SISTEMA PENALE

FASCICOLO 5/2020

ISSN 2704-8098

Sistema penale (*SP*) è una rivista *online*, aggiornata quotidianamente e fascicolata mensilmente, ad accesso libero, pubblicata dal 18 novembre 2019.
La *Rivista*, realizzata con la collaborazione scientifica dell'Università degli Studi di Milano e dell'Università Bocconi di Milano, è edita da Progetto giustizia penale, associazione senza fine di lucro con sede presso il Dipartimento di Scienze Giuridiche "C. Beccaria" dell'Università degli Studi di Milano, dove pure hanno sede la direzione e la redazione centrale. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione.
La *Rivista* si uniforma agli standard internazionali definiti dal *Committe on Publication Ethics* (COPE) e fa proprie le relative linee guida.

Peer review I contributi che la direzione ritiene di destinare alla sezione "*Articoli*" del fascicolo mensile sono inviati a un revisore, individuato secondo criteri di rotazione tra i membri del Comitato scientifico, composto da esperti esterni alla direzione e al comitato editoriale. La scelta del revisore è effettuata garantendo l'assenza di conflitti di interesse. I contributi sono inviati ai revisori in forma anonima. La direzione, tramite la redazione, comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se la valutazione è positiva, il contributo è pubblicato. Se il revisore raccomanda modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se il revisore esprime parere negativo alla pubblicazione. La direzione si riserva la facoltà di pubblicare nella sezo "*Altri contributi*" una selezione di contributi diversi dagli articoli, non previamente sottoposti alla procedura di *peer review*. Di ciò è data notizia nella prima pagina della relativa sezione.
Di tutte le operazioni compiute nella procedura di *peer review* è conservata idonea documentazione presso la redazione.

Modalità di citazione Per la citazione dei contributi presenti nei fascicoli di *Sistema penale*, si consiglia di utilizzare la forma di seguito esemplificata: N. COGNOME, *Titolo del contributo*, in *Sist. pen.* (o *SP*), 1/2020, p. 5 ss.

5/2020

RESPONSABILITÀ PENALE DELL'*INTERNET SERVICE PROVIDER* E CONCORSO DEGLI ALGORITMI NEGLI ILLECITI *ONLINE*: IL CASO *FORCE* V. *FACEBOOK*

di Alice Baccin

Ogni giorno miliardi di utenti affollano il mondo virtuale e approfittano degli spazi concessi dagli internet service provider *per condividere innumerevoli contenuti, talvolta anche illeciti.*
Muovendo da un caso approdato di recente dinnanzi alle corti statunitensi – Force v. Facebook *– l'Autrice si propone di indagare se possa sussistere una responsabilità penale in capo agli* internet service provider *per la veicolazione di contenuti illeciti da parte di terzi e, in particolare, se l'uso di algoritmi di associazione e filtraggio capaci di selezionare i contributi più apprezzati e di garantirne un'enorme diffusione possa far perdere loro la tradizionale qualifica di "intermediari neutri" in favore del riconoscimento di un ruolo attivo nella commissione del reato, soprattutto alla luce dell'enorme autonomia di cui queste nuove tecnologie dispongono e dell'irrilevante ruolo dei gestori di piattaforme* online *nell'esposizione dei contenuti.*
L'analisi della sentenza darà l'impulso ad una riflessione in chiave comparatistica che non mancherà di esaminare, da ultimo, le posizioni espresse in proposito dalla giurisprudenza nostrana, nel tentativo di isolare alcune fondamentali questioni e di individuare possibili risposte.

1. La responsabilità degli *internet service provider* per i contenuti illeciti pubblicati da terzi: un quadro generale.

Una delle principali questioni con la quale il diritto penale è stato chiamato a confrontarsi negli ultimi decenni, in concomitanza con la progressiva espansione di

Internet e il suo pervasivo impiego, attiene alla configurabilità di una responsabilità penale in capo agli *internet service provider (ISP)* per i contenuti illeciti pubblicati da terzi[1].

Ogni giorno, infatti, un numero imponente di condotte penalmente rilevanti[2] si consuma *online*, in contesti – quali *social network*, forum, piattaforme dedicate o semplici siti *web* che consentono l'interazione – messi a disposizione da soggetti il cui *business* principale consiste nel creare spazi virtuali e, a carico dei quali, dottrina e giurisprudenza si sono chieste se possa sussistere una qualche forma di responsabilità, alla luce dell'effettivo contributo prestato nella diffusione di contenuti lesivi.

Nati con lo scopo di fornire un accesso alle principali reti di comunicazione elettronica e di consentire la diffusione passiva di contenuti, gli *Internet Service Providers* hanno, con il tempo, cambiato radicalmente volto, abbandonando, via via, la propria veste di "intermediari neutri" in favore di un ruolo maggiormente attivo, che si sostanzia nell'intervenire concretamente nei contenuti pubblicati dagli utenti allo scopo di aumentarne la visibilità, incrementarne le potenzialità di interazione e consentirgli maggiori *chances* di diffusione. A questo mutamento di funzione si è accompagnato, com'era inevitabile, anche un cambio di prospettiva sul piano della responsabilità, divenendo imprescindibile chiedersi se sussista a loro carico un qualche obbligo di controllo rispetto ai contenuti pubblicati da terzi e a che titolo possano essere chiamati a risponderne qualora abbiano concretamente influito nella veicolazione di materiale illecito.

Sebbene alcune parziali risposte siano giunte sul piano civile[3], lo stesso non si può dire per l'ambito penale, laddove il principale orientamento attuale tende ad

---

[1] Letteratura amplissima. Si veda, *e multis*, SIEBER U., *Responsabilità penali per la circolazione di dati nelle reti internazionali di computer. Le nuove sfide di Internet*, in *Riv. trim. dir. pen. econ.*, 1997, 3, p. 775 ss; SEMINARA S., *La responsabilità penale degli operatori su internet*, in *Dir. inform.*, 1998, 4-5, p. 745 ss; PICOTTI L., *La responsabilità penale dei service providers in Italia*, in *Dir. pen. proc.*, 1999, 4, p. 504 ss; RUGGIERO F., *Individuazione nel ciberspazio del soggetto penalmente responsabile e ruolo dell'internet provider*, in *Giur. merito,* 2001, 2, p. 586 ss.; SPAGNOLETTI V., *La responsabilità del provider per i contenuti illeciti di Internet,* in *Giur. merito*, 2004, 9, p. 1922 ss; INGRASSIA A., *Il ruolo dell'ISP nel cyberspazio: cittadino, controllore o tutore dell'ordine?* in *Dir. pen. cont.*, 8 novembre 2012; BARTOLI R., *Brevi considerazioni sulla responsabilità penale dell'internet service provider*, in *Dir. pen. proc.*, 2013, 5, pp. 600 ss.; PETRUSO R., *Responsabilità degli intermediari di Internet e nuovi obblighi di conformazione: Robo-Takedown, Policy of Termination, notice and take steps*, in *Eur. dir. priv.*, 2017, 2, p. 451 ss.; INGRASSIA A., *Responsabilità penale degli internet service provider: attualità e prospettive*, in *Dir. pen. proc.*, 2017, 12, pp. 1261 ss.

[2] Dalla diffamazione alla pedopornografia, passando per la propaganda terroristica, l'apologia di reato e i fenomeni legati al cd. *revenge porn*, sono molteplici gli illeciti penali che si consumano nel *cyberspazio* in una dimensione di totale (o quasi) anomia.

[3] Si vedano, tra gli altri: RICCIO G.M., *La responsabilità civile degli Internet providers*, Milano, Giappichelli, 2002; PARODI C., *La responsabilità dei provider e l'accertamento degli illeciti telematici*, in *Dir. pen. proc.*, 12/2002, pp. 1549 ss.; GAMBINI M. *Le responsabilità civili dell'Internet service provider*, Edizioni Scientifiche Italiane, 2006; DE CATA M., *La responsabilità civile dell'internet service provider*, Milano, Giuffré, 2010; Marucci B., *La responsabilità civile in Rete: la necessità di introdurre nuove regole*, in *www.comparazionedirittocivile.it,* fasc. 4/2014; COCUCCIO M., *La responsabilità civile per fatto illecito dell'Internet Service Provider*, in *Resp. civ. prev.,* vol. 80, fasc. 4, 2015, pp. 1312 ss.; PANETTA R., *La responsabilità civile degli internet service provider e la tutela del diritto d'autore*, in *Dir. Ind.*, 7 marzo 2017; CAMILLETTI F., *Alcune considerazioni sui profili giuridici dei social network*, in *Contratti*, 4/2017, pp. 451 ss.

escludere la punibilità per i *providers*, e deve fare i conti con una serie di dubbi circa il modello di responsabilità più adeguato da applicare[4].

La dottrina italiana, infatti, partendo dal quadro normativo offerto dal D.lgs. 70/2003[5] (di recepimento della cd. Direttiva *e-commerce*[6]) e, in particolare dagli artt. 16 e 17 ivi contenuti, ha configurato tre fondamentali modelli di responsabilità: una prima forma di rimprovero a titolo di concorso commissivo tra l'autore del contenuto lesivo e il *provider*, una seconda ipotesi incentrata sulla responsabilità da reato omissivo improprio per non aver impedito il reato altrui (art. 40 cpv. c.p.), oppure una terza via basata sul non aver adeguatamente sorvegliato sulla condotta degli utenti e dunque per non aver attuato tutte le misure necessarie a limitare le conseguenze del reato, sul modello del reato omissivo proprio[7].

La giurisprudenza di legittimità, invece, ha adottato soluzioni divergenti, dapprima escludendo la sussistenza di una posizione di garanzia in capo ai *provider* nel *leading case Google vs. Vividown*[8] e in seguito ritenendo responsabile di diffamazione il legale rappresentante di una società attiva nel settore per omesso impedimento degli *effetti* del reato, non essendosi costui adoperato per rimuovere un contenuto diffamatorio pur avendone avuto notizia[9].

---

[4] Vi sono alcune essenziali difficoltà nel muovere un rimprovero sul piano penale ad un Internet Service Provider, che si sostanziano precipuamente nel suo essere soggetto non fisico ma un'organizzazione all'interno del quale individuare un destinatario delle norme penali, e nel suo agire in un non luogo nel quale è difficile comprendere quale sia la normativa applicabile e chi abbia giurisdizione.
I possibili modelli di responsabilità oscillano tra due alternative estreme: prevedere la totale impunità dell'ISP funzionale a garantirne la libertà di espressione, e intervenire, al contrario, in modo pervasivo per prevenire qualsiasi tipo di illecito. Così INGRASSIA A., *Il ruolo dell'ISP nel cyberspazio: cittadino, controllore o tutore dell'ordine?*, cit.

[5] D.lgs. 9 aprile 2003, n. 70, "Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico". Per un commento alla normativa vedi: TESCARO M., *La responsabilità dell'internet provider nel D.lgs. 70/2003*, in *Resp. civ.*, 3/2010.

[6] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a «taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno». Per un approfondimento circa la responsabilità degli *Internet Service Provider* per come configurata dalla direttiva in esame si veda: BAISTROCCHI P., *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, in *Santa Clara Computer & High Tech L. J.*, 19(1), 2002, pp. 111-130.

[7] Per una trattazione completa sul tema vedi: SPAGNOLETTI V., *La responsabilità del provider per i contenuti illeciti di Internet*, cit.; INGRASSIA A., *Responsabilità penale degli internet service provider: attualità e prospettive*, cit.

[8] Cass. Pen., Sez. III, 17 dicembre 2013, n. 5107, commentata da INGRASSIA A., *La sentenza della Cassazione sul caso Google*, in *Dir. pen. cont.*, 6 febbraio 2014. Si veda anche SARTOR G., VIOLA DE AZEVEDO CUNHA M., *Il caso Google-Vividown tra protezione dei dati e libertà di espressione online*, in *Dir. Inform.*, fasc. 4-5, 2010, pp. 645 ss.

[9] Cass. Pen., Sez. V, 27 dicembre 2016, n. 54946. Nello specifico, la controversia era sorta dopo che il legale rappresentante della società Kines s.r.l., gerente il sito internet www.agenziacalcio.it, era stato ritenuto responsabile di concorso nel reato di diffamazione, a seguito della mancata rimozione di un articolo lesivo della reputazione del presidente della Lega Nazionale Dilettanti della Federazione Italiana Gioco Calcio; articolo di cui il gestore del sito aveva avuto notizia dall'autore stesso.
Assolto in primo grado e condannato in appello, l'imputato ha proposto ricorso per Cassazione chiedendo la riforma della sentenza per essere venuto a conoscenza del contenuto offensivo solo dopo alcuni giorni dalla pubblicazione, a diffamazione già avvenuta. Gli ermellini, tuttavia, nel ritenere il ricorso infondato hanno sposato la tesi dei giudici del gravame per «aver l'imputato mantenuto consapevolmente l'articolo

In ambito internazionale, e in particolare statunitense, la fondamentale disciplina in materia di *ISP* è rappresentata dal Titolo 47 *U.S. Code*, § 230 del 1996, che, oltre a predisporre una sostanziale immunità[10] sul piano civilistico per gli *interactive computer service*, esclude contestualmente la propria applicabilità in ambito penale[11], laddove sembrerebbe, dunque, residuare uno spazio per una eventuale responsabilità da reato anche se, di fatto non vi è, ad oggi, alcun precedente di sorta[12].

