

ONLINE HATE SPEECH: LA PROSPETTIVA DELL'UNIONE EUROPEA
TRA REGOLAMENTAZIONE DELLA CONDOTTA DEI PRESTATORI DI
SERVIZI INTERMEDIARI E RICORSO AL DIRITTO PENALE

ILARIA ANRÒ*

Sommario

Introduzione. – 1. Il contrasto all'*hate speech* attraverso le regole circa la moderazione dei contenuti *online*. – 1.1 Alle origini della disciplina in tema di *online hate speech*: la Direttiva sul commercio elettronico. – 1.2 La responsabilizzazione dei PSI attraverso gli strumenti di *soft law*. – 1.3 La nuova direttiva sui media audiovisivi ed il regolamento relativo al contrasto della diffusione di contenuti terroristici *online*. – 1.4 Il futuro della regolamentazione dell'*online hate speech*: il *Digital Services Act*. – 2. L'azione dell'Unione nei confronti delle condotte penalmente rilevanti. – 2.1 La Decisione Quadro: la lotta contro le condotte di odio attraverso il diritto penale. – 2.2 L'inserimento di *hate speech* e *hate crime* tra i reati europei: una nuova proposta della Commissione europea. – 3. Osservazioni conclusive.

Abstract

The aim of this contribution is to outline the evolution of the main instruments of EU law for contrasting online hate speech, through the strands of internal market regulation on the one hand, from the e-Commerce Directive to the DSA, and the use of European criminal law on the other hand, from the Framework Decision to the recent proposal of the European Commission to extend the list of offences recognised by the European Union under Article 83 TFEU to hate speech and hate crimes.

Suggerimento di citazione

I. ANRÒ, *Online hate speech: la prospettiva dell'Unione europea tra regolamentazione della condotta dei prestatori di servizi intermediari e ricorso al diritto penale*, in *Osservatorio sulle fonti*, n. 1/2023. Disponibile in: <http://www.osservatoriosullefonti.it>

* Professore associato di Diritto dell'Unione europea nell'Università degli Studi di Milano.
Contatto: ilaria.anro@unimi.it

Introduzione

L'*online hate speech* si presenta come un fenomeno fortemente transnazionale, tale da richiedere, per un contrasto efficace, una regolamentazione sovranazionale: un messaggio di odio in rete, infatti, può propagarsi velocemente e coinvolgere persone presenti in più Stati, nonché essere riproposto su diverse piattaforme. Come ricordato dall'avvocato generale Spunar, inoltre, «su *internet* si scrive con l'inchiostro, non a matita»¹ e i contenuti di odio possono rimanere *online* per molto tempo, nonché essere riprodotti su diversi siti o *social network*.

L'ordinamento dell'Unione europea presenta diversi strumenti che concorrono al contrasto di tale fenomeno². Occorre tenere presente, tuttavia, che la disciplina di *internet* e delle regole di condotta dei prestatori di servizio in questo settore può incidere su diritti fondamentali come il diritto alla *privacy* e la libertà di espressione, i quali possono essere concepiti in maniera diversa a seconda degli ordinamenti nazionali³. Nella dimensione europea si affiancano, quindi, strumenti di *hard law* e *soft law*, sperimentando nuove forme di regolazione e di collaborazione tra autorità pubbliche e private per la tutela dei diritti fondamentali.

In particolare, occorre osservare come l'azione dell'Unione europea per il contrasto all'*hate speech* (*online* ma non solo) si svolga secondo due direttrici: da un lato, l'adozione di norme dirette alla regolamentazione della condotta dei prestatori di servizi intermediari ("PSI"), ovvero i fornitori di servizi nel modo digitale consistenti nel trasporto («mere conduit»), memorizzazione temporanea («caching») e memorizzazione di informazioni fornite dal

¹ Cfr. Conclusioni dell'avvocato generale Spunar del 5 giugno 2019, in causa C-18/18, *Glawisch-nig-Piesczek*, par. 1, ECLI:EU:C:2019:458.

² I contributi in dottrina dedicati alla dimensione sovranazionale del discorso di odio e al bilanciamento dei diversi diritti coinvolti sono piuttosto numerosi: si veda, *ex multis*: M. BASSINI, *Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione*, in *Rivista Italiana di informatica e diritto*; 2021, p. 43 ss.; M. D'AMICO, B. LIBERALI (a cura di), *La costituzione non odia. Conoscere, prevenire e contrastare l' hate speech online*, Torino, 2021; G. PITRUZZELLA, O. POLLICINO, *Disinformation and Hate Speech. A Constitutional Perspective*, Milano, 2020; G. ZICCARDI, *Online Political Hate Speech in Europe: the Rise of New Extremism*, Oxford, 2020; M. SPATTI, *L'azione dell'Unione europea nella lotta all'odio online: la responsabilizzazione dei social media*, in AA.VV., *Temi e questioni di diritto dell'Unione europea. Scritti offerti a Claudia Morviducci*, Bari 2019, p. 909; G. ZICCARDI, *L'odio online. Violenza verbale e ossessioni in rete*, Milano, 2016, spec. p. 70.

³ Sul rapporto tra libertà di espressione e regolamentazione del "potere digitale" vedi per tutti O. POLLICINO, *Potere Digitale*, in *Enciclopedia del diritto*, in corso di pubblicazione. V. anche, dello stesso Autore, *Judicial Protection of Fundamental Rights on the Internet*, Oxford, 2021, nonché le riflessioni, svolte a proposito di un caso italiano, di C. CARUSO, *La libertà di espressione presa sul serio. CasaPound c. Facebook, Atto I*, e M. CASTELLANETA e P. De SENA, *La libertà di espressione e le norme internazionali, ed europee, prese sul serio: sempre su CasaPound c. Facebook*, entrambi su *Sidiblog*, 20 gennaio 2020.

destinatario su richiesta di quest'ultimo («hosting»)⁴, dall'altro lato il ricorso a norme per l'incriminazione delle condotte di odio considerate penalmente rilevanti. Dunque, strumenti tipicamente di mercato interno e atti di cooperazione giudiziaria in materia penale concorrono per la tutela della persona di fronte a manifestazioni di odio.

Resta sullo sfondo il tema (o problema) definitorio: non vi è una definizione precisa a livello di Unione europea di *online hate speech* e dunque le condotte riconducibili a tale fenomeno sono caratterizzate attraverso strumenti che prevedono regole solo per determinati