico del *provider*, per l'omessa rimozione di contenuti di stampo terroristico a seguito di un ordine dell'autorità competente: in questo caso, tuttavia, il *Conseil constitutionnel* ha concluso per la conformità a costituzione delle disposizioni scrutinate, sul triplice presupposto della determinatezza dell'oggetto (esclusivamente contenuti di natura terroristica precisamente definiti e tassativamente individuati), della possibilità d'impugnazione dell'ordine di rimozione e della previsione di cause di esclusione della responsabilità per il *provider* che, ad esempio, non abbia potuto provvedere alla rimozione per impossibilità lui non imputabile.

4.3. Alcuni ulteriori spunti possono, infine, derivare dall'analisi dell'ordinamento statunitense, nell'ambito del quale è la *Section 230 CDA*[82], introdotta nel 1996, a costituire il principale referente normativo in tema di responsabilità del *provider*[83]. Ai limitati fini della presente analisi, basterà ora osservare come tale disposizione sia stata introdotta allo scopo di stabilire *espressamente* in via legislativa che il fornitore di un

[79] In questi termini, *Conseil constitutionnel*, 18.6.2020, cit.
[80] Cfr. ancora in questi termini, *Conseil constitutionnel*, 18.6.2020, cit.
[81] Cfr. *Conseil constitutionnel*, 13.8.2022, n. 2022-841 DC, consultabile *online* su www.legifrance.gouv.fr.
[82] Più correttamente, si tratta della *Section* 230 del *Title* 47 dell'*US Code*, introdotta con il *CDA* del 1996. Si riporta il testo: «*47 U.S. Code § 230 - Protection for private blocking and screening of offensive material: (c)Protection for "Good Samaritan" blocking and screening of offensive material: (1)Treatment of publisher or speaker: No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. (2)Civil liability: No provider or user of an interactive computer service shall be held liable on account of—(A)any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (B)any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1)*».
[83] Cfr. D. K. Citron, M. A. Franks, *The Internet as a Speech Machine and Other Myths Confounding Section 230 Reform*, in *UCLF* 2020, 45 ss.; V. C. Brannon, *Liability for Content Hosts: An Overview of the Communication Decency Act's Section 230*, in *Library of Congress. Congressional Research Service,* 6.6.2019; E. Goldman, *An Overview of the United States' Section 230 Internet Immunity,* in *Oxford Handbook of Online Intermediary Liability,* cit., 155 ss.

servizio informatico non *possa* essere considerato (*rectius*: qualificato, ai fini dell'applicazione della relativa disciplina) né come "editore", né come "autore", rispetto ai contenuti pubblicati dagli utenti[84]; d'altro canto, la medesima disposizione prevede altresì (e per converso) che nessun *provider* possa essere ritenuto responsabile per aver *limitato* l'accesso a contenuti ritenuti illeciti o altrimenti discutibili.

In particolare, una disciplina così articolata mirava a un duplice scopo, volendosi da un lato evitare che sui *provider* potesse ricadere un regime di responsabilità troppo gravoso (qual era quello, appunto, dell'editore o dell'autore) ma, dall'altro lato, intendendosi altresì incentivare e tutelare eventuali spontanee iniziative di "*content-filtering*", da parte dei singoli fornitori. Del resto, nella successiva interpretazione giurisprudenziale la disposizione è stata ampliata ben oltre l'originario intento legislativo, estendendosi l'ambito di applicazione di un siffatto "scudo" da responsabilità persino alle ipotesi in cui – com'è stato osservato – i singoli *provider* «incoraggiano azioni illegali, mantengono deliberatamente contenuti manifestamente dannosi o prendono parte alle attività illegali degli utenti», così dandosi forma, secondo la dottrina più critica, a un «potere senza responsabilità»[85].

Proprio in un siffatto contesto si discute oggi, dunque, della riforma della *Section 230*, sia pur con la consapevolezza che si tratti di un processo considerevolmente rallentato e complicato dalle narrazioni, dalle precomprensioni, dai miti o financo dagli equivoci che spesso condizionano la disciplina del fenomeno tecnologico e che impediscono di mettere a fuoco l'attuale ruolo delle piattaforme e degli intermediari *online*[86]: tra questi, ad esempio – ciò che è particolarmente significativo nella prospettiva che ci occupa – la persistente tendenza a considerare internet e le piattaforme quale mezzo neutrale di garanzia della libertà di espressione e non già quale attore del mercato dotato di considerevole potere (almeno) economico.

Ciò premesso, interessa ora soprattutto soffermare l'attenzione su alcuni modelli che attualmente si contrappongono, nel dibattito dottrinale relativo alla riforma della *Section 230*. Tra questi: (i) un primo modello coincide con la proposta di prevedere la responsabilità del *provider* che mantenga consapevolmente sul proprio sito (*knowingly*

[84] Come rammenta E. Goldman, *op. cit.*, 161, l'applicazione di tale esenzione è esclusa là dove venga in rilievo il diritto penale federale.

[85] I virgolettati sono tratti da D. K. Citron, M. A. Franks, *op. cit.*, 52. In senso critico v. anche D. Lichtman, E. Posner, *Holding Internet Service Providers Accountable*, in *Sup Court Eco Rev* 2006, 14, 221 ss., che propongono di ricorrere a un modello di *indirect liability*, nel senso di «*bring yet another entity into the chain of liability*».

[86] Cfr. D. K. Citron, M. A. Franks, *op. cit.*, 53: «*online advertising business model continues to incentivize revenue-generating content that causes significant harm to the most vulnerable among us*». Al riguardo può farsi riferimento anche a M. Lamanuzzi, *Il "lato oscuro della rete": odio e pornografia non consensuale. Ruolo e responsabilità dei gestori delle piattaforme* social *oltre la* net neutrality, in www.lalegislazionepenale.eu, 24.5.2021, in part. 17-18, ove l'A. si riferisce al caso c.d. «*Force v. Facebook*», deciso dalla *Court of Appeal* dello Stato di New York (in senso assolutorio) e relativo all'accusa, elevata a carico del *social network*, a titolo di concorso, perché le attività automatizzate di indicizzazione avevano attribuito visibilità ad alcuni post di incitamento al terrorismo. In relazione alle determinanti della riforma, cfr. anche E. Goldman, *op. cit.*, 171 ss.

hosting) contenuti illeciti[87]; (ii) un secondo paradigma si concentra, invece, sulla necessità di prevedere la responsabilità dell'intermediario il cui modello di *business* si fondi sul caricamento di contenuti illeciti da parte degli utenti[88]; (iii) un terzo schema, infine, contemplerebbe l'esclusione da responsabilità a favore del solo *provider* che provi di aver adottato misure ragionevoli per impedire e fronteggiare eventuali usi illeciti del servizio fornito[89].