Stante una tale divergenza di opinioni, risulta evidente come si sia ben lontani dal navigare in acque chete, e assuma, anzi, decisiva rilevanza il singolo caso nel fare, di volta in volta, maggiore chiarezza. Solo un'attenta analisi della casistica giurisprudenziale, infatti, può aiutare gli interpreti ad avere contezza di come il diritto vivente si atteggi dinnanzi alla questione della responsabilità degli *ISP*, visto e considerato anche il quadro normativo oramai obsoleto e l'incidenza determinante dei processi automatizzati nelle scelte editoriali di ciascun *provider* online.

Chiunque si occupi di *social media*, ad oggi, si affida, infatti, ad algoritmi di associazione e filtraggio[13] per l'intera selezione dei contenuti mostrati e per la gran parte del controllo di quanto pubblicato, in totale assenza di una mente "umana" a presiedere le attività delle piattaforme o a sorvegliare il comportamento degli utenti.

Rimettere il monitoraggio dei contenuti al solo umano, sarebbe, invero, impensabile, essendo costui ontologicamente impossibilitato a svolgere una sorveglianza esauriente a fronte del numero spropositato di utenti attivi ogni minuto sulla rete. Come fare quindi a costruire un modello di responsabilità penale quando

---

sul sito, consentendo che lo stesso esercitasse l'efficacia diffamatoria» e come tale accresciuto l'effetto del reato.

[10] Il concetto di "immunità" è da ricondurre a quella che potremmo definire una completa esenzione di responsabilità per l'*Internet Service Provider*. L'ordinamento statunitense, infatti, esclude qualsivoglia tipo di rimprovero a carico degli intermediari *online* per i contenuti pubblicati da terzi.

[11] *Title* 47 *U.S. Code* § 230 (2)(e)(1).

[12] Se in tema di responsabilità civile, infatti, i precedenti sono molteplici, in ambito penale le Corti statunitensi non sono mai state chiamate a pronunciarsi. L'unico caso ad oggi in essere dinnanzi ad un giudice americano è il cd. *Megaupload case*, che vede in qualità di imputati, a titolo di concorso, l'*hosting provider* Megaupload e i suoi amministratori per aver ripetutamente diffuso materiale coperto dal diritto d'autore, infrangendo norme di carattere penale (*Title* 18 *U.S. Code*, § 371). La controversia, in essere oramai da qualche anno, dovrebbe andare a decisione il prossimo aprile, dopo l'ennesimo rinvio da parte della Corte della Virginia.

[13] Gli algoritmi, definibili come procedimenti che da un dato *input* portano la macchina ad un determinato *output*, possono essere suddivisi in varie categorie. Per "algoritmi di associazione" intendiamo tecnologie capaci di mettere in correlazione entità diverse, trovare un collegamento. Gli "algoritmi di filtraggio", invece, sono processi in grado di escludere o includere informazioni sulla base di criteri precedentemente identificati in fase di programmazioni. I *social media* e, più in generale, i *provider* di contenuti *online*, si avvalgono di questo genere di tecnologie per ottimizzare la propria piattaforma e attrarre un maggior numero di utenti. Gli algoritmi di associazione e filtraggio, infatti, scandagliano le preferenze di ciascun fruitore e, sulla base di queste, gli mostrano contenuti *ad hoc* che possano interessargli. Per approfondimenti sul tema, *e multis*: DOMINGOS P., *L'algoritmo definitivo. La macchina che impara da sola e il futuro del nostro mondo,* Milano, Bollati Boringhieri, 2015; DIAKOPOULOS N., *Algorithmic Accountability Reporting: On the Investigation of Black Boxes*, in *Columbia Journalism School*, p. 3, 2014.

progressivamente scompaia l'umano (rimproverabile quantomeno a titolo di colpa) e residui solo la macchina?

Ad affrontare per primo in modo esauriente la questione è stato l'ordinamento statunitense e, in particolare la *United States Court of Appeal* dello Stato di New York, con il celebre caso *Force v. Facebook*[14], uno dei più discussi arresti giurisprudenziali recenti che ha visto, in qualità di convenuto, il social network di Mark Zuckerberg accusato di aver concorso con Hamas nella realizzazione di alcuni attentati terroristici in Israele nei quali persero la vita dei cittadini americani[15].

Il *complaint* attoreo, infatti, introduce per la prima volta la questione delle scelte algoritmiche nascoste dietro la piattaforma, e propone di riconsiderare il ruolo tradizionalmente riconosciuto a Facebook di intermediario neutro alla luce dell'attività di manipolazione dei contenuti che esso effettuerebbe proprio in virtù di processi automatizzati.

Rigettate in primo e secondo grado, le tesi di parte attrice hanno condotto i giudici di New York ad una sentenza senza dubbio meritevole di approfondimento, sia per la riflessione riguardante il contributo causale apportato dagli algoritmi, sia per la *dissenting opinion* resa da uno dei componenti del collegio, utile in chiave comparatistica per confrontare il nostro modello di responsabilità degli *ISP* con l'immunità invece riconosciutagli nel sistema statunitense, soprattutto alla luce della nozione *hosting provider* attivo applicabile ai *social network*, forse, anche sul piano penale.

2. I fatti e le allegazioni di parte nel processo dinnanzi alla *District Court of New York*.

I fatti oggetto di causa si collocano tutti tra il 2014 e il 2016 e vedono coinvolti cinque cittadini americani rimasti uccisi nel corso di svariati attacchi terroristici perpetrati da Hamas, la nota organizzazione islamista palestinese, in territorio israeliano[16].

---

[14] *Force v. Facebook, Inc.* No. 18-397 (2nd Cir. 2019). Il testo della sentenza è disponibile online al seguente *link*.

[15] Il legame tra le attività legate al terrorismo e l'uso dei *social media* è un argomento tutt'altro che nuovo e vi sono molteplici precedenti analoghi al caso *Force v. Facebook.* La critica principale che viene mossa alle piattaforme *online* riguarda la facilità con cui le organizzazioni terroristiche reperiscono uomini e mezzi tramite i contatti realizzati in rete e la facilità con cui diffondono i propri contenuti senza incontrare alcun ostacolo. Per un approfondimento sul tema, *e multis*: MARCU M., BALTEANU C., *Social media – A Real Source of Proliferation of International Terrorism*, in *Annales Universitas Apulensis Series Oeconomica* 16(1), 2014, pp. 162-169; WEIMANN G., *Terrorist Migration on Social Media*, in *Geo. J. Int'l Aff.*, 16(1), 2015, pp., 180-187; GATES S., PODDER S., *Social media, Recruitment, Allegiance and the Islamic State*, in *Perspectives on Terrorism*, 9(4), 2015, pp. 107-116; BERTRAM L., *Terrorism, the Internet and the Social Media Advantage: Exploring how terrorist organizations exploit aspects of the internet, social media and how these same platforms could be used to counter-violent extremism.*, in *Journal of Deradicalization*, n. 7, 2016, pp. 225-252; WEIMANN G., *The Emerging Role of Social Media in the Recruitment of Foreign Fighters*, in de Guttry A., Capone F., Paulussen C., *Foreign Fighters under International Law and Beyond*, Springer, 2016, pp. 77-95; TSESIS A., *Social Media Accountability for Terrorist Propaganda*, in *Fordham L. Rev.*, 86 (2), 2017, pp. 605-631.

[16] Si tratta di Yakov Naftali Fraenkel, un *teenager* rapito dagli uomini di Hamas al ritorno da scuola e successivamente ucciso a colpi di pistola a Gush Etzion; Chaya Zissel Braun, neonata di 3 mesi travolta da

A seguito degli attacchi, l'unico superstite e i parenti delle vittime intraprendono un'azione legale dinnanzi alla *District Court* dello Stato di New York, intenzionati a dimostrare la corresponsabilità del noto *social network* Facebook per aver favorito gli attentatori, consentendo ad Hamas di mantenere la propria pagina, di veicolare messaggi che istigassero al compimento di azioni violente e facilitandogli il reclutamento di eventuali cellule terroristiche grazie ai collegamenti spontaneamente creati dal sito tra l'organizzazione e una platea di possibili simpatizzanti altrimenti non raggiungibili.

Stando a quanto riportato dalle parti attrici, infatti, le modalità di attacco utilizzate dagli aggressori in danno delle vittime rispecchierebbero quelle suggerite da alcuni *post* pubblicati da Hamas nei giorni precedenti i fatti, i quali avrebbero incoraggiato i terroristi ad agire seguendo un preciso schema o a colpire determinati soggetti *target*[17].

Secondo le ricostruzioni degli attori, quindi, Facebook sarebbe responsabile ai sensi dell'*Anti Terrorism Act (ATA)* – le cui norme sono racchiuse nel Titolo 18 *U.S. Code* § 2333[18], § 2339A[19] e § 2339B[20] – per avere consapevolmente concorso con Hamas nella

---

un'automobile scagliatasi contro la folla in una stazione a Gerusalemme; Richard Lakin, dapprima colpito con un'arma da fuoco e, successivamente, finito a coltellate durante un'incursione di Hamas in un autobus a Gerusalemme; Taylor Force, studente pugnalato mentre passeggiava sul lungomare di Tel Aviv e Menachem Mendel Rivkin, pugnalato al collo da un esponente di Hamas mentre si recava in un ristorante nei pressi di Gerusalemme, unico sopravvissuto nonostante le gravissime ferite riportate.

[17] Ad esempio, una delle vittime sarebbe stata rapita e uccisa in seguito alla pubblicazione di un *post* nel quale Hamas incitava al rapimento di soldati israeliani (probabilmente confusa per un possibile appartenente alle forze armate); un'altra sarebbe rimasta vittima di un'automobile impazzita lanciatasi contro la folla dopo la comparsa di un *post* inneggiante l'uccisione di israeliani mediante l'utilizzo di veicoli, e ancora, uno dei *killer* sarebbe stato un utente abituale del *social network* invogliato da alcuni *post* in tema di accoltellamenti casuali.

[18] Il Titolo 18 *U.S. Code* §2333(d)(2) disciplina la responsabilità civile della persona *"who aids and abets, by knowingly providing substantial assistance, or who conspires with the person who committed such an act of international terrorism"*, riconoscendo all'offeso o ai suoi eredi la possibilità di esercitare un'azione per ottenere il risarcimento del danno.

[19] Il Titolo 18 *U.S. Code* § 2339A, rubricato "*Providing material support to terrorists*" sancisce che: "*Whoever provides material support or resources or conceals or disguises the nature, location, source, or ownership of material support or resources, knowing or intending that they are to be used in preparation for, or in carrying out, a violation of section 32, 37, 81, 175, 229, 351, 831, 842(m) or (n), 844(f) or (i), 930(c), 956, 1091, 1114, 1116, 1203, 1361, 1362, 1363, 1366, 1751, 1992, 2155, 2156, 2280, 2281, 2332, 2332a, 2332b, 2332f, 2340A, or 2442 of this title, section 236 of the Atomic Energy Act of 1954 (42 U.S.C. 2284), section 46502 or 60123(b) of title 49, or any offense listed in section 2332b(g)(5)(B) (except for sections 2339A and 2339B) or in preparation for, or in carrying out, the concealment of an escape from the commission of any such violation, or attempts or conspires to do such an act, shall be fined under this title, imprisoned not more than 15 years, or both, and, if the death of any person results, shall be imprisoned for any term of years or for life. A violation of this section may be prosecuted in any Federal judicial district in which the underlying offense was committed, or in any other Federal judicial district as provided by law.*"

[20] *Title* 18 *U.S. Code* § 2339B, rubricato: *"Providing material support or resources to a designated foreign terrorist organization"* si colloca a completamento della *section* precedente disciplinando la responsabilità penale di chiunque fornisca supporto materiale o risorse ad un'organizzazione terroristica estera. Per un commento alla normativa in esame si vedano, *e multis*: JONAKAIT R.N., *A Double Due Process Denial: The Crime of Providing Material Support or Resources to Designated Foreign Terrorists Organizations,* in *N. Y. L. Sch. L. Rev.*, 48(1)(2), 2003-2004, pp. 125-172; COMERFORD B.P., *Preventing Terrorism by Prosecuting Material Support*, in *Notre Dame*

realizzazione degli attacchi terroristici senza mai intervenire con la censura (la pagina di Hamas è pubblica, chiunque può accedervi senza incontrare alcun tipo di "schermo") o impedire che i *post* incriminati venissero indirizzati ad eventuali simpatizzanti.