In breve: mentre il primo modello risolve la questione dell'eventuale inadempimento del *provider* a un obbligo di rimozione attribuendo a quest'ultimo (per via legislativa) la responsabilità a titolo di concorso nell'illecito commesso dall'utente, il secondo paradigma pare invece rimandare alla distinzione tra condotte «neutrali» e condotte concorsuali, correttamente riconducendo nell'ambito di queste ultime quelle attività del professionista consapevolmente strumentali rispetto all'illecito dell'utente. Il terzo paradigma spicca, invece, in termini di novità, introducendo un riferimento alla prevenzione organizzativo-cautelare dei comportamenti illeciti su internet, là dove esso condiziona la responsabilità del *provider* al presupposto (negativo) dell'omessa adozione di misure adeguate e ragionevoli per moderare i contenuti diffusi sulla rete.

5. I recenti sviluppi che si osservano a livello europeo e nel panorama comparatistico confermano in definitiva l'avvertita esigenza, indicata in premessa, di "aggiornare" la riflessione penalistica relativa alla *responsabilità* (o alla *responsabilizzazione*) del *provider*, dovendosi anzitutto prendere atto del suo mutato ruolo nell'era del "capitalismo delle piattaforme": se, infatti, il modello originariamente dettato dalla Direttiva 2000/31 è tuttora attuale per quei fornitori "passivi" di servizi digitali (ad es. di connessione, di *webmail*), che, come recita lo stesso Cons. 42 della Direttiva, si limitano ad attività «di ordine meramente tecnico, automatico e passivo», la riflessione penalistica non può certo trascurare i paralleli processi di «*platformization*»[90], che vedono appunto in alcune piattaforme digitali non più *meri intermediari*, ma attori economici che «intervengono attivamente nella produzione, selezione e circolazione delle informazioni»[91].

[87] Proposta attribuibile al Prof. Geoffrey Stone, per cui cfr. D. K. Citron, M. A. Franks, *op. cit.,* 70.
[88] Secondo il modello dell'istigazione o del concorso (là dove il *provider* solleciti o distribuisca consapevolmente i contenuti illeciti caricati dagli utenti), per cui cfr. ancora D. K. Citron, M. A. Franks, *op. cit.,* 70.
[89] La proposta, attribuibile a Citron e Wittes, recita così: «*No provider or user of an interactive computer service that takes reasonable steps to address unlawful uses of its service that clearly create serious harm to others shall be treated as the publisher or speaker of any information provided by another information content provider in any action arising out of the publication of content provided by that information content provider*» (cfr. D. K. Citron, M. A. Franks, *op. cit.,* 71).
[90] Cfr. in termini M. Santaniello, *La regolazione delle piattaforme e il principio della sovranità digitale*, in *RivDPol* 2021, 3, 579 ss. e in part. 582.
[91] Cfr. ancora M. Santaniello, *op. cit.,* 584.

Tale rilettura del ruolo dei *provider*, che ispira la proposta delineata nel par. 5.1, non esaurisce peraltro le possibili prospettive di sviluppo dell'indagine: a ben vedere, infatti, la sempre più marcata *pervasività* delle tecnologie informatiche in ogni aspetto della vita quotidiana richiama anche il diverso modello teorico del «panottico digitale»[92], che per converso mette in luce la *capacità* degli attori della società dell'informazione di «protocollare l'intera vita»[93] degli utenti, registrando ogni traccia digitale, che si «imprime fedelmente nella rete»[94]. Ai limitati fini che ora interessano, tale seconda prospettiva di indagine ispira la riflessione di cui al par. 5.2, nel quale si muove dalla visione dei fornitori di servizi digitali quali *nodi* della *rete* e, di conseguenza, quali titolari di un inedito (quanto controverso) potere di sorveglianza e controllo sugli utenti, che assume peculiare rilievo per la definizione di nuovi modelli di contrasto alla diffusione di contenuti illeciti *online*. Infine, il modello proposto nel par. 5.3 è ispirato a considerazioni ancora diverse, e cioè alla presa d'atto del ruolo dei fornitori di servizi digitali in un contesto di tale integrazione tra mondo virtuale e mondo fisico – qual è quello odierno – che «la dipendenza sociale dalla stabilità e dalla sicurezza del cyberspazio, già indispensabili per l'economia digitale e la sfera pubblica, raggiunge persino la sicurezza umana e il funzionamento basilare delle infrastrutture»[95].

5.1. Come si accennava, una prima prospettiva di sviluppo consiste nella riconsiderazione del tema della responsabilità (penale) del *provider*, a partire dalla comprensione del nuovo modello di *business* spesso sottostante alla prestazione di servizi digitali, basato su una tendenziale esternalizzazione della produzione agli utenti e sulla monetizzazione, in vario modo, delle loro reciproche relazioni. Com'è stato condivisibilmente sottolineato, infatti, gli intermediari *online* operano tendenzialmente «attraverso strutture e logiche organizzative d'impresa»[96]: una caratteristica, quest'ultima, che non pare di secondario rilievo nell'ottica di comprendere quale modello d'incriminazione (e di prevenzione) meglio si attagli alla realtà da regolare[97].

---

[92] Cfr. B.C. Han, *Nello sciame. Visioni del digitale*, Roma 2015, 88 ss.
[93] Cfr. ancora B.C. Han, *op. cit.,* 88.
[94] B.C. Han, *op. cit.,* 89.
[95] L. Denardis, *Internet in ogni cosa. Libertà, sicurezza e privacy nell'era degli oggetti interconnessi*, trad.it, Roma 2021, 18.
[96] Cfr. B. Panattoni, *Gli effetti dell'automazione sui modelli di responsabilità: il caso delle piattaforme online,* in *DPenCont* 2019, 2, 33 ss., e in part. 52.
[97] In proposito, cfr. N. Helberger, J. Pierson e T. Poell, *Governing online platforms: From contested to cooperative responsibility*, in *InfSoc* 2018, 34, 1 ss., là dove si propone un modello di «*cooperative responsibility*» per coinvolgere i *provider* nella prevenzione degli illeciti *online*. Al riguardo, B. Panattoni, *Gli effetti dell'automazione sui modelli di responsabilità*, cit., 52, ipotizza «una «responsabilità organizzativa» («*responsibility for the design of organizations*»), derivante dall'aver disegnato la piattaforma in modo da non essere in grado di controllare, prevenire o rimuovere la disponibilità di contenuti illeciti accessibili o gestiti dagli utenti».

La questione merita di essere analizzata più nel dettaglio, prendendo quale ipotesi di lavoro le piattaforme di c.d. *social media*, il cui funzionamento riposa sulla condivisione di contenuti *online* da parte degli iscritti. Se, in generale, il modello di *business* adottato dai fornitori di servizi digitali rappresenta una «nuova forma di attività economica» che si contraddistingue per la capacità di trarre profitto «attraverso l'intermediazione digitale» [98], non è men vero, per contro, che le piattaforme di *social media* «non producono e non vendono nulla, se non pubblicità e informazioni sugli utenti»[99]. Invero, è proprio l'osservazione empirica[100] a dimostrare come esse *di fatto* traggano (almeno buona parte de)i propri profitti dalla diffusione di annunci pubblicitari (riconducibili a un c.d. «*behavioral advertising business model*»[101]) – la cui capacità di generare un ritorno economico è essenzialmente determinata dal volume delle interazioni e delle condivisioni da parte degli utenti[102] – ovvero dalla «monetizzazione» dei dati (singoli e aggregati) degli utilizzatori, a sua volta funzionale alla diffusione di messaggi pubblicitari personalizzati[103], secondo un paradigma che è stato definito "economia dell'attenzione"[104].

Non pare, dunque, azzardato ipotizzare che in una posizione intermedia tra l'*hosting provider* attivo "*à la* Pirate Bay" – la cui attività sostanzialmente *si riduce* alla condivisione di contenuti illeciti (perché ad es. protetti da diritto d'autore) e, dunque, a un uso *interamente illecito* delle tecnologie digitali – e il *provider* (individuale) incolpevole, semplice destinatario di un ordine di rimozione – cui, come si è visto, risulta tuttora impossibile attribuire un qualsivoglia obbligo di garanzia, – debba prendersi in considerazione un terzo "idealtipo" di piattaforma *online*, che pur dominando la scena del *web*, sembrerebbe tuttora tendenzialmente (quanto sorprendentemente) estraneo al dibattito dottrinale in tema di responsabilità (penale) del *provider*: si allude, come si è anticipato, al fornitore di servizi digitali che svolga su

[98] Cfr. S. Vallas, J. B. Schor, *What Do Platforms Do? Understanding the Gig Economy,* in *Ann Rev Soc* 2020, 46, 273 ss., e in part. 282: la società che gestisce la piattaforma si occupa della «ripartizione dei compiti», della «raccolta dei dati» e del «trattenimento dei profitti», ma cede il controllo sulle transazioni e sulle modalità di lavoro direttamente agli utenti. Cfr. analogamente N. Helberger, J. Pierson e T. Poell, *op. cit.*, 1: «*online platforms can be defined as socio-technical architectures that enable and steer interaction and communication between users through the collection, processing, and circulation of user data*».

[99] Ancora cfr. D. K. Citron, M. A. Franks, *op. cit.*, 52. Osservano S. Vallas, J. B. Schor, *op. cit.*, 275, come le piattaforme di *social media* ricavino essenzialmente i propri profitti dalla vendita di dati degli utenti.

[100] Per cui si rinvia nuovamente a S. Vallas, J. B. Schor, *op. cit.*, 273 ss., nonché al *Dissenting Statement Of Commissioner Rohit Chopra, In re Facebook, Inc.* – Commission File No. 1823109, consultabile su www.ftc.gov, 24.7.2019.

[101] Cfr. D. K. Citron, M. A. Franks, *op. cit.*,53.

[102] Cfr. D. K. Citron, M. A. Franks, *op. cit.*, 52, ma anche S. Vallas, J. B. Schor, *op. cit.*, 275, ove gli A. illustrano i diversi modelli di *business* delle piattaforme.

[103] Cfr. ancora il Dissenting Statement del Commissioner Rohit Chopra, cit., 2: «*Behavioral advertising generates profits by turning users into products, their activity into assets, their communities into targets, and social media platforms into weapons of mass manipulation*». In senso per certi versi contrario cfr. A. Mantelero, *La responsabilità on-line: il controllo nella prospettiva dell'impresa*, in *DInf* 2010, 3, 405 ss. e in part. 408 ss.

[104] Cfr. M. Staglianò, *op. cit.*, 79.

internet un'attività d'impresa *lecita* e che tragga profitti in dipendenza e in proporzione con il traffico e le condivisioni da parte degli utenti.

Proprio il modello generale delineato dal d. lgs. 231/2001 si rivela, dunque, di estremo interesse, ai fini della presente riflessione: al riguardo basterà osservare come la dimostrata insussistenza di una posizione di garanzia (individuale) in capo al *provider* per i contenuti illeciti pubblicati dagli utenti di certo non impedisca di valutarne eventuali profili di responsabilità e (di responsabilizzazione) "a livello" dell'*organizzazione*. Invero, com'è stato osservato a ragione, anche i più recenti dibattiti in ordine alla responsabilità del *provider* risultano tuttora influenzati da una (controproducente e superata) logica dicotomica «*host-editor*», che polarizza erroneamente le opzioni regolatorie disponibili nell'alternativa tra il regime di tendenziale "irresponsabilità" tipico dell'«*host provider*» e, per converso, il modello del c.d. «*editor*», che implicherebbe un'opposta responsabilità piena per (il controllo dei) contenuti pubblicati dagli utenti[105].

Così formulata, tuttavia, la questione non rispecchia le effettive «capacità delle piattaforme di *prevenire*» determinati eventi ritenuti socialmente indesiderabili (in concreto: la diffusione di contenuti illeciti), né del resto riflette la misura in cui esse per certi versi *contribuiscono* a "dar forma" alle interazioni e ai comportamenti degli utenti[106]. Cosicché – e lasciando impregiudicata la (necessaria) responsabilità individuale dei singoli utilizzatori[107] – è proprio la richiamata rilettura in senso "economico-imprenditoriale" del ruolo delle "piattaforme" a suggerire di ipotizzarne una forma di coinvolgimento nella prevenzione degli illeciti *online* sul modello (e nei limiti) della responsabilità (para-penale) d'impresa.

In questo senso, anziché riflettere nei termini di (piuttosto irrealistici) obblighi d'impedimento individuali rispetto a singoli contenuti illeciti pubblicati dagli utenti, si potrebbe allora ragionare nei termini di un modello di responsabilità che è stato definito di «*prospective design responsibility*»[108], nel quale assume preminente rilievo l'adozione da parte dell'intermediario di un'organizzazione (d'impresa) funzionale a prevenire la diffusione di contenuti illeciti[109], nella misura (e nei limiti) in cui questi si inseriscono nell'attività economica prestata (e, dunque, sul presupposto che, caso per

[105] L'osservazione e i virgolettati sono tratti da N. Helberger, J. Pierson e T. Poell, *op. cit.*, 2.
[106] Cfr. ancora N. Helberger, J. Pierson e T. Poell, *op. cit.*, 2.
[107] Come condivisibilmente osservano N. Helberger, J. Pierson e T. Poell, *op. cit.*, 3, alla responsabilità individuale dei singoli utenti spetta comunque un ruolo essenziale per assicurare, in generale, un certo livello di deterrenza e un incentivo ad assumere comportamenti responsabili.
[108] Cfr. Ancora N. Helberger, J. Pierson e T. Poell, *op. cit.*, 4.
[109] Come osservano M. L. Montagnani, A. Tropova, *Safe harbours in deep waters: a new emerging liability regime for Internet intermediaries in the Digital Single Market*, in *IJLIT* 2018, 26, 4, 294 ss., 3, un simile modello da responsabilità «organizzativa» può anche essere variamente modulato in ragione dell'illiceità dei singoli contenuti (ad es. distinguendosi tra contenuti di natura terroristica o pedopornografica da messaggi diffamatori).

caso, il descritto funzionamento delle piattaforme renda *direttamente* riferibile ai vertici dell'impresa la diffusione dei contenuti illeciti).

In tal senso, proprio il Modello di organizzazione, gestione e controllo previsto dal d. lgs. 231/2001 in tema di responsabilità amministrativa da reato degli enti – che, del resto, contempla tra i c.d. reati-presupposto fattispecie di sicuro interesse nell'ottica proposta, tra le quali ad es. i delitti con finalità di terrorismo, i delitti in materia di pedopornografia o di violazione del diritto d'autore – potrebbe rappresentare un paradigma dell'adempimento preventivo *esigibile* da parte dei singoli *provider*[110].

Un simile modello non si tradurrebbe, infatti, (almeno idealmente) nell'imposizione a carico dei fornitori di servizi digitali di un indeterminato obbligo di "sorveglianza" sulle attività degli utenti, ma piuttosto configurerebbe in capo ai medesimi un regime di *accountability* del tutto analogo a quello che già si riscontra in numerosi altri settori economici, là dove s'impone all'ente di organizzarsi in modo da impedire che vengano commessi (determinati) reati *nel suo interesse o a suo vantaggio*; ciò che, ad esempio, può accadere qualora nella "politica d'impresa" definita dal *management*[111] sia previsto (o, comunque, risulti indifferente) che la piattaforma, in ragione del suo funzionamento e delle connesse modalità di conseguimento dei profitti, possa trarre vantaggio (anche) da eventuali attività illecite degli utenti o, anzi, tragga da queste il maggior ritorno economico.

5.2. Una seconda cornice teorica che, come anticipato, pare essenziale considerare per delineare ulteriori possibili modelli di *responsabilità/responsabilizzazione* del *provider* nell'attuale società digitale è quella che fonde l'immagine della *rete*[112] (della quale il *provider* è un *nodo*) con l'analisi del concreto funzionamento delle tecnologie informatiche, le quali si distinguono per la *capacità* potenziale di ritenere la traccia digitale di tutto ciò che accade, nonché di conformare digitalmente i comportamenti degli utenti.

Benché tale modello sia stato sovente richiamato per mettere in guardia dai risvolti negativi della digitalizzazione – nella misura in cui la connessione in rete consente non soltanto il «controllo totale»[113] degli utenti, ma rende possibile anche il successivo «sfruttamento economico» dei dati raccolti, in quel «mercato dei comportamenti futuri» che contraddistingue il «capitalismo della sorveglianza» –, sorprende però che

[110] In argomento cfr. ad es. G. Miceli, *Profili evolutivi della responsabilità in Rete: il ruolo degli Internet Service Provider tra prevenzione e repressione*, in www.medialaws.eu, 11.10.2017.

[111] Cfr. ancora il Dissenting Statement del Commissioner Rohit Chopra, cit., 19, in relazione al ruolo dei soggetti apicali: « *Corporate executive officers and directors serving on corporate boards play a critical role in ensuring compliance with applicable law and regulation*».

[112] Per cui cfr. le riflessioni di A.L. Barabási, *Link. La nuova scienza delle reti*, Torino 2022. In ordine all'impatto di tale struttura sul "sistema di governo" di internet, cfr. B. Carotti, *Il sistema di governo di internet*, Milano 2016.

[113] Cfr. ancora B.C. Han, *Nello sciame*, cit., 90 s., che ritiene che «sorveglianza e controllo siano una parte essenziale della comunicazione digitale»

di tali caratteristiche non si tenga quasi mai conto quando si tratti di individuare le più efficaci forme di contrasto ai comportamenti illeciti *online*[114]. Infatti, con la progressiva estensione dell'«ambito del calcolabile a tutta la realtà umana» le tecnologie informatiche e digitali hanno ormai assunto le dimensioni di un «fatto sociale totale»[115] e la loro intrinseca struttura *reticolare* è capace di incidere sulla forma e sulla natura delle relazioni sociali e di lavoro, ma anche di contestare la stessa vocazione esclusiva dello Stato a governarle, attribuendo inedite e sempre più ampie posizioni di potere a quei soggetti (spesso privati) che controllano i "nodi" delle reti e dei sistemi, con l'effetto di disgregare le tradizionali relazioni istituzionali nel governo dei comportamenti umani[116].

Ebbene, pare allora che proprio da tali caratteristiche debba partirsi per valorizzare l'essenziale ruolo dei *provider* nel rendere *tecnicamente possibile* il contrasto degli illeciti *online*, come emerge da alcune delle suggestioni provenienti dal contesto europeo e come del resto può già notarsi – nell'ordinamento italiano – nella (sola) l. 71/2017, dedicata al fenomeno del c.d. *cyberbullismo*: un paradigma, quest'ultimo, che si vuole ora portare quale esempio di un approccio ben più "maturo" al tema della repressione e del contrasto ai comportamenti illeciti in rete.

La peculiarità – ma anche, ad avviso di chi scrive, la validità di tale intervento normativo – dipende, in particolare, dal fatto che il legislatore abbia introdotto strumenti di tutela e di contrasto ritagliati "su misura"[117] sul fenomeno da regolare, ad esempio predisponendo una procedura per mettere *direttamente* in contatto il *provider* e la vittima di *cyberbullismo*, al fine della rimozione dei contenuti, e non delegando tale eventualità alla sola auto-organizzazione del prestatore di servizi digitali; strumenti, lo si anticipa sin d'ora, che potrebbero senz'altro costituire un modello generale di riferimento, là dove si tratti di gestire i tratti caratteristici della società dell'informazione nell'ottica del diritto penale.

---

[114] Invero, quasi nessuno dei più recenti interventi normativi riconducibili al *cybercrime* contiene specifiche disposizioni pragmaticamente modellate sulle caratteristiche della rete e sui poteri dei fornitori di servizi digitali.

[115] I virgolettati sono tratti da A. Garapon, J. Lassegue, *La giustizia digitale. Determinismo tecnologico e libertà*, trad. it, Bologna 2021, 79.

[116] Cfr. ad es. V. Katz, *Regulating the sharing economy*, in *BTLR* 2015, 30, 1067 ss., ma anche J. Cohen, *op. cit.*; nonché M. Leiser, A. Murray, *The Role of Non-State Actors and Institutions in the Governance of New and Emerging Digital Technologies*, in *The Oxford Handbook of Law, Regulation and Technology,* cit., 671 ss. In termini più generali, W. Hoffmann-Riem, *op. cit.*, 159 ss., propone di inquadrare le diverse proiezioni di una nuova tecnologia entro le categorie di *output* (per intendere i processi, i prodotti, i servizi resi possibili dalla nuova tecnologia), *impact* (per descrivere gli effetti sui soggetti che ne sono direttamente o indirettamente interessati, es. gli utenti) e infine *outcome* (per alludere ai cambiamenti indotti da una determinata tecnologia a livello "macro", nel lungo periodo e sull'intera società, ad es. «sulle strutture di mercato, sull'ordine democratico, sull'esecuzione delle garanzie costituzionali»).

[117] Cfr. M. C. Parmiggiani, *Il* cyberbullismo, in *Cybercrime*, cit., 631 ss.; C. Grandi, *Il "reato che non c'è": le finalità preventive della legge n. 71 del 2017 e la rilevanza penale del cyberbullismo*, in *SI* 2017, 12, 1440 ss.; C. Panicali, *Il cyberbullismo: i nuovi strumenti (extrapenali) predisposti dalla legge n. 71/2017 e la tutela penale*, in *RCivPrev* 2017, 6, 2081 ss.

Muovendo, infatti, dal riscontro, supportato da studi di carattere psicologico e sociologico, che l'uso di mezzi informatici o telematici conferisca agli atti di (*cyber*)bullismo alcune caratteristiche singolari e particolarmente allarmanti – perché l'ambiente digitale, oltre ad acuire la diffusività massiva del messaggio, assicura altresì al perpetratore alcuni "vantaggi" sul piano personale (difficile reperibilità, assenza di limiti spazio-temporali), così indebolendo le sue remore etiche e rendendo tale fenomeno criminoso più frequente e più pervasivo – il legislatore non è intervenuto sul piano del diritto penale sostanziale (introducendo disposizioni *speciali*), ma ha agito sul versante dei rimedi, al fine di pervenire a una tutela (né simbolica, né *mediata*, quanto invece) *diretta* dei soggetti che ne siano vittima.

A tal fine, per quanto ora interessa, il legislatore ha introdotto nella l. 71/2017 strumenti extra-penali di carattere *preventivo* e *successivo* (questi ultimi, di natura sia cautelare, sia ripristinatoria), prevedendo ad esempio all'art. 2 la possibilità di inoltrare (anche) al gestore del sito internet o del *social media*[118] una specifica istanza per l'oscuramento, la rimozione o il blocco dei contenuti illeciti eventualmente diffusi ai danni di minori nella rete internet, [119], che per l'appunto valorizza, nella direzione dell'*effettività*, il potere del «gestore del sito internet» rispetto all'accesso ai contenuti.

Il coinvolgimento dei *provider* nelle attività di *law enforcement – lato sensu* intese – da parte delle autorità nazionali pare, in effetti, - proprio in ragione del *ruolo* e delle *capacità* che essi hanno nel *web* - l'unica soluzione capace di assicurare *l'effettività* di un regime di contrasto ai contenuti e ai comportamenti illeciti altrimenti destinato ad arrestarsi di fronte alla *pervasività*, all'*invisibilità*, alla *de-territorializzazione* e all'*anonimato* in rete[120]: con ciò, beninteso, non si prospetta l'attribuzione ai fornitori di servizi digitali di un autonomo ruolo di "giustizieri" della rete, ma si rileva l'importanza di considerarli (e regolarli) come *ordinari* e *strutturali* attori dell'(ormai altrettanto *ordinario*) contesto digitale (ad es. *responsabilizzandoli* mediante la previsione di specifici obblighi di cooperazione istruttoria o di esecuzione dei provvedimenti di autorità pubbliche).

[118] Il co. 2 dell'art. 2 prevede, poi, che qualora, entro le ventiquattro ore successive al ricevimento dell'istanza di cui al comma 1, il soggetto responsabile non abbia comunicato di avere assunto l'incarico di provvedere all'oscuramento, alla rimozione o al blocco richiesto, ed entro quarantotto ore non vi abbia provveduto, o comunque nel caso in cui non sia possibile identificare il titolare del trattamento o il gestore del sito internet o del social media, l'interessato può rivolgere analoga richiesta, mediante segnalazione o reclamo, al Garante per la protezione dei dati personali, il quale, entro quarantotto ore dal ricevimento della richiesta, provvede ai sensi degli articoli 143 e 144 del d. lgs. 30.6.2003, n. 196.

[119] In argomento cfr. ancora C. Grandi, *op. cit.*, 1441 ss.

[120] Cfr. J. Clough, *Principles of Cybercrime*, Cambridge 2010, 5 ss., ove l'A. identifica quali sfide determinanti del *cybercrime*: «*scale*», «*accessibility*», «*anonimity*», «*portability and transferability*», «*global reach*», «*absence of capable guardians*».

5.3. Infine, come si anticipava, una terza immagine che può utilmente entrare nel dibattito *attuale* sulla responsabilità dei fornitori di servizi digitali è quello dell'*infrastruttura*, alla luce della graduale percezione della specifica condizione di *vulnerabilità* e di *dipendenza* che il pervasivo ricorso alle tecnologie informatiche ha determinato nell'intera società dell'informazione [121]. In conseguenza della quale, dunque, il *provider* non è soltanto un soggetto economico o un "nodo" della rete, ma diventa altresì, in conseguenza dell'integrazione dell'infrastruttura cibernetica nel mondo fisico e della sempre maggiore (e più ampia) *interdipendenza reciproca* (nella misura in cui un attacco informatico può avere ripercussioni sulla realtà materiale, ma specularmente un attacco alla dimensione fisica delle reti o dei sistemi informatici si abbatte anche sul relativo contenuto digitale) [122], un attore della *governance* della sicurezza.

Si allude, in particolare, al modello di gestione "preventiva" della «sicurezza informatica»[123] (o *cybersecurity*), che si è progressivamente sviluppato *a complemento* delle misure di repressione penale dei c.d. *computer crimes*, sul versante della tutela dell'integrità delle reti, dei dati e dei sistemi, nel quale pare possibile enucleare altresì anche uno *specifico* statuto per il fornitore di servizi digitali. A differenza dei precedenti, peraltro, un siffatto paradigma non è estraneo al diritto positivo, per quanto si tratti di disposizioni di recente introduzione.

Particolarmente significativi nella prospettiva che ora interessa sono, infatti, la Direttiva UE n. 1148/2016, c.d. NIS («recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione»)[124], recepita con il d. lgs.

---

[121] Cfr. U. Sieber, *Legal Aspects of Computer-Related Crime in the Information Society*, CONCRIME-Study, 1998, 2: «*The vulnerability of today's information society in view of computer crime is still not sufficiently realised: Businesses, administrations and society depend to a high degree on the efficiency and security of modern information technology*». Cfr. anche P. Severino, *Le frontiere della sicurezza informatica e prevenzione del* cybercrime, in www.open.luiss.it, 8.9.2017, 5, ove l'A. sottolinea il nesso tra *cybersecurity* e «duttilità delle tecniche d'attacco» informatico. Cfr inoltre L. D'Agostino, Cybersecurity*, (auto)regolazione e governance del rischio.* Quid de iure poenali*?*, in www.lawreview.luiss.it, 2017, 1, 126 ss. e in part. 127, nel senso che la scelta di porre l'accento sulla *cybersecurity* dipende dalla «crescente informatizzazione dei processi comunicativi e dei rapporti economici», la quale a sua volta è connessa a un «aumento del rischio di *cybercrime*».

[122] Cfr. L. Denardis, *op. cit., passim.*

[123] Che M. Hildebrandt, *Law for computer scientists and other folks*, Oxford 2020, 165, definisce come «*confidentiality, integrity, and availability (CIA) of either data, computing systems, or both*». In argomento cfr. anche R. Flor, *Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, in *DInt* 2019, 3, 453 ss. e in part. 454: i *cyber-attacks* compromettono la c.d. *CIA-Triad* (*Confidentiality*, *Integrity*, *Availability*), nonché 456, ove l'A. illustra come la nozione di *cybersecurity* includa la tutela di tutte le componenti del *cyberspace* (e, dunque, «*computers*, informazioni, *ICTs,* reti, *ICT-based infrastructures*»; essa, in definitiva, può considerarsi un bene giuridico di natura «super-individuale e collettiva» ("intermedio" rispetto alla lesione di altri beni di natura economica o sociale). Cfr. anche L. Picotti, *Cybersecurity: quid novi?*, in *DInt* 2020, 1, 11 ss.

[124] Il cui contenuto è integrato dal Regolamento di Esecuzione (UE) 2018/151 della Commissione del 30.1.2018, recante modalità di applicazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio per quanto riguarda l'ulteriore specificazione degli elementi che i fornitori di servizi digitali devono prendere in considerazione ai fini della gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi e dei parametri per determinare l'eventuale impatto rilevante di un incidente.

18.5.2018, n. 65, nonché il d.l. 21.9.2019, n. 105 (conv. l. 18.11.2019, n. 133), in materia di «perimetro di sicurezza nazionale cibernetica», specificamente concepiti per disciplinare la materia della sicurezza informatica in modo sistematico e onnicomprensivo[125].

Come si è anticipato, tali interventi normativi rispondono espressamente all'intenzione programmatica – avvertita come particolarmente urgente, a livello europeo – di «ridurre drasticamente il *cybercrime*» promuovendo al contempo lo sviluppo di risorse industriali e tecnologiche adeguate a garantire e rafforzare preventivamente la *cybersecurity*[126], coinvolgendo (e responsabilizzando) altresì gli attori privati. Coerentemente con le premesse dianzi illustrate, la direttiva 2016/1148 si segnala proprio per la creazione di un "sotto-sistema" di obblighi di sicurezza e obblighi di notifica, che coinvolgono ad un tempo gli operatori di servizi essenziali[127] e i fornitori di servizi digitali[128], con l'intento di «promuovere una cultura della gestione dei rischi e garantire la segnalazione degli incidenti più gravi»[129].

Nella prospettiva che in questa sede rileva, e senza soffermarsi su un'analisi di dettaglio dell'intera disciplina[130], la direttiva indica in particolare agli Stati membri di provvedere affinché gli operatori di servizi essenziali, ma anche i fornitori di servizi digitali, adottino «misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi» per la sicurezza delle reti e dei sistemi, precisandosi che tali misure debbano tener conto «delle conoscenze più aggiornate in materia» e debbano assicurare un livello di sicurezza «adeguato al rischio esistente»[131], nonché misure

[125] In argomento, cfr. ad es. A. Mantelero et al., *The common EU approach to personal data and cybersecurity regulation*, in *IJLT* 2021, 28, 297 ss., ove gli Autori elencano altri regolamenti o direttive europei che, pur indirettamente, hanno imposto ai fornitori di servizi nella società dell'informazione l'adozione di presidi di sicurezza, funzionali alla tutela dell'integrità dei programmi, delle reti, dei dati e delle transazioni. Tra queste rientrano, ad esempio, la direttiva sui servizi di pagamento (PSD2) e il regolamento eIDAS (electronic IDentification Authentication and Signature) sull'identità digitale. Cfr. anche R. Flor, *op. cit.,* 457 ss., che vi riconduce la direttiva 2013/40, la direttiva 2017/541 sulla lotta contro il terrorismo, il regolamento europeo 2016/679, nonché la più recente direttiva 2019/713.

[126] Cfr. *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace* del 7.2.2013.

[127] Da identificarsi avuto riguardo a tre parametri: a) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali; b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi; e c) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio (art. 5).

[128] Con ciò intendendosi, in conformità con la Direttiva UE 2015/1535 «qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi».

[129] In questi termini cfr. Direttiva UE 2016/1148, *considerando* n. 4.

[130] Giova precisare come la struttura portante del sistema delineata nella Direttiva riposi sull'adozione da parte dei singoli Stati membri di una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi, comprensiva di una valutazione dei principali rischi e dell'individuazione di «misure di preparazione, risposta e recupero» che includano forme di cooperazione tra pubblico e privato.

[131] Come osserva R. Flor, *op. cit.,* 459, i fornitori di servizi digitali nell'approntare le misure di sicurezza devono tener conto «di ulteriori elementi quali, oltre a quelli già previsti per gli operatori di servizi essenziali, la portata

adeguate «per prevenire e minimizzare l'impatto di incidenti» a carico della sicurezza della rete e dei sistemi informativi, prevedendosi altresì sanzioni *effettive, proporzionate* e *dissuasive*, a garanzia del rispetto delle citate prescrizioni. La concreta attuazione di tale ultima previsione si ritrova nel decreto di recepimento n. 65/2018, là dove, per l'ipotesi dell'omessa adozione delle misure di gestione del rischio e di prevenzione e minimizzazione dell'impatto degli incidenti (nonché per l'omessa notifica degli incidenti rilevanti e per l'inadempimento degli ulteriori obblighi e istruzioni), si prevede l'applicazione di una sanzione amministrativa pecuniaria, a carico dell'operatore di servizi essenziali o del fornitore di servizi digitali.

Per certi versi analoga è altresì la disciplina di cui al d.l. 105/2019 (conv. l. 133/2019)[132], in materia di «perimetro di sicurezza nazionale cibernetica», istituito al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale[133]. Nuovamente, tra i destinatari degli obblighi di sicurezza e di notifica sono ricompresi anche gli "operatori privati": significativamente, tuttavia, non soltanto i fornitori di servizi digitali, quanto invece tutti gli "operatori privati" dai quali, come si anticipava, dipenda l'esercizio di una "funzione essenziale", ovvero la prestazione di un "servizio essenziale" per gli interessi dello Stato e che a tal fine impieghino reti, sistemi informativi e servizi informatici. Ciò che, dunque, conferma l'intuizione teorica secondo la quale, «in un contesto di sistemi che incorporano componenti sia digitali sia materiali», «tutte le aziende sono oggi società tecnologiche»[134].

Infine, il "sotto-sistema" della *cybersecurity* è stato ulteriormente integrato dalle disposizioni del Regolamento UE 2019/881 (c.d. *Cybersecurity Act*), con il quale – nell'ambito della più ampia *Digital Single Market Strategy* europea – si sono poste le basi per l'introduzione di un sistema di certificazione della *cybersecurity* per le

dell'alterazione o del turbamento del funzionamento del servizio e la portata dell'impatto sulle attività economiche e sociali».

[132] Per cui cfr. L. Picotti, R.M. Vadalà, *Sicurezza cibernetica: una nuova fattispecie delittuosa a più condotte con estensione della responsabilità degli enti*, in www.sistemapenale.it, 5.12.2019.

[133] I criteri individuati dal decreto per l'inclusione di operatori pubblici e privati nel perimetro nazionale di sicurezza cibernetica sono piuttosto ampi, identificandosi a) nell'esercizio di una funzione essenziale dello Stato, ovvero di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato; e b) l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale.

[134] Cfr. L. Denardis, *op. cit.*, 25.

tecnologie dell'informazione e della comunicazione, con l'intento rafforzare ancor più anticipatamente la *resistenza* agli attacchi informatici, mediante la diffusione di «prodotti, servizi e processi tecnologici» sviluppati secondo il principio della c.d. «*security by design*»[135]. Alla luce di tale finalità, la nuova disciplina "risale" allora lungo l'ideale catena che già univa l'utente al *provider*, per mirare direttamente al *produttore* dei dispositivi, dei servizi e dei processi tecnologici, cui si richiede di proteggere «l'economia e la società» dalla *vulnerabilità* informatica integrando determinati requisiti di sicurezza già *all'interno* dei prodotti (*hardware* e *software*) digitali[136].

Tale sintetica panoramica senz'altro consente di cogliere un'ascesa "verticale" del *punto* d'intervento prescelto da legislatore (interno o europeo), che ora coincide con il c.d. *gatekeeper* dell'ambiente digitale[137] (il fornitore, l'operatore o il produttore), da coinvolgere in una inedita «cultura della prevenzione del *cyber-risk*» e, dunque, nella «valutazione e gestione del rischio»[138]: ciò è a dire, in altre parole, che *anche* nel settore delle tecnologie informatiche e digitali si è presa contezza, nel definire le scelte di politica criminale, del ruolo centrale degli attori *privati*, in quanto destinatari di precisi (e pervasivi) obblighi di sicurezza e *responsabilizzati* per la gestione dei rischi informatici mediante l'adozione di misure di carattere tecnico e organizzativo[139].

D'altra parte, benché, come si è visto, il mancato adempimento a siffatti obblighi sia per ora esclusivamente sanzionato nella forma dell'illecito (penale o amministrativo) omissivo *proprio*, parrebbe altresì doveroso chiedersi se la convergenza tra il riconoscimento degli «emergenti interessi giuridici della riservatezza informatica, dell'integrità e della disponibilità dei sistemi informatici e dei dati», da un lato, e la costruzione di un sistema di «obblighi d'intervento» a carico dei c.d. *gatekeeper* della società dell'informazione, dall'altro, non valga da sé a costituire in capo a questi ultimi una (inedita) posizione di garanzia[140].

---

[135] Cfr. R. Flor, *op. cit.*, 461. Giova sottolineare, inoltre, come nelle definizioni del Regolamento (art. 2), la nozione di «cibersicurezza» sia estremamente ampia, comprendendo «l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche» e come la stessa nozione di «minaccia informatica» a sua volta si estenda fino a ricomprendere «qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone».

[136] In tal senso, il Regolamento include tra gli obiettivi di sicurezza, ad esempio, la protezione dei dati, la segmentazione delle possibilità di accesso ai dati medesimi, l'autonoma individuazione e documentazione delle *dipendenze* e delle *vulnerabilità*, la sicurezza «fin dalla progettazione e per impostazione predefinita».

[137] Cfr. A. D. Murray, *Nodes and Gravity in Virtual Space*, in *Legisprudence*, 2011, 5, 195 ss. e T. J. Holt, *Regulating Cybercrime through Law Enforcement and Industry Mechanisms*, in *Ann American Academy Pol Soc Sci*, 2018, 140 ss.

[138] Cfr. P. Severino, *op. cit.*, 8-9.

[139] Sottolinea un siffatto mutamento anche R. Flor, *op. cit.*, 466-467.

[140] Cfr. in questi termini R. Flor, *op. cit.*, 467. Osserva al riguardo L. Picotti, *Cybersecurity: quid novi?*, cit., 14, come nel settore della sicurezza informatica si debba constatare il passaggio da un sistema di adempimenti «privati e disponibili» a un a un complesso di obblighi «di natura pubblica», i quali dovrebbero però essere oggetto di presidi, vigilanza e controlli anche sull'opposto versante di eventuali abusi e usi impropri.

6. - All'esito dell'analisi sinora condotta, pare allora che l'iniziale ipotesi di ricerca abbia trovato significative conferme e che, dunque, la responsabilizzazione dei fornitori di servizi digitali rappresenti un tema di significativa attualità: i modelli da ultimo proposti rappresentano, in effetti, soltanto uno spunto per considerare con il necessario *pragmatismo* il ruolo che i *provider* hanno nell'attuale società digitale e, di conseguenza, per esemplificare le funzioni che ad essi possono essere più utilmente attribuite, con un approccio quasi casistico, che può portare alla creazione di un ventaglio di regimi alternativi ma anche potenzialmente sovrapposti, in dipendenza dell'angolo visuale di volta in volta adottato.

Soprattutto, si vuole, sottolineare come nessuno dei modelli proposti (quello del *business*, che responsabilizza il *provider* rispetto all'attività economica esercitata; quello della *rete*, che responsabilizza il *provider* per la posizione rivestita; quello dell'*infrastruttura*, che responsabilizza il *provider* rispetto alla struttura che egli gestisce) propugna in realtà la creazione di un regime "eccezionale", muovendo anzi dall'implicito presupposto che il fornitore di servizi digitali debba essere riguardato e regolato al pari di ogni altro attore socio-economico: appunto, per l'attività esercitata, per la peculiare posizione rivestita, o ancora per la specifica infrastruttura gestita.

Ben più problematiche paiono, invece, quelle tendenze che, partendo dall'idea mitizzata del *provider* quale «azienda-mondo»[141] (in ragione delle dimensioni, dei poteri, della vocazione a *ordinare* i comportamenti degli utenti), finiscono per attribuirgli un ruolo parastatale ed *extra-ordinem*: si allude, nello specifico, a quell'«orizzontalizzazione»[142] degli obblighi di controllo che incardina in capo ai *provider* veri e propri obblighi di sorveglianza, intervento, prevenzione e denuncia, con una latitudine tale per cui questi ultimi debbono ingerirsi tanto (e problematicamente[143]) nella *valutazione* circa l'eventuale rilevanza penale di determinati comportamenti, quanto nella *determinazione* delle relative conseguenze. In questo modo li si trasforma, però, «in arbitri della legalità *online*», pur in mancanza della specifica «competenza» e della necessaria «indipendenza»[144].

[141] Cfr. M. Stagliano, *op. cit.*, 49.
[142] Cfr. A. Garapon, J. Lassegue, *op. cit.*, 206.
[143] Una conferma in tal senso si ritrova, ad esempio, nelle *Conclusioni* presentate dall'Avvocato Generale Saugmandsgaard Øe il 15.7.2021, in relazione alla Causa C.G.U.E. C-401/19 (Repubblica di Polonia contro Parlamento europeo, Consiglio dell'Unione europea), reperibili su www.curia.europa.eu, e in particolare nel § 197, ove l'A.G. testualmente osserva: «Ne consegue, in maniera generale, che, se i prestatori intermedi si trovano in una posizione favorevole, sotto il profilo tecnico, per lottare contro la presenza di determinate informazioni illecite diffuse tramite i loro servizi, non ci si può aspettare dagli stessi che essi procedano a «valutazioni autonome» della legalità delle informazioni in questione».
[144] Cfr. ancora per i virgolettati, le citate *Conclusioni* dell'Avvocato Generale Saugmandsgaard Øe.

Del pari problematica pare altresì la trasformazione del sistema (in costruzione) di *accountability* [145] dei fornitori di servizi digitali (che si vorrebbero istituzioni «intermedie» «*trusted and trustworthy*»[146]) in una vera e propria posizione di garanzia per eventuali illeciti commessi dagli utenti. Proprio a partire dall'esigenza di «effettività» del sistema giuridico, infatti, già i primi commentatori divisavano un simile mutamento della struttura del rimprovero penale, rilevando come il funzionamento stesso delle tecnologie informatiche e digitali faccia sì che gli autori individuali dei comportamenti illeciti siano in ogni caso «meno sensibili alla minaccia di sanzioni anche penali» rispetto a «quanto possano esserlo invece gli imprenditori e professionisti, che stabilmente forniscono accessi e servizi» [147], così dovendosi far ricadere (non tanto sui primi, quanto) su questi ultimi, per ragioni di "utilità" politico-criminale, le conseguenze negative derivanti dall'azione illecita altrui[148].

Un simile schema determinerebbe, tuttavia, un'inammissibile torsione funzionalistica del paradigma d'imputazione, che si discosterebbe dal tradizionale modello della "pura" deterrenza/prevenzione generale: invero, si chiamerebbero soggetti *diversi* dai destinatari del precetto «a rendersi partecipi della creazione dei presupposti essenziali per assicurare il rispetto del messaggio normativo» *da parte di altri*[149]. Ciò che, allora, imporrebbe (paradossalmente) di ragionare in termini di *allocazione* della responsabilità penale tra i soggetti ritenuti più atti ad assicurare il rispetto dei precetti, piuttosto che di effettiva *attribuzione* della responsabilità penale per un fatto materialmente realizzato.

[145] G. Frosio, M. Husovec, *Accountability and Responsibility of Online Intermediaries*, in *Oxford Handbook of Online Intermediary Liability,* cit., 614, nel senso che «*Responsible behaviour beyond the law finds justification in intermediaries' corporate social responsibilities and their role in implementing and fostering human rights*».

[146] J. M. Balkin, *op. cit.*, 7 ss.

[147] L. Picotti, *Fondamento e limiti della responsabilità penale dei* service-providers *in* internet, cit., 383.

[148] Cfr. ad es. F. Pasquale, A. J. Cockfield, *Beyond Instrumentalism: A Substantivist Perspective on Law, Technology, and the Digital Persona*, in *MSLR* 2018, 821 ss. e in part. 842, i quali appunto sottolineano come l'omessa considerazione degli *internet service providers* quali soggetti centrali di un nuovo panorama economico abbia drammaticamente inciso sull'inefficacia della disciplina adottata per internet.

[149] Le espressioni sono tratte da G. A. De Francesco, *Disciplina penale societaria e responsabilità degli enti: le occasioni perdute dalla politica criminale*, in *DPP* 2003, 8, 929 ss. e in part. 929, che per l'appunto le utilizzava per descrivere il diverso modello della responsabilità da reato dell'ente, con suggestioni generali che paiono tuttavia rilevanti anche nell'ambito della presente riflessione.