Il titolo 18 *U.S. Code*, sezione 2339 punisce, infatti, chiunque fornisca un supporto materiale a terzi o comunque agevoli la commissione, tra gli altri, di atti di terrorismo, intendendo per "supporto" non solo e non tanto il sostegno finanziario, il rifornimento di armi e munizioni o l'appoggio logistico, ma anche eventuali consigli o assistenza tecnica; qualsiasi «sostegno tangibile o intagibile o servizio»[21] che qualcheduno fornisca all'autore di un atto di violenza rivolto contro più soggetti, contro membri del Congresso o contro beni appartenenti al patrimonio federale[22].

Nell'ottica della norma, dunque, il fatto che Facebook abbia mantenuto la presenza di centinaia di *accounts* utilizzati da Hamas o riconducibili ai suoi membri e a vari gruppi affiliati, non solo avrebbe di gran lunga facilitato all'organizzazione la diffusione delle proprie idee ma avrebbe anche favorito la raccolta di uomini e mezzi in vista degli attacchi, contribuendo attivamente alla loro realizzazione con un effettivo sostegno[23].

Gli unici sforzi messi in atto dal *social network* per impedire il proliferare di Hamas, riportano gli attori, si sarebbero concretizzati nella sospensione degli *accounts* ad esso riconducibili per qualche tempo, e nel fare in modo che le pagine non fossero visibili in Israele, mancando totalmente l'adozione di misure più drastiche e realmente idonee a tacitare per sempre questo genere di pubblicazioni.

L. Rev., 80(2), gennaio 2005, pp. 723-758; SAID W.E., *The Material Support Prosecution and Foreign Policy*, in *Ind. L. J.*, 86(2), 2011, pp. 543-594; HELTON J.E., *Construction of a Terrorist under the Material Support Statute 18 U.S.C. Sec. 2339B*, in *Am. U. L. Rev.*, 67(2), dicembre 2017, pp. 553-602.

[21] DOYLE C., *Terrorist Material Support: An overview of 18 U.S. Code § 2339A and § 2339B*, in *CRS Report*, 8 dicembre 2016, *Congressional Research Service*. Si veda anche: ABRAMS N., *The Material Support Terrorism Offenses: Perspectives Derived from the (Early) Model Penal Code*, in *J. Nat'l Security L. & Pol'y*, 1(1), 15 giugno 2005, pp. 5-35.

[22] Non solo i reati di terrorismo sono ricompresi nell'elenco delle fattispecie presupposto della sezione 2339, vi rientrano anche: l'utilizzo di armi chimiche, l'aggressione, il rapimento o l'uccisione di membri del Congresso, operazioni coinvolgenti materiale nucleare, genocidio, distruzione di beni appartenenti al patrimonio federale, l'esplosione di una bomba in una proprietà federale, l'aggressione o l'assassinio di un connazionale statunitense all'estero e altre fattispecie aventi per oggetto una diversità di beni giuridici tutelati.

[23] A riportarlo è il *complaint* presentato dalle parti attrici dinnanzi alla *United States District Court, Southern District of New York*, sec. II (B) – *section* "*Hamas and Facebook*", punto 72, p. 16. La struttura dell'atto introduttivo del giudizio contempla un'attenta analisi dell'utilizzo di Facebook da parte di Hamas soffermandosi sulla descrizione degli *account* ad esso riconducibili, elencando i nomi dei soggetti riferibili all'organizzazione dotati di un proprio profilo e spiegando accuratamente tutte le potenzialità comunicative insite nel *social network*, e come esse siano ampiamente valorizzate dal consapevole uso che i terroristi ne fanno quotidianamente. Il *complaint* è disponibile al seguente *link*. Il titolo 18 *U.S. Code* § 2339 (a) (b) non è nuovo a questo genere di usi, spesso infatti funge da base legale per *complaint* analoghi a quello in esame; si vedano, in proposito: KNOX E.G., *The Slippery Slopes of Material Support Prosecutions: Social Media Support to Terrorists*, in *Hastings L. J.*, 66(1), dicembre 2014, pp. 295-330; BROWN N.I., *Fight Terror, Not Twitter: Insulating Social Media from Material Support Claims*, in *Loy. L. A. Ent. Rev.*, 37(1), 2016, pp. 1-51; FELTNER K.A., *Swipe Rights for ISIS: Social Media and Material Support to Foreign Terrorist Organization*, in *B. U. Pub. Int. L. J.*, 26(1), 2017, pp. 95-114.

Affermano gli attori: «*Indeed, upon information and belief, Facebook regularly monitors its website for pornographic materials which are removed immediately. […] However, Facebook has refused to actively monitor its online social media network to block HAMAS's use of Facebook. […] Instead, Facebook knowingly permits HAMAS to use its online social media platform, and only reviews HAMAS's use Facebook in response to third party complaint*»[24], provvedendo alla rimozione di singoli *post* individualmente segnalati come offensivi e ritenendo quanto pubblicato, in linea di massima, conforme alla propria *policy*.

Nonostante la suggestiva e articolata costruzione della pretesa, il *complaint* attoreo non ha trovato, in primo grado, alcun accoglimento. Il giudice investito della questione, infatti, ha escluso che si potesse parlare di responsabilità di Facebook sulla base di quella fondamentale norma – il Titolo 47 *U.S. Code* § 230(c)(1)[25] – che impedisce l'attribuzione della responsabilità civile in capo ai cd. *interactive computer service* per quanto pubblicato da altri *information content provider* e ha provveduto a rigettare la domanda[26].

La disposizione in esame, infatti, interviene instaurando un regime particolare di esenzione da qualsiasi forma di responsabilità per ogni sito *web* o piattaforma *online* in riferimento ai contenuti pubblicati da parti terze al suo interno, e offre una copertura completa ai *provider* trattandoli alla stregua di meri editori.

3. I motivi di appello.

Terminato il processo di primo grado, gli attori hanno impugnato la sentenza dinnanzi all'organo giurisdizionale successivo, la *United States Court of Appeal for the Second Circuit* dello Stato di New York, chiedendo una completa revisione della sentenza, sia sul piano sostanziale che su quello processuale.

A viziare la decisione della *District Court* sarebbe, sostengono i parenti delle vittime, un'erronea applicazione del Titolo 47 *U.S. Code* § 230(c)(1), avendo la Corte frainteso completamente il ruolo giocato da Facebook (definito "intermediario neutro" dalla sentenza) e non avendo considerato l'effettivo sostegno dato ad Hamas. In particolare, secondo gli attori, ad apportare un fondamentale contributo causale nelle stragi sarebbero stati gli algoritmi di sistema utilizzati dal *social network*, capaci di veicolare messaggi di odio e violenza e di mettere in relazione il profilo dei terroristi con una vastissima schiera di potenziali seguaci.

Inoltre, Facebook non avrebbe nemmeno attuato tutte le strategie necessarie a rimuovere i contenuti di Hamas, limitandosi ad intervenire solo su alcuni *post* o ponendo

---

[24] *Complaint*, section IV(C), *"Facebook Has the Ability to Monitor and Block Use of Facebook by Hamas"*, punti 284-286, p. 52.

[25] La disposizione in esame, di centrale importanza per la questione in esame, recita: *"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"*.

[26] Per le motivazioni della sentenza resa dalla *District Court* si veda *Force v. Facebook*, 18-397 (2nd Cir. 2019), pp. 19 ss.

in essere misure blande e infruttuose (argomentazione con la quale gli attori riprendono quanto lamentato in primo grado).

Da ultimo, sostengono le parti attrici, anche a voler ritenere concretamente applicabile la §230 (c)(1) sul piano delle pretese civilistiche, rimarrebbe comunque uno spazio per la responsabilità penale della piattaforma di Zuckerberg in virtù di un'espressa previsione contenuta nella stessa norma. La section 230 (e)(1) stabilisce, infatti, che *nothing in this section shall be construed to impair the enforcement of […] any other Federal criminal statute"*, impedendo, quindi, che l'*affirmative defence* contenuta alla lettera C (1) possa evitare la persecuzione dei reati previsti dal Titolo 18 *U.S. Code* § 2333 (quindi delle norme contenute nel *Anti-Terrorism Act – ATA*) e dal cd. *JASTA (Justice Against Sponsors of Terrorism Act)*.

4. La sentenza di appello.

Lungi dall'essere in qualche modo satisfattivo, il giudizio di appello (terminato nell'estate del 2019) ha visto gli attori soccombere nuovamente, avendo i giudici del collegio confermato in toto l'applicazione della *section* 230 per come correttamente intesa dalla Corte distrettuale, peraltro in piena conformità ad una serie di esperienze giudiziali analoghe vertenti sullo stesso tema[27].

Force v. Facebook, infatti, è solo l'ultimo della nutrita schiera di precedenti[28] che ha visto i principali social network e, più in generale, le maggiori piattaforme *online*, essere chiamati a rispondere di concorso in azioni terroristiche davanti alle autorità statunitensi; esperienze conclusesi in tutti i casi con il rigetto delle domande attoree per sostanziale inconsistenza delle premesse e per il riconoscimento dell'immunità ai sensi della § 230.

---

[27] Si veda, in proposito: TATE E. B., *Maybe Someone Dies: The Dilemma of Domestic Terrorism and Internet Edge Provider Liability*, in *B. C. L. Rev.*, 60(6), 2019, pp. 1731-1770.

[28] Nel corso del presente paragrafo chi scrive si soffermerà sui due più rilevanti – *Fields v. Twitter* e *Cohen v. Facebook* – ma è doveroso riportare qui anche alcuni altri casi che hanno visto coinvolti i principali *social network* per concorso in azioni terroristiche.
Ancora in fase di decisione è *Cain e Gonzalez v. Twitter*, 17 Civ. 122 (PAC) (S.D.N.Y. Apr. 25, 2017), nel quale la moglie di Alex Pinczowsky, vittima insieme alla sorella Sacha di un attacco terroristico avvenuto all'aeroporto di Bruxelles, e la madre di di Nohemi Gonzalez (anch'essa uccisa nell'attacco) hanno intrapreso un'azione civile dinanzi alla District Court di New York contro Twitter. È curioso come la causa sia ancora in decisione a causa di un disaccordo in merito alla competenza del giudice adito, dovuto al fatto che il padre della ragazza aveva precedentemente cominciato, all'insaputa della moglie, una causa presso una Corte californiana – *Reynaldo Gonzalez v. Twitter Inc., Google Inc. e Facebook Inc.* – vertente sullo stesso oggetto e i due giudizi sono stati lì riuniti in attesa di andare a sentenza.
Il testo del *complaint* di *Cain e Gonzalez v. Twitter* è disponibile a questo *link*.
Del 2019 è invece *Palmucci v. Twitter*, 18-cv-03947-WHO (N.D. Cal. Apr. 17, 2019), controversia scaturita dal *complaint* di una donna rimasta ferita in un attentato terroristico a Parigi e rigettato in toto dalla *Northern District Court of California* decisa a conformarsi agli ormai numerosi precedenti che sanciscono l'immunità degli intermediari digitali.
Il testo della sentenza è disponibile a questo *link*.

Risale al 2016, ad esempio, il caso *Fields v. Twitter*, nel quale il noto social network è stato convenuto in giudizio per aver fornito supporto materiale all'ISIS nell'uccisione di due cittadini americani ad Amman, in Giordania.

Analogamente a quanto accaduto per *Force v. Facebook*[29], la parte attrice impostò il proprio *complaint*[30], dapprima, sul Titolo 18 *U.S. Code* § 2339 (a) e (b) e, una volta ottenuto il rigetto ai sensi del Titolo 47 *U.S. Code* § 230(c)(1), sul ruolo che Twitter avrebbe avuto concedendo agli esponenti dello Stato Islamico di creare un account dedicato, travalicando le proprie funzioni di editore di contenuti e fornendo un vero e proprio sostegno[31]. A detta dell'attore, infatti, la pubblicazione di contenuti da parte di un gruppo di terroristi sarebbe stata del tutto estranea alla *ratio* di tutela della libertà di espressione offerta dalla § 230, risultando Twitter un vero e proprio divulgatore di materiale pericoloso.

La *United States District Court, Northern District of California*[32], investita del caso, rigettò la domanda nel merito riconoscendo la natura di "*content neutral*" di Twitter e ritenendo che non fosse stato in alcun modo provato il nesso di causalità intercorrente tra la concessione in utilizzo di un *account* da parte di Twitter e l'attacco subito dai due cittadini americani. Sostenne, inoltre, che non si potesse in alcun modo parlare di supporto fornito dal *social network* all'ISIS, dato l'amplissimo impiego che ne viene quotidianamente fatto anche da utenti di natura diversa. Se è vero, infatti, che esso permette ai terroristi di veicolare i propri messaggi, è altresì vero che consente anche a centinaia di migliaia di altri individui di postare ogni giorno i più svariati contenuti, dimodoché ritenerlo uno strumento nelle mani dell'ISIS significherebbe fraintenderne lo scopo, oltre che addossargli una responsabilità inesistente.

Per di più, affermò la Corte, ritenere che la libertà di espressione garantita dalla *section* 230 passi per l'imposizione ai social network di alcuni vincoli di carattere censorio (quali ad esempio l'adozione di *policies* che rimuovano sistematicamente ciascun contenuto potenzialmente offensivo) significherebbe esorbitare rispetto ai confini della norma stessa, riconoscendole dei limiti che essa non pone e correndo il rischio che i *provider* riducano i servizi forniti o addirittura li eliminino totalmente[33].

Controversia affine per oggetto a quelle sinora considerate (e in particolare a *Force v. Facebook*, al punto da essere stata trattata congiuntamente dalla corte distrettuale) fu anche il caso *Cohen v. Facebook*, che portò davanti alla giustizia statunitense il *complaint* di 20.000 israeliani intenzionati ad ottenere una condanna di Facebook per avere, quest'ultimo, contribuito a farli vivere in un clima di costante minaccia per la propria incolumità personale, essendo costoro continuo bersaglio di potenziali attacchi da parte dei terroristi palestinesi.

---

[29] Per un commento: WITTES B., BEDELL Z., *Did Congress Immunize Twitter Against Lawsuits for Supporting ISIS?*, in *Lawfareblog.com*, 22 gennaio 2016.

[30] Il testo del *First Amended Complaint* è consultabile qui.

[31] Qui il testo del *Second Amended Complaint*.

[32] La sentenza di rigetto del *Second Amended Complaint* è disponibile al seguente *link*.

[33] Goldman E., *Twitter Defeats ISIS "Material Support" Lawsuit Again–Fields v. Twitter*, in *Technology e Marketing Law Blog*, 21 novembre 2016.

In linea con quanto sostenuto nel *complaint* di *Force v. Facebook* infatti, l'uso di Facebook avrebbe permesso ai terroristi di raccogliere seguaci più agilmente, e avrebbe aumentato le *chances* degli attori di poter essere rapiti e uccisi a causa della continua propaganda *online* di odio e istigazione alla violenza.

La sentenza[34] resa dalla Corte distrettuale anche in quest'ultimo caso rigettò il *complaint* presentato dalle parti, ritenendo che le doglianze proposte fossero caratterizzate da una molteplicità di salti logici e si sostanziassero, essenzialmente, in un insieme di congetture. Le vittime, infatti, intendevano dimostrare il coinvolgimento di Facebook in attacchi terroristici ancora non avvenuti e nei quali supponevano di rimanere coinvolte prima ancora che si verificassero, dimostrando, peraltro, come non fosse in alcun modo possibile attestare l'esistenza di un'effettiva correlazione tra l'attività del *social network* e l'aumento del rischio di azioni violente da parte dei terroristi e figurando questa possibilità unicamente come una supposizione[35].

5. La fattispecie applicabile: *Title 47 U.S. Code §230 (Community Decency Act, 1996)* e l'impunità per i *provider* di un *interactive computer service*.

Al fine di comprendere al meglio le motivazioni con le quali le Corti statunitensi rigettano sistematicamente questo genere di pretese, nondimeno in *Force v. Facebook*, è necessario un breve approfondimento in merito a contenuto e portata applicativa del *Title* 47 *U.S. Code* § 230(c)(1)[36], ovverosia quella norma che non consente alcuno spazio per la responsabilità degli *interactive computer services* in riferimento a quanto pubblicato da terze parti e che rappresenta un *unicum* dell'ordinamento statunitense[37].

La *section* 230 – rubricata *Protection for private blocking and screening of offensive material* – si colloca nella più ampia cornice del *Communication Decency Act (CDA)* redatto dal Congresso nel 1996, che integra il primo tentativo sia di regolamentazione della circolazione del materiale pornografico *online*, sia di protezione dei minori da contenuti sessualmente espliciti rinvenibili in rete.

Volto a sanzionare usi distorti di *Internet*, il CDA contemperava in sé la duplice esigenza di apporre un freno ad un uso deviato della rete e di mantenerne, al contempo la più ampia libertà, rifiutandosi di intervenire eccessivamente o di inibirne le potenzialità di sviluppo con pesanti ingerenze del potere politico. Fu proprio

---

[34] Disponibile a questo *link*.

[35] Per un confronto tra le argomentazioni della Corte nei due casi *Cohen v. Facebook* e *Force v. Facebook* vedi: SPIVAK R., *Facebook Immune from Liability Based on Third-Party Content*, in *Lawfare*, 23 marzo 2017.

[36] Peraltro, è la stessa Corte a procedere ad una compiuta analisi della disposizione riportandone genesi normativa e interpretazione corrente. Vedi: *Force v. Facebook, Inc.* No. 18-397 (2nd Cir. 2019), pp. 23 ss.

[37] Una disposizione di analogo contenuto non esiste in alcun altro ordinamento al mondo. Gli USA – da sempre particolarmente sensibili alla tutela della libertà di espressione e di iniziativa economica – sono finora i primi e gli unici ad averla introdotta (soprattutto per la massiccia presenza di *companies* attive nel settore all'interno del proprio territorio) e risultano una sorta di "paradiso normativo" per chi voglia intraprendere questo genere di attività.

quest'ultima necessità a far sorgere l'esigenza di inserire la §230: un'*affirmative defense*[38] finalizzata ad evitare che il *provider* o lo *user* di un *interactive computer service* potessero essere ritenuti l'editore (*publisher*) o il divulgatore *(speaker*) delle informazioni pubblicate dagli *information content provider* e a proteggerli, dunque, da qualsiasi attribuzione di responsabilità[39].

Ratio della norma è, quindi, evitare qualsiasi accostamento tra il l'intermediario digitale e quanto venga pubblicato nel suo sito da un soggetto terzo, impedendo che venga ritenuto corresponsabile per quanto divulgato o addirittura "complice" alle idee sostenute. Ciascun *provider* è (e deve rimanere) un semplice fornitore, il concedente di uno spazio in rete nel quale sia possibile pubblicare svariati contenuti, senza che si debba, per ciò stesso, accusarlo di propaganda o trasformarlo in un predicatore intenzionale di quanto diffuso da terzi.

«*It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress…chose to immunize service providers to avoid any such restrictive effect*»[40].

L'opportunità di inserire una simile previsione nel CDA non è, tuttavia, da ricondursi unicamente alla volontà del Congresso di mantenere la libertà di espressione degli operatori *online*, ma deve imputarsi anche alla necessità di risolvere un contrasto giurisprudenziale sorto negli Stati Uniti agli inizi degli anni '90, e puntualmente ripreso dalla *Court of Appeal* di *Force v. Facebook* nella sua disamina in tema di § 230.

All'atto della promulgazione, infatti, esistevano due precedenti discordanti in tema di responsabilità dell'*information content provider*, i quali risolvevano in modo diametralmente opposto la questione concernente la responsabilità degli operatori *online* per i contenuti pubblicati da terze parti, rendendo estremamente complessa la definizione di questioni analoghe.

Il primo precedente – *Cubby, Inc. v. Compuserve, Inc.*[41] – aveva visto, nel 1991, la *District Court* di New York assolvere dall'accusa di diffamazione il *provider* titolare di un

---

[38] Nel sistema di *common law* con "*affirmative defense*" si intende una disposizione che consente all'imputato (o al convenuto, se in processo civile) di andare esente da responsabilità anche qualora sia effettivamente l'autore di un illecito. Difficilmente inquadrabile nel nostro sistema, il concetto di *affirmative defense* potrebbe essere (forse) riconducibile a quello di scriminante, ma sarebbe comunque imprecisa come analogia essendo, quello delle cause di giustificazione, un istituto meramente penalistico nell'ordinamento italiano e la difficoltà di trovare un esatto corrispondente.

[39] Si vedano, in proposito, ROSENFELD S., *The CDA as A Safe Harbor for Interactive Computer Service Providers*, in *L. A. Law*, 36(8), novembre 2013, pp. 13-17; CECIL A. L., *Taking Back the Internet: Imposing Civil Liability on Interactive Computer Services in an Attempt to Provide an Adequate Remedy to Victims of Nonconsensual Pornography*, in *Wash. & Lee L. Rev.*, 71(4), 2014, pp. 2513-2556.

[40] *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997), citato in *Force v. Facebook*, No. 18-397 (2nd Cir. 2019), p. 25 con nota di PANTAZIS A., *Zeran V. America Online, Inc.: Insulating Internet Service Providers from Defamation Liability*, in *Wake Forest L. Rev.*, 34(2), 1999, pp. 531-566.

[41] *Cubby, Inc. v. Compuserve, Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991) con note di SASSAN A. J., *Cubby Inc. v. Compuserve Inc.: Comparing Apples to Oranges: The Need for a New Media Classification*, in *Software L. J.*, 5(4), dicembre 1992, pp. 821-844; CONNER D. J., *Cubby v. Compuserve, Defamation Law on the Electronic Frontier*, in

forum online per contenuti ivi pubblicati da una società terza. La decisione si fondava sull'idea che questo genere di soggetti non potesse esercitare un controllo su tutto il materiale condiviso e, anzi, andasse ritenuto esente da responsabilità al pari di un *bookstore* o di una biblioteca che raccolgono volumi e opere di qualsiasi genere senza per questo essere ritenuti corresponsabili di quanto scritto.

Il secondo precedente del 1995, invece, affrontava nuovamente la tematica della responsabilità degli *ISP* con riferimento a *Prodigy Services Co.*, un *provider* di svariati servizi *online* accusato di diffamazione a seguito di un *post*, comparso nella propria piattaforma, nel quale l'autore insinuava la tenuta di condotte fraudolente da parte di vertici della nota società di brokeraggio Stratton Oakmont[42].

Ad esito del giudizio, diversamente da quanto accaduto nel caso precedente, la *Supreme Court di New York* ritenne *Prodigy* responsabile, in virtù del controllo che essa provvedeva ad effettuare, sulla base della propria *policy*, su ciascun contenuto pubblicato. La scelta di supervisionare quanto pubblicato, infatti, avrebbe messo la società in una posizione del tutto diversa rispetto a *Compuserve Inc.*, poiché avrebbe le avrebbe consentito di avvedersi dei contenuti offensivi e di intervenire tempestivamente per rimuoverli; operazione, invece, non eseguita.

L'introduzione della §230, optando per la totale immunità degli *interactive computer services* finì per porre fine al contrasto, effettuando una sorta di *overruling* rispetto a *Stratton Oakmont, Inc. v. Prodigy Servs Co*. e regolando in via definitiva il tema della responsabilità degli *internet service provider*.

Al fine di rendere esplicito quali fossero i soggetti beneficiari dell'immunità, inoltre, il Congresso optò per riservare una specifica parte dello spazio normativo della *section* – § 230 (C)(f) – alle definizioni, esplicitando cosa si debba intendere per *interactive computer service* e *information content provider*.

Con *interactive computer service*[43] - chiarisce infatti la disposizione – si intendono tutti i servizi di informazione[44] o i *provider* di *software*[45] che forniscano o abilitino l'accesso da parte di una molteplicità di utenti ad un *server*, includendo nella nozione anche

---

Geo. Mason Indep. L. Rev., 2(1), 1993, pp. 227-248.

[42] *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, No. 31063794, 1995, WL 323710 (N.Y. Sup. Ct. May 24, 1995). v

[43] 47 U.S. Code § 230 (C)(f)(2) con note di MIRANDA D. P., *Defamation in Cyberspace: Stratton Oakmont, Inc. v. Prodigy Services Co.*, in *Alb. L. J. Sci. & Tech.*, 5(2), 1996, pp. 229-248; JOHNSON R. H. JR., *Defamation in Cyberspace: A Court Takes a Wrong Turn on the Information Superhighway in Stratton Oakmont, Inc. v. Prodigy Services Co.*, in *Ark. L. Rev.*, 49(3), 1996-1997, pp. 589-624. In merito al rapporto tra *Cubby, Inc. v. Compuserve, Inc.* e la sentenza in esame si veda: SIDERITS M. C., *Defamation in Cyberspace: Reconciling Cubby, Inc. v. Compuserve, Inc. and Stratton Oakmont v. Prodigy Services Co.*, in *Marq. L. Rev.*, 79(4), 1996, pp. 1065-1082.

[44] Il concetto di "servizi di informazione" viene a sua volta chiarito dal Titolo 47 *U.S. Code* § 153 (24), il quale chiarisce come si tratti di servizi che offrano la possibilità di generare, acquisire, catalogare, trasformare, processare, recuperare, utilizzare o rendere disponibili informazioni tramite la pubblicazione elettronica. Nella nozione non vanno in alcun modo ricomprese, per espressa previsione della norma in esame, le compagnie attive nel settore della telecomunicazione.

[45] La § 230 (C)(f)(2) parla di *access software provider*, definendoli al punto 4 come i *providers* di *software* (*client* o *software*) o coloro i quali forniscano strumenti che permettano: (a) di filtrare, selezionare, permettere o bloccare contenuti; (b) di scegliere, individuare, analizzare o classificare contenuti o (c) trasmettere, ricevere, mostrare, inoltrare, nascondere, cercare, organizzare, riorganizzare o tradurre contenuti.

servizi e sistemi che consentano di accedere ad *Internet* e quelli utilizzati in biblioteche o istituti scolastici e universitari.

Con *information content provider*[46], invece, si fa riferimento a ciascuna persona o ente che sia responsabile, in tutto o in parte, della creazione e dello sviluppo di informazioni veicolate mediante *internet* o qualsiasi altro *interactive computer service*.

Facebook, agendo da intermediario che fornisce l'accesso ad un *server* o comunque ad uno spazio *online* ad una varietà più o meno ampia di utenti, rientra ampiamente nel significato della prima definizione, sebbene la *ratio* in origine posta a fondamento della *section* 230 non fosse in alcun modo riconducibile ai *social media* e si concentrasse, piuttosto, nella prevenzione della diffusione di contenuti osceni a danno dei minori.

6. L'applicabilità del Titolo *47 U.S. Code* § 230 a Facebook nel caso di specie: la nozione di *publisher*.

L'interpretazione della § 230 volge, dunque, al più assoluto garantismo nei confronti degli *interactive computer service*, scriminandone il comportamento in tutti i casi nei quali i contenuti postati provengano da terze parti.

Gli attori di *Force v. Facebook*, tuttavia, escludono che il *social network* di Zuckerberg possa essere ritenuto tale e sostengono, anche in sede di appello, che la sua attività non consista affatto in una semplice pubblicazione di informazioni altrui, ma si concretizzi in una vera e propria manipolazione delle stesse, al fine di ampliarne la visibilità e dare vita ad interazioni tra utenti, anche grazie all'impiego di algoritmi di associazione.

La Corte, posta dinnanzi ad una possibile erronea applicazione della norma da parte dei giudici di primo grado, procede ad una autonoma riflessione sulla natura di Facebook e sul precetto in esame, proponendo quello che viene definito un «*test* tripartito»[47] e arrivando a dimostrare per gradi l'opportunità di ritenere il *social network* immune.

Volendo analizzare compiutamente il testo della § 230 (c)(1) tre sono, infatti, le situazioni nelle quali essa risulta applicabile ed esclude la responsabilità civile[48]:

1) Quando si sia in presenza di un *provider* o *user* di un *interactive computer service* per come definito dalla disposizione stessa.

2) Qualora le allegazioni della parte attrice trattino il convenuto come *publisher* o *speaker* dell'informazione al centro della controversia.

3) Quando l'informazione sia stata condivisa da un *information content provider* altro rispetto all'*interactive computer service*.

---

[46] 47 *U.S. Code* § 230 (C)(f)(3).

[47] SPIVAK R., *Cohen v. Facebook* e *Force v. Facebook* vedi: SPIVAK R., *Facebook Immune from Liability Based on Third-Party Content*, cit.

[48] *Force v. Facebook, Inc.* No. 18-397 (2nd Cir. 2019), p. 27.

Posto che il *complaint* attoreo non smentisce la qualifica di *interactive computer service* di Facebook ma intende trattarlo come *"publisher"* dei contenuti di Hamas, diventa cruciale, dice la Corte, precisare cosa si intenda con *"publisher"* e verificare se Facebook non sia in realtà – come sostenuto dai giudici della *District Court* – un intermediario neutro.

Il concetto di "*publisher"* viene usualmente impiegato dalla giurisprudenza statunitense per indicare un "soggetto che renda pubblico qualcosa"[49], un "riproduttore di un lavoro destinato alla fruizione da parte del pubblico"[50] o, ancora, "qualcuno il cui *business* si sostanzi nel pubblicare"[51] ed è stato esteso anche ai distributori, ricomprendendo tra questi coloro la cui attività si concretizzi nel consentire l'utilizzo dei propri strumenti per veicolare informazioni[52].

Nell'ottica della norma, quindi, chiunque svolga semplicemente la funzione di editore di contenuti altrui deve andare immune da responsabilità civile, dovendo essere ritenuto sì, un *"publisher"*, ma a titolo generale, quale mero "concessore di spazio" e non un sostenitore intenzionato alla propaganda.

Il semplice fatto di concedere un *account* nel quale pubblicare contenuti e messaggi «rientra nel cuore di ciò che significa essere editore di informazioni ai sensi della § 230»[53] e dunque elimina qualsiasi dubbio in merito ad una presunta connivenza tra il *social network* e l'organizzazione terroristica, confermando anzi la piena applicabilità della norma al caso di specie.

6.1. Gli algoritmi e le decisioni editoriali automatizzate: i dubbi interpretativi sulla nozione di publisher.

Venendo all'ulteriore allegazione degli attori, a conferma del sostegno prestato da Facebook alla diffusione dei contenuti di Hamas vi sarebbe l'utilizzo di algoritmi di sistema per consentire una maggiore visibilità dei *post*, suggerire agli utenti profili, pagine e gruppi dedicati, dare vita ad interazioni altrimenti non possibili tra l'organizzazione e soggetti del tutto estranei.

Com'è noto, infatti, ciascun *social network* si avvale di sistemi automatizzati per ottimizzare il proprio funzionamento. Li usa per monitorare i gusti e le preferenze dei propri *users*, per elaborare contenuti che potrebbero essere di loro gradimento e sottoporglieli (mediante *banner* personalizzati, *pop up*, suggerimenti di contatto o segnalazioni) e, infine, per suggerire loro profili di altri utenti che gli siano affini sotto determinati profili.

---

[49] *Klayman v. Zuckerberg*, 753 F.3d 1354, 1359 (D.C. Cir. 2014) che riprende il *Webster's Third New International Dictionary 1837* (1991).

[50] *Federal Trade Commission v. Leadclick Media, LLC*, 838 F.3d at 175, riprende *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1102 (9th Cir. 2009).

[51] *Ibidem*

[52] Ad estendere la portata del termine è la sentenza sul caso *Zeran v. America Online, Inc.*, cit. p. 8.

[53] *Force v. Facebook, Inc.* No. 18-397 (2nd Cir. 2019), p. 31.

In modo non diverso, anche gli algoritmi di Facebook operano su più livelli per garantire la qualità del servizio e la fornitura di contenuti sempre più interessanti, così da trattenere gli *user*s e al contempo immagazzinare dati utili a migliorare le prestazioni di sistema.

Secondo gli attori proprio l'uso di questo genere di automatismi atti ad amplificare i contenuti di Hamas, accrescendone a dismisura il numero dei destinatari farebbe venir meno la natura "neutra" del social di Mark Zuckerberg, concretizzandosi piuttosto in una attività di intervento attivo. «*Facebook* – riporta il *complaint* – *does not act as the publisher of Hamas's content within the meaning of section 230 (c)(1) because it uses algorithms to suggest content to users, resulting in matchmaking*»[54].

È chiaro, infatti, che qualora un frequentatore abituale della piattaforma cominciasse a visitare regolarmente i profili dell'organizzazione, a stringere amicizia con esponenti vari, iscriversi a gruppi chiusi o mettere *like* alle pagine affiliate, gli algoritmi percepirebbero il suo interesse in questo senso, provvedendo immediatamente a suggerirgli contenuti analoghi e quindi diffondendo materiale pericoloso. Ma non solo, la capacità degli strumenti tecnologici di captare gli interessi degli utenti è tale da suggerire gli *account* correlati all'organizzazione anche qualora un soggetto si avventuri occasionalmente sulla pagina di Hamas, rilevando persino la minima percentuale di interesse verso un determinato contenuto.

In sede di appello, dunque, la doglianza degli attori si sposta, rispetto al primo grado, dal terreno della responsabilità per non essere consapevolmente intervenuto a censurare quanto pubblicato da Hamas e non aver vigilato a sufficienza, a quello dell'automazione insita dietro le scelte di sistema di Facebook, intendendo ottenere ragione non tanto in virtù del volontario supporto fornito da quest'ultimo ad Hamas, quanto più perché il lavorio degli algoritmi avrebbe accresciuto a dismisura la risonanza del materiale pubblicato dai terroristi.

Ad opinione dei giudici di New York anche questa seconda argomentazione è da ritenersi del tutto infondata. Restringere o addirittura escludere la portata della § 230 qualora entrino in gioco elementi di intelligenza artificiale significherebbe, infatti, svuotare la norma di senso, in primo luogo poiché moltissimi altri *interactive computer services* in passato ritenuti immuni ex §230 si avvalgono di algoritmi[55] per il proprio *business* e in secondo luogo perché la creazione di collegamenti e accostamenti tra chi diffonde l'informazione e chi la riceve è quanto di più normale accada anche al di fuori della rete.

Inoltre, afferma sempre la *Court of Appeal*, gli *interactive computer services* assumono decisioni editoriali relativamente ai contenuti di parti terze da sempre, sin dai

---

[54] *Force v. Facebook, Inc.* No. 18-397 (2nd Cir. 2019), p. 32.

[55] La Corte a questo proposito cita, a titolo di precedente, *Carafano v. Metrosplash.com* 339 F.3 1119, un caso nel quale il sito di *dating* Matchmaker.com è stato ritenuto immune ai sensi della § 230 sebbene utilizzasse algoritmi per mettere in contatto i potenziali partner sulla base di gusti e preferenze precedentemente espressi. Si veda, in proposito: STILLWELL W., *Carafano v. Metrosplash.com: An Expansion of Tort Immunity for Web Service Providers under 47 U.S.C. 230, Even When They Take a Greater Editorial Role in Publishing Material from Third Parties*, in *Tul. J. Tech. & Intell. Prop.*, vol. 6, 2004, pp. 307-318.

primi anni di *Internet*: «*the services have always decided, for example, where on their sites (or other digital property) particular third-party content should reside and to whom it should be shown. Placing certain third-party on a homepage, for example, tends to recommend that content to users more than if it were located elsewhere on a website. […] Internet services have also long been able to target the third-party content displayed to users based on, among other things, users' geolocation, language of choice, and registration information.* »[56]

Il fatto che, con l'evolversi della tecnologia, i *providers* abbiano accresciuto la propria abilità nel creare collegamenti e nel rintracciare possibili interessati ai propri contenuti non deve in alcun modo penalizzarli: soverchieremmo, infatti, il senso della norma se decidessimo di punirli perché troppo bravi nel condurre il proprio *business*!

La valenza della §230 nel caso di specie è dunque indubbia: indipendentemente dall'uso degli algoritmi, l'automazione delle scelte editoriali non può e non deve in alcun modo escludere l'immunità degli *interactive computer services*, beneficiando costoro dello sgravo di responsabilità a prescindere dalle modalità con le quali tali scelte vengano effettuate.

6.2. Facebook: information content provider *o intermediario neutro?*

Il dibattito sviluppatosi attorno all'uso degli algoritmi dà modo alla Corte di precisare, infine, anche la propria posizione circa la configurabilità di Facebook come *information content provider*, indirettamente avanzata nel *complaint* attoreo proprio quale conseguenza dell'utilizzo di strumenti di intelligenza artificiale per la gestione della piattaforma.

Stando alla lettera della norma, infatti, la nozione di *information content provider* fa da contraltare a quella di *interactive computer service*, e definisce colui il quale crei o sviluppi delle informazioni che poi saranno divulgate mediante un servizio *online*.

L'impiego di sistemi automatizzati da parte di Facebook, sostengono gli attori, avrebbe senza dubbio consentito al *social network* di rimaneggiare i contenuti correlati al terrorismo e di svilupparli nel senso voluto dalla norma, in un intervento tutt'altro che passivo sufficiente a stravolgerne completamente la natura, e dunque ad escludere l'applicabilità della § 230.

Nel concetto di "*development*" espresso dalla disposizione, infatti, potrebbero rientrare svariate operazioni: dalla modifica *in melius/in pejus* del materiale fornito da altri, alla correlazione con informazioni collegate o l'ampliamento della fascia di soggetti cui farle pervenire, con il risultato che potrebbe residuare uno spazio anche per le operazioni messe in atto dagli algoritmi nella loro quotidiana funzione.

È possibile parlare di "sviluppo" dell'informazione quando uno strumento dotato di intelligenza artificiale ne incrementi la portata, le visualizzazioni o influisca nella diffusione del contenuto pubblicato riconducendolo ad utenti in qualche modo affini o interessati? Avvicinare l'informazione ad utenti che non sarebbero mai stati in

[56] *Force v. Facebook, Inc.* No. 18-397 (2nd Cir. 2019), p. 35.

grado di trovarla se non fosse stata loro suggerita può essere considerato uno sviluppo ai sensi della § 230?

La risposta a questi interrogativi passa necessariamente per l'esatta comprensione dell'accezione conferita dalla § 230 (f)(3) al termine "*development*", una questione che la Corte affronta avvalendosi del cd. *material contribution test* già utilizzato in precedenza in altre controversie analoghe per tracciare una linea di demarcazione tra la semplice pubblicazione di contenuti terzi e il concreto intervento sulle informazioni condivise, e dunque per attribuire o meno l'immunità a chi abbia fornito uno spazio *online* a parti terze[57].

Nel decidere il caso *Federal Trade Commission v. Leadclick Media, LLC*[58], ad esempio, gli stessi giudici di *Force v. Facebook* avevano ritenuto Leadclick LLC (una compagnia attiva nel *marketing* il cui *business* consisteva nel mettere in contatto commercianti interessati a promuovere il proprio prodotto ed editori terzi disponibili a pubblicizzarli) un "*developer*" poiché interveniva nell'operato delle terze parti fornendo loro specifiche disposizioni su come costruire l'*advertising* in modo da trarre in inganno i potenziali acquirenti.

O ancora, nel caso *Fair House Council of San Fernando Valley v. Roommates.Com LLC*[59] il noto sito *web Roommates.Com* (finalizzato alla ricerca di una sistemazione in abitazioni condivise con altre persone) era stato ritenuto responsabile della violazione di alcune norme californiane in materia di discriminazione per il semplice fatto di obbligare gli utenti, in fase di registrazione, a compilare un questionario in cui venivano richiesti alcuni dati sensibili (ad esempio, orientamento sessuale, provenienza, esistenza di figli).

Secondo i giudici, infatti, sebbene a fungere da *information content provider*, nel caso di specie, fossero gli utenti all'atto della registrazione, Roommates.Com avrebbe perso la qualifica di intermediario passivo di informazioni fornite da altri chiedendo loro di rispondere a delle domande prestabilite e finendo, di fatto, per manipolare i dati forniti e riproporli agli utenti già registrati per come risultanti sulla base del questionario stesso.

Riguardo all'attività posta in essere da Facebook sui contenuti di Hamas, i giudici della *Court of Appeal* escludono senza riserve che possa trattarsi di contributo materiale, dal momento che, non solo mancherebbe qualsivoglia tipo di intervento concreto ma è anche perfettamente conforme ai termini e alle condizioni del social network consentire a ciascun utente di pubblicare liberamente.

---

[57] Così lo si definisce nel caso *Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1269 n. 4 (9th Cir. 2016) il quale a sua volta riprende *Jones v. Dirty World Entertainment Recordings LLC*, 755 F.3d at 413-14, ripreso da *Force v. Facebook, Inc.* No. 18-397 (2nd Cir. 2019), p. 42.

[58] *Federal Trade Commission v. Leadclick Media, LLC*, cit. p. 10. La sentenza *Force v. Facebook, Inc.* lo riprende in qualità di precedente (pp. 42-43) accostandolo ad altri casi celebri nei quali il *material contribution test* è stato utilizzato per dirimere la controversia.

[59] *Fair House Council of San Fernando Valley v. Roommates.Com LLC*, 521 F.3d 1157 (9th Cir. 2008) citato da *Force v. Facebook, Inc.* No. 18-397 (2nd Cir. 2019), p. 43. Si veda, in merito, SYMER B. M., *Interactive Service Liability for User-Generated Content after Roommates.com*, in *U. Mich. J. L. Reform*, 43(3), 2010, pp. 811-840 ss.

Permettendo a chiunque di condividere senza esercitare un preventivo controllo, Facebook non gioca alcun ruolo di propaganda attiva e agisce, a tutti gli effetti, da "intermediario neutro". Il fatto, poi, che quanto condiviso dagli *users* finisca per avere ampia diffusione in virtù del continuo operare di algoritmi non ha nulla a che vedere con l'alterazione materiale, limitandosi Facebook a mettere in correlazione tra loro elementi affini a prescindere dal contenuto.

«The algorithms take the information provided by Facebook users and "match" it to other users – again, materially unaltered – based on objective factors applicable to any content, whether it concerns soccer, Picasso, or plumbers»[60].

Gli algoritmi hanno indubbiamente accresciuto la visibilità, la fruibilità e la disponibilità del materiale pubblicato da Hamas, ma è scopo precipuo dell'attività di *hosting* enfatizzare il materiale condiviso, e non può che ritenersi infondata l'argomentazione degli attori in base alla quale Facebook non dovrebbe avere alcun ruolo nell'organizzazione o distribuzione dei contenuti altrui: se così fosse, infatti, esso perderebbe completamente di senso essendo nato essenzialmente per permettere ai propri utenti di comunicare pensieri propri.

Infine, la pretesa delle parti attrici non merita accoglimento nemmeno sotto il profilo dell'omessa vigilanza e omesso intervento del *social network* rispetto ai contenuti allarmanti pubblicati da Hamas.

Stando a quanto affermato dallo stesso Facebook nella propria comparsa di risposta[61], infatti, non solo sussiste un divieto di postare contenuti estremi o pericolosi sulla base dei *Terms of Service* (e quindi i gruppi armati come Hamas sarebbero di per sé abusivi), ma il sistema adotta anche una strategia multilaterale di prevenzione articolato su più livelli[62], in modo tale da esercitare un controllo pressoché continuo rispetto a quanto pubblicato ogni giorno. Il suo impegno, quindi, non può essere in alcun modo messo in dubbio e, sostiene la *Court of Appeal*, sebbene i controlli possano non essere sempre effettivi e non rimuovere tempestivamente eventuali contenuti inappropriati (è anche impensabile che si riescano a sorvegliare centinaia di migliaia di utenti ogni minuto) non può essere sufficiente la parziale inefficacia delle strategie di controllo messe in campo ad escludere l'immunità *ex* § 230.

---

[60] *Force v. Facebook, Inc.*, No. 18-397 (2nd Cir. 2019), p. 47.

[61] La sentenza di appello riporta quanto sostenuto dalla parte convenuta a p. 14 e ss.

[62] La strategia multilaterale di Facebook conta tre livelli di intensità diversa:

a) procedure interne di monitoraggio e filtraggio del materiale pubblicato, attivi nel rimuovere la maggior parte dei post allarmanti prima ancora che gli utenti possano segnalarli;
b) sistemi di intelligenza artificiale in grado di bloccare o rimuovere contenuti correlati al terrorismo (o ad altre ideologie analoghe);
c) un *team* specializzato di migliaia di persone che rispondono alle segnalazioni degli utenti e rimuovano il materiale inappropriato tempestivamente.
   A questi si affianca, inoltre, una squadra specializzata antiterrorismo che conta all'incirca 150 componenti tra ingegneri, esponenti dell'ambito accademico, *prosecutors* ed esperti legali.

7. La *dissenting opinion*.

Rigettate tutte le argomentazioni contenute nel *complaint* attoreo, la *United States Court of Appeal for the Second District* dello Stato di New York conferma la sentenza resa in primo grado dalla *District Court* e riconosce l'immunità di Facebook ai sensi della *Section* 230 (c)(1), impedendo che venga ritenuta corresponsabile di Hamas per gli attentati commessi in Israele ai danni dei cinque cittadini statunitensi.

Com'è noto, tuttavia, il sistema statunitense consente – a differenza del nostro – che vengano rese pubbliche le cd. *dissenting opinions*, i pareri discordanti, cioè, di chi, tra i membri del collegio giudicante, sia in disaccordo con quanto deciso dalla maggioranza[63].

Nel caso di specie, a manifestare un'opinione in parte dissenziente[64] è il giudice Katzmann, il quale riporta il proprio parere in calce alla sentenza resa dal collegio.

La divergenza tra quanto espresso in sentenza e l'opinione dissenziente risiede in due aspetti principali: in primo luogo, nella portata della § 230 che sarebbe, forse, più ristretta rispetto a quanto affermato dal collegio giudicante e non si estenderebbe alla protezione dell'editore per contenuti di terrorismo; in secondo luogo nell'esatta qualifica da assegnare a Facebook sulla base del *Communications Decency Act*, vista e considerata la determinante influenza che gli algoritmi hanno nel suo funzionamento.

La *Section* 230, infatti, è nata unicamente come mezzo di tutela dei minori rispetto al materiale osceno rinvenibile *online*, ed è stata, negli anni, estesa a tutti i contenuti pubblicati da terzi in rete, avendo le Corti fatto propria una nozione ampia di "informazione".

Lungi dal sostenere l'inapplicabilità della norma agli intermediari digitali, Katzmann riconosce nell'uso dell'intelligenza artificiale un importante elemento di novità che, accrescendo le abilità dei terzi (in questo caso di Hamas) di raggiungere un'*audience* altrimenti insperata, è in grado di trasformare i *social media* in collaboratori effettivi dell'organizzazione, alterandone la natura di intermediari neutri.

Le argomentazioni di parte attorea, sostiene il magistrato, non rimproverano a Facebook di aver pubblicato contenuti terzi potenzialmente pericolosi, quanto più di aver giocato un ruolo attivo nell'aggregare i terroristi e nel facilitarne le operazioni, e la *Section* 230 fornisce l'immunità a coloro i quali pubblichino contenuti derivanti da parti terze solo qualora si limitino alle tradizionali funzioni editoriali (ovvero decidere se, quando e in che modo pubblicare), non coprendo in alcun modo attività quali: suggerire

---

[63] SCHEPIS F., *La dissenting opinion nel sistema di giustizia costituzionale dalle origini al XX secolo*, in *Salvis Juribus*, 2 marzo 2018. Sul tema vedi anche: ANZON A., *L'opinione dissenziente: atti del seminario svoltosi in Roma, Palazzo della Consulta, nei giorni 5 e 6 novembre 1993*, Milano, Giuffré, 1995; ASPRELLA C., *L'opinione dissenziente del giudice*, Roma, Aracne, 2014; CASSESE S., *Una lezione sulla cosiddetta opinione dissenziente*, in *Quaderni di diritto costituzionale*, fasc. 4, 2009, pp. 973-983; SCALIA A., *The Dissenting Opinion*, in *Journal of the Supreme Court History*, vol. 1994, pp. 33-44.

[64] Quella del giudice Katzmann è *in part dissenting and in part concurring opinion*, una tipologia particolare di opinione dissenziente mediante la quale il magistrato esprime disaccordo solo in riferimento alla decisione su alcuni motivi di doglianza, concordando, invece, su quanto deciso dal Collegio in merito agli altri e alla decisione finale.

possibili profili, gruppi o pagine con cui stringere amicizia e proporre contenuti sulla base delle preferenze in precedenza espresse[65].

«First, Facebook uses algorithms to create and communicate its own message: that it thinks you, the reader – you, specifically – will like this content. And second, Facebook's suggestions contribute to the creation of real-world social networks. The result of at least some suggestions is not just that the user consumes a third-party's content. Sometimes, Facebook's suggestions allegedly lead the users to become part of a unique global community, the creation and maintenance of which goes far beyond and differs in kind from traditional editorial functions»[66].

Il ruolo assolutamente proattivo giocato da Facebook nel dare vita ad un *network* di persone che altrimenti non sarebbe mai venuto ad esistenza (a causa degli scarsi mezzi a disposizione di Hamas) fa sì che esso debba venire considerato, a tutti gli effetti, un *information content provider* e pertanto non possa beneficiare dell'immunità prevista ai sensi della *Section* 230.

La *dissenting opinion* del giudice Katzmann, tuttavia, se da un lato si discosta dalla maggioranza con riferimento all'applicabilità della § 230 e alla natura di *provider* di Facebook, finisce per concordare con la decisione finale del collegio per quanto concerne la responsabilità del noto *social network* nella riuscita degli attacchi omicidi in Israele.

Pur individuando un contributo decisivo di Facebook nella propaganda antisraeliana di Hamas, infatti, è comunque difficile – sostiene Katzmann – provare la sussistenza del nesso di causalità tra i collegamenti generati dalla piattaforma e gli attentati, fermo restando l'indubbio impegno che dovrebbe esserci, da parte di tutti i *social media*, nell'impedire a questo genere di organizzazioni di diffondere i propri contenuti.

Infine, sostiene il giudice, è sicuramente giunta l'ora, per il Congresso, di riconsiderare la previsione di cui alla *section* 230 alla luce dell'incontrollata espansione che ha caratterizzato i *social media* negli ultimi anni.

All'epoca della promulgazione, infatti, *Internet* si apprestava soltanto a diventare uno strumento di uso comune, manifestando limitati problemi di fruizione e permettendo interazioni minime fra gli utenti: sarebbe stato semplicemente impossibile, per il legislatore, riuscire a prevederne lo straordinario sviluppo, i molteplici utilizzi che

---

[65] Katzmann cita svariati precedenti (p. 15 della *dissenting opinion*), anche ripresi dal collegio in sentenza, per evidenziare proprio come essi si differenzino e quindi correttamente applichino la § 230 in virtù della diversa attività posta in essere dai *social media* convenuti in quel caso e Facebook. «*For instance, a claim against a newspaper based on the content of a classified ad (or the decision to publish or withdraw that ad) would fail under the CDA not because newspaper traditionally publish classified ads, but rather because such a claim would necessarily treat the newspaper as the publisher of the ad-maker's content. Similarly, the newspaper does not act as an "information content provider" – and thus maintains its CDA protection – when it decides to run a classified ad because it neither "creates" nor "develops" the information in the ad. 47 U.S.C. § 230 (f)(3).* (*Dissenting opinion*, pp. 15-16)». In particolare: *Jane Doe No. 1 v. Backpage.Com, LLC*, 817 F.3d 12, 19 (1st Cir. 2016); *Jones v. Dirty World Entertainment Recordings LLC*, cit. p. 13; *Barnes v. Yahoo!, Inc.*, cit. p. 10; *Zeran v. America Online, Inc.*, cit. p. 8; *Klayman v. Zuckerberg*, 753 F.3d 1354, 1359 (D.C. Cir. 2014); *Ben Ezra, Weinstein, & Co., Inc. v. America Online, Inc.*, 206 F.3d 980, 986 (10th Cir. 2000).

[66] *Dissenting opinion*, pp. 16-17.

ne sarebbero derivati e i fenomeni distorsivi che in esso avrebbero preso vita, con la conseguenza di dover necessariamente rivedere, ad oggi, una disposizione per certi versi obsoleta.

«While the majority and I disagree about whether § 230 immunizes interactive computer services from liability for all these activities or only some, it is pellucid that Congress did not have any of them in mind when it enacted the CDA. […] Congress could not have anticipated the pernicious spread of hate and violence that the rise of social media likely has since fomented. Nor could Congress have divined the role that social media providers themselves would play in this tale»[67].

8. Una riflessione finale: quale responsabilità penale per gli *internet service provider* nei contesti automatizzati?

In chiave comparatistica il caso *Force v. Facebook* suscita particolare interesse per due ordini di ragioni: la possibilità di istituire un parallelismo tra gli ordinamenti italiano e statunitense in riferimento alla responsabilità degli *Internet Service Provider* e la riflessione in tema di algoritmi, un proficuo terreno di indagine per il giurista che intenda confrontarsi con il ruolo che i moderni strumenti dotati di intelligenza artificiale stanno acquisendo nella risoluzione di istanze giuridiche complesse.

Nella controversia in esame, infatti, vi è un essenziale elemento di novità rispetto ai casi precedentemente giunti dinnanzi alle Corti statunitensi, ed è la discussione attorno agli algoritmi quali fonte di responsabilità per l'*interactive computer service*, essendo questi ritenuti dagli attori il *discrimen* essenziale per escludere l'applicazione della § 230.

Tralasciando per un momento l'esito negativo del processo e dunque la sancita irrilevanza dell'utilizzo di strumenti intelligenti per la gestione della piattaforma, è innegabile come lo spostamento del *focus* dalla semplice responsabilità del *social network* per contenuti inappropriati – ripetutamente scriminata ai sensi della norma in rilievo – all'influenza degli algoritmi nelle interazioni tra utenti (e, quindi, alla possibile natura di *hosting provider attivo* di Facebook) abbia spinto i magistrati a riconsiderare la portata applicativa della *Section* 230 e a misurarsi con una questione del tutto nuova.

Avendo permesso a degli algoritmi di associazione e filtraggio di maneggiare i contenuti immessi da terzi nella piattaforma, il *social network* sarebbe andato, infatti, ben oltre la sua funzione di semplice editore, e avrebbe giocato il ruolo attivo di chi si «inserisce nell'*iter* esecutivo [della pubblicazione], almeno parzialmente [e] prosegue quello messo in atto dall'autore primario o originario, emergendo quale indispensabile anello causale nella diffusione del contenuto illecito»[68].

---

[67] *Dissenting opinion*, p. 33.

[68] ACCINNI G. P., *Profili di responsabilità penale dell'*hosting provider *"attivo"*, in *Arch. pen.*, fasc. 2, maggio-agosto 2017, p. 11.

L'affermazione di responsabilità a carico dell'*hosting provider attivo*[69] a fronte di questo tipo di azioni trova la sua compiuta formulazione anche nelle giurisprudenze europea e italiana (di merito e di legittimità)[70] e, con riferimento al diritto interno, in quello che viene considerato il *leading case* in materia – *RTI vs. Yahoo!*[71] – deciso dal Tribunale di Milano[72].

I giudici meneghini hanno provveduto, infatti, a definire l'*hosting provider* attivo come: «*il prestatore dei servizi della società dell'informazione il quale svolge un'attività che esula da un servizio di ordine meramente tecnico, automatico e passivo, e pone, invece, in essere una condotta attiva, concorrendo con altri nella commissione dell'illecito*» e hanno escluso l'applicabilità del regime speciale di esenzione istituito dall'art. 16 D.lgs. 70/2003, che prevede l'esclusione di responsabilità per il prestatore di un servizio quando costui non sia effettivamente a conoscenza dell'illiceità dell'attività o dell'informazione o si attivi immediatamente per rimuoverle o disabilitarne l'accesso nel momento in cui si avveda della loro esistenza[73].

In altre parole, il *provider* che si avvalga di un *team* editoriale specificamente orientato alla diffusione dei contenuti, sfrutti determinati processi automatizzati e svolga attività di gestione, indicizzazione e organizzazione del materiale postato sarà automaticamente ritenuto *hosting provider* attivo e non potrà godere del regime speciale di esenzione, poiché la conoscenza effettiva del contenuto verrà presunta a fronte della rilevante manipolazione delle informazioni costantemente effettuata.

Sebbene osteggiata da altre pronunce di merito di segno contrario[74], questa impostazione è stata definitivamente consacrata, da ultimo, anche dalla Cassazione

---

[69] TOSI E., *L'evoluzione della responsabilità civile dell'*internet service provider *passivo e attivo*, in *Dir. Industriale*, 6, 2019, pp. 590 ss.

[70] Per un *excursus* giurisprudenziale in materia di responsabilità civile degli ISP vedi: ALLEGRI M.R., *Alcune considerazioni sulla responsabilità degli intermediari digitali, e particolarmente dei* social network provider*, per i contenuti prodotti dagli utenti*, in *Informatica dir.*, vol. XXVI, 2017, n. 1-2, pp. 69-112.

[71] Trib. Milano, Sez. Spec. Propr. Ind. e Intellettuale, 9 settembre 2011, n. 10893, con nota di SARACENO A., *Note in tema di violazione del diritto d'autore tramite internet* in *Riv. dir. ind.*, 2012, 364 ss.

[72] Nello stesso senso anche Trib. Milano, 20 gennaio 2011 (con nota di BELLAN A., *Per una* reasonable liability*: critiche alla responsabilità oggettiva dei* provider *e tutela dei diritti su* internet, in *Dir. Ind.*, 3/2012, pp. 243 ss.); Trib. Roma, Sez. IX spec. in materia di imprese, 27 aprile 2016 (con nota di SIMONI M., *La responsabilità degli* hosting provider *quali prestatori 'automatici, tecnici e passivi' della società dell'informazione*, in *Dir. Ind.*, 5/2017, pp. 455 ss.); Trib. Roma, XVII Sez. Civ., 10 gennaio 2019, n. 693 (con nota di FRIGERIO F., *Attivo anche se inconsapevole. Il Tribunale di Roma sanziona Vimeo e conferma i caratteri della responsabilità dell'*hosting provider *attivo*, in *Rivista del diritto dei media*, 2/2019, pp. 258 ss.)

[73] L'articolo 16 D.lgs. 70/2003 esonera da responsabilità il *provider* qualora non sia effettivamente a conoscenza del fatto che l'attività o l'informazione pubblicata è illecita.

[74] Trib. Torino, I Sez. Civ., 7 aprile 2017, n. 1928 (con nota di VOZZA V., *La responsabilità civile degli* Internet Service Provider *tra interpretazione giurisprudenziale e dettato normativo*, in *Danno e Resp*, 1/2018, pp. 97 ss.); anche l'ordinanza del Tribunale di Napoli Nord nel noto caso di Tiziana Cantone ha provveduto a ribadire come l'obbligo di sorveglianza del *provider* sia esclusivamente successivo e la sua responsabilità per la mancata rimozione di contenuti offensivi insorga solo nel momento in cui ne abbia effettiva conoscenza, qualificandosi come responsabilità successiva eventuale e plurisoggettiva (Trib. Napoli Nord, 3 novembre 2016 con nota di BOCCHINI R., *La responsabilità di Facebook per la mancata rimozione di contenuti illeciti*, in *Giur. It.*, 3/2017, pp. 629 ss.).

civile[75], che ha fatto propria la presunzione di effettiva conoscenza dell'*hosting provider* attivo alla luce dei numerosi interventi usualmente attuati dagli intermediari per incrementare i propri servizi e aumentare la diffusione dei contenuti; salvo poi riconoscere il dovere del giudice di verificare sempre caso per caso la natura di *hosting provider* attivo e la possibilità per quest'ultimo di superare la presunzione fornendo in giudizio prova contraria, nonché ricomprendendo nella nozione tutti i *social media* analoghi a Facebook[76].

Questo concetto di *conoscenza effettiva* del contenuto è elemento dirimente anche in ambito penale e ha visto la giurisprudenza di legittimità atteggiarsi in due modi differenti: dapprima ritenendo responsabile, con sentenza 27 dicembre 2016 n. 54946, il legale rappresentante di una società gerente un sito *internet* per non aver rimosso un contenuto diffamatorio di cui era venuto a conoscenza, poi escludendo la sussistenza di qualsivoglia obbligo di controllo *ex ante* da parte del *provider* e dunque di un obbligo giuridico di impedire l'evento[77] (in conformità, peraltro, con quanto previsto dall'articolo 17 D.lgs. 70/2003[78]).

Tralasciando le molteplici voci di critica giunte dalla dottrina nei confronti del primo dei due arresti citati[79], è evidente come il combinato disposto delle due giurisprudenze (civile e penale) in ambito di *hosting provider* attivi possa aprire uno spiraglio ad una responsabilità, di fatto, oggettiva degli *ISP* che si avvalgano di strumenti automatizzati.

Se, infatti, la conoscenza del contenuto illecito pubblicato da terzi viene data per presupposta ogniqualvolta l'*internet service provider* giochi un ruolo in qualche modo attivo nel trattare l'informazione, e se è vero che la maggior parte di questi soggetti si avvale di algoritmi per rendere il proprio spazio virtuale maggiormente performante, ne conseguirà un suo automatico contributo causale nella commissione del reato. Il tutto senza considerare che l'attività di enfatizzazione e gestione dei contenuti illeciti portata avanti dagli algoritmi è totalmente autonoma, e prescinde, nella maggior parte dei casi, dalla volontà dell'umano che se ne avvalga.

---

[75] Cass. civ., Sez. I, 19 marzo 2019, n. 7708 con nota di BOCCHINI R., *Responsabilità civile dell'*hosting provider *– la responsabilità civile, plurisoggettiva, successiva ed eventuale dell'*ISP, in *Giur. It.*, 12/2019, pp. 2604 ss. La Corte esemplifica le attività del *provider* attivo in: «filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione o promozione di contenuti, operate mediante una gestione imprenditoriale del servizio, come pure l'adozione di una tecnica di valutazione comportamentale degli utenti per aumentarne la fidelizzazione».

[76] TORMEN L., *La linea dura della Cassazione in materia di responsabilità dell'*hosting provider *(attivo e passivo)*, in *Nuova Giur. Civ.*, fasc. 5, 2019, pp. 1039 ss.

[77] Cass. Pen., Sez. V, 8 novembre 2018 (dep. 20 marzo 2019), n. 12546 con nota di PAGELLA C., *La Cassazione sulla responsabilità dei blogger per contenuti diffamatori (commenti) pubblicati da terzi*, in *Dir. pen. cont.*, 17 maggio 2019.

[78] PINO G., *Assenza di un obbligo generale di sorveglianza a carico degli* internet service providers *sui contenuti immessi da terze parti*, in *Danno e resp.*, 8/2004, pp. 832 ss.

[79] Su tutte: INGRASSIA, *Responsabilità penale degli* internet service provider*: attualità e prospettive*, cit. p. 1.; CURRELI C., *La controversa responsabilità del gestore di un sito* web*, in caso di diffamazione commessa da terzi*, in *Resp. civ. prev.*, 2017, 5, p. 1648 ss.

Il rischio che delle macchine attivate per scopi leciti – nella fattispecie rendere maggiormente interessante la piattaforma per gli utenti e creare collegamenti funzionali ai loro interessi – volgano all'illecito veicolando informazioni pericolose o lesive della dignità altrui è elevatissimo e non prevedibile, dal momento che, per quanto programmato, questo genere di tecnologie apprende in autonomia dal contesto circostante e seleziona autonomamente i passi da compiere. Non a caso siamo nell'era del cd. *machine learning*, e cioè dell'apprendimento autonomo degli agenti artificiali.

La possibilità che possa sorgere una responsabilità per il *social* avvalsosi di strumenti dotati di intelligenza artificiale sussiste, peraltro, in una molteplicità di ambiti diversi, che prescindono dalla propaganda terroristica in rilievo per *Force v. Facebook*. Basti pensare all'*hate speech*, al cyberbullismo o, più in generale, ai contenuti discriminatori verso disabili, minoranze etniche o categorie deboli; di talché diventa rilevante costruire un modello di responsabilità effettivamente tarato sulle caratteristiche del sistema.

Un commento razzista particolarmente apprezzato dagli utenti con centinaia di *likes*, ad esempio, viene automaticamente posto dagli algoritmi di Facebook in cima alla lista dei commenti affinché goda della massima esposizione; un post diffamatorio ricondiviso svariate volte diventa virale nel giro di poche ore perché suggerito nelle bacheche degli amici di chi lo abbia condiviso o abbia messo *like*. Qualunque contenuto di Facebook (o di altri *social media*) riceva particolare attenzione viene automaticamente sovraesposto dal *social network* addirittura all'insaputa degli umani programmatori e soprattutto travalicando quelle che sarebbero state le primarie intenzioni del sistema, sicuramente non intenzionato alla pubblica diffamazione o alla diffusione di contenuti allarmanti[80]. Ne consegue che addebitare la responsabilità a titolo di concorso commissivo all'*hosting provider* in virtù di una "presunzione di conoscenza" significherebbe optare per una risposta sanzionatoria iniqua, rivelandosi, peraltro, difficilissimo per l'*ISP* provare di aver ignorato il contenuto illecito nonostante l'effettivo contributo apportato dagli algoritmi.

Come costruire, quindi, un modello di responsabilità penale che possa effettivamente dimostrarsi adeguato quando l'algoritmo commetta autonomamente l'illecito e l'umano non ne abbia contezza o non possa impedirlo?[81]

---

[80] Un tema, questo, particolarmente rilevante anche sul piano della libertà di informazione all'interno dei *social media* e della *filter bubble* nella quale ciascun utente si trova rinchiuso proprio a causa delle scelte algoritmiche effettuate a monte dai sistemi algoritmici. L'estrema personalizzazione dei contenuti, infatti, lungi da garantire il pluralismo di idee, finisce molto spesso per annientarlo definitivamente, conferendo particolare rilievo solo a determinate informazioni selezionate sulla base delle preferenze espresse e, peraltro, molto spesso nocive (pensiamo al fenomeno *fake news*). In merito, PITRUZZELLA G., *La libertà di informazione nell'era di* Internet, in Pitruzzella G., Pollicino O., Quintarelli S., *Parole e potere. Libertà di espressione*, hate speech *e* fake news, Milano, Egea, 2017, pp. 28 e ss.; BIANCA M., *La filter bubble e il problema dell'identità digitale*, in *Rivista di diritto dei media*, 2/2019, pp. 39 ss.

[81] Un interrogativo, questo, al quale hanno tentato di dare alcune risposte, *e multis*, PAGALLO U., *Saggio sui robot e il diritto penale*, in Vinciguerra S., Dassano F. (a cura di), *Scritti in memoria di Giuliano Marini*, Napoli, Edizioni Scientifiche Italiane, 2010, pp. 595 ss.; RIONDATO S., *Robot: talune implicazioni di diritto penale*, in Moro P., Sarra C. (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, Franco Angeli, 2017, pp. 85 ss.; MAGRO B., Robot, *Cyborg e intelligenze artificiali*, Cadoppi A., Canestrari S., Manna A., Papa M. (diretto

La risposta ci pone di fronte ad alcune fondamentali problematiche, indissolubilmente legate all'autonomia raggiunta dalle nuove tecnologie in tutti i campi di applicazione. «Le macchine intelligenti, come prodotto soggettivizzato, possono tenere – infatti – dei veri e propri comportamenti attivi assolutamente imprevedibili, derivanti dal lavorìo autoevolutivo del *machine learning*, tali che qualunque danno da essi derivante sfugga inesorabilmente alle capacità previsionali dei programmatori».[82]

Potremmo pensare di ritenere responsabile l'utente finale – Facebook, in questo caso, ma più in generale chiunque faccia uso di applicazioni dotate di intelligenza artificiale – sulla base di un modello colposo, ovverosia per essersi affidato all'innovazione tecnologica e aver assunto deliberatamente il rischio di verificazione degli illeciti, ma ci scontreremmo inevitabilmente con il divieto di responsabilità oggettiva vigente nel nostro ordinamento.

A fronte di un algoritmo capace di "autodeterminarsi" sul piano delle funzioni svolte, infatti, chiamare a rispondere l'utente finale per aver colposamente confidato in un suo operato conforme alla legge significherebbe punirlo per delle semplici scelte imprenditoriali, mancando in lui qualsiasi componente soggettiva in ordine alla realizzazione del fatto reato.

Teorizzata da Peter Asaro[83] e ripresa, sul versante italiano, da Giovanni Sartor[84], la teoria della responsabilità dell'utente finale poggia le proprie basi sulla *vicarious liability* degli ordinamenti anglosassoni[85], e intende dare accesso, nell'ordinamento penale italiano, ad una forma di responsabilità analoga a quella di padroni e committenti per il danno cagionato dai propri sottoposti già esistente nel diritto civile (articolo 2049 c.c.).

Degli effetti prodotti dall'agente, dunque, dovrebbe rispondere l'utilizzatore, "colpevole", in qualche modo, di aver confidato nelle capacità razionali della macchina e nella sua abilità di ottenere un certo risultato. Le intelligenze artificiali sono caratterizzate da un'elevata imprevedibilità declinabile sotto due profili: un'imprevedibilità teorica che rende molto difficile, se non impossibile, stabilire in anticipo come una macchina capace di adattarsi al contesto potrebbe agire; e una imprevedibilità pratica connessa alla difficoltà di un utilizzatore di controllarne i comportamenti. Date queste due caratteristiche, pertanto, chiunque decida di fare uso di strumenti di questo genere potrà essere ritenuto responsabile a titolo di colpa cosciente, avendo consapevolmente scelto di affidarsi ad un sistema di cui non

---

da), *Cybercrime*, Utet Giuridica, Milano 2019, pp. 1179 ss.; BASILE F., *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Dir. pen. cont.*, 29 settembre 2019.

[82] CAPPELLINI A., Machina delinquere non potest? *Brevi appunti su intelligenza artificiale e responsabilità penale*, in *Criminalia*, 27 marzo 2019, p. 499 ss.

[83] ASARO P., *A body to kick, but no soul to damn. Legal Perspectives on Robotics*, in Lin P., Abney K., Bekey G.A., *Robot Ethics. The Social and Ethical Implications of Robotics,* Cambridge, MIT Press, 2012.

[84] SARTOR G., *L'intenzionalità degli agenti* software *e la loro disciplina giuridica*, in *Researchgate.net*, 2 novembre 2002.

[85] Una peculiare forma di responsabilità oggettiva, vigente in ambito penale, che punisce chi si avvalga di persone o mezzi per il raggiungimento di un determinato scopo, essendo del tutto irrilevante la sussistenza in capo a costui di uno stato soggettivo di colpevolezza.

conosceva appieno il funzionamento e confidato nella propria capacità di gestire gli eventi.

Volendo dare un sostegno normativo compatibile con l'assetto penalistico alla responsabilità dell'utente finale per come ipotizzata da Asaro e Sartor dovremmo guardare, probabilmente, alla disciplina del concorso di persone nel reato e, più in particolare, all'articolo 116 c.p. in tema di concorso anomalo, assimilando l'*hosting provider* attivo (o comunque l'*user* finale) al concorrente chiamato a rispondere anche dell'evento non voluto ma prevedibile quale probabile sviluppo del reato. L'utente ultimo dell'algoritmo, infatti, sarebbe pienamente conscio della capacità dello stesso di evolvere costantemente e di optare per scelte illecite, e dunque potrebbe essere chiamato a rispondere del suo operato facilmente prevedibile.

Questa impostazione, seppur apparentemente risolutiva, non parrebbe applicabile al caso in esame, dal momento che l'utilizzatore dell'algoritmo, non solo, non sta compiendo alcun reato effettivamente voluto, ma si trova comunque in una situazione di rischio tollerato. Sarebbe piuttosto opportuno introdurre una nuova figura, una "colpa da programmazione" che consenta di addossare la responsabilità all'umano e di prospettare parallelamente una scusante per il caso in cui si siano attuate tutte le misure idonee a prevenire la realizzazione di reati da parte di macchine intelligenti[86].

Un'ulteriore possibilità potrebbe risiedere nell'addossare la responsabilità ai programmatori dell'algoritmo, chiamandoli a rispondere non soltanto in ordine ai malfunzionamenti o agli errori commessi in sede di programmazione, ma anche al reato posto in essere dalle macchine intelligenti in totale autonomia. Anche in questo caso, tuttavia, il modello in esame faticherebbe a trovare applicazione nel nostro ordinamento, fondandosi esclusivamente su una responsabilità di tipo oggettivo.

Inoltre, se arrivassimo a ritenere sviluppatori e *designers* responsabili dell'illecito commesso dalla macchina rallenteremmo pesantemente il progresso tecnologico, dal momento che nessun tecnico si arrischierebbe più a programmare sistemi cognitivamente avanzati in grado di coadiuvare le attività umane.[87]

Da ultimo, potremmo pensare di intervenire in via preventiva (perlomeno per quanto concerne i *social network*) tentando la via della regolamentazione estrema e della riprogrammazione degli algoritmi sino ad oggi utilizzati dagli *ISP* affinché rimuovano qualsiasi tipo di contenuto allarmante[88]; ma allora viene da chiedersi che ne sarebbe della

---

[86] Questa è l'ipotesi di MAGRO M.B., *Biorobotica, robotica e diritto penale,* in Provolo D., Riondato S., Yenisey F., *Genetics, Robotics, Law, Punishment,* Padova University Press, 2014, p. 499 ss.

[87] LIMA D., *Could AI Agents Be Held Criminally Liable? Artificial Intelligence and the Challenges for Criminal Law,* in *S. C. Law. Rev*, n°69, 2018.

[88] L'introduzione di sistemi di filtraggio e blocco, tuttavia, se potrebbe (forse) essere risolutivo mettendo in campo il controllo *ex ante*, non sé comunque scevro da problemi di sorta. L'impiego di algoritmi di questo tipo, infatti, oltre a rivelarsi un onere complesso e costoso per i *providers*, manifesta delle criticità anche sul piano pratico, essendo molto complesso effettuare una verifica estesa sulla varietà di *server* attivi e programmare i sistemi automatizzati affinché rimuovano o segnalino tutti i tipi di contenuti. Molteplici possono essere, le forme di illiceità del contributo postato ed è difficile che, in fase di settaggio degli algoritmi, gli sviluppatori siano in grado di prevederli tutti e allenare le macchine ad eliminarli. Così GAMBINI M., *Intelligenza artificiale e diritto – algoritmi e sicurezza*, in *Giur. It.*, 7/2019, pp. 1657 ss.

"neutralità" della rete libera da ingerenze, e della libertà di espressione in quello spazio garantita[89].

Il caso *Force v. Facebook* per primo lancia un allarme, ci impone di riflettere per non farci cogliere impreparati e, nella persona del giudice Katzmann, ammonisce il legislatore invitandolo a rivedere la *Section* 230, in evidente obsolescenza, o perlomeno a ridefinirne la portata. Un monito, questo, che dovrebbe essere al centro dell'attenzione, per indurci a ripensare le categorie giuridiche conosciute e cominciare ad interrogarci seriamente sul rapporto tra intelligenza artificiale e diritto: un settore pressoché anomico, che non può più restare tale.

[89] Sul tema si vedano i contributi di POLLICINO O., *La prospettiva costituzionale sulla libertà di espressione nell'era di Internet*, in Pitruzzella G., Pollicino O., Quintarelli S., *Parole e potere. Libertà di espressione, hate speech e fake news*, cit.; PETRUSO R., *Responsabilità delle piattaforme online, oscuramento di siti web e libertà di espressione nella giurisprudenza della Corte europea dei diritti dell'Uomo*, in *Dir. Inform.*, fasc. 3, 1° giugno 2018, pp. 511 ss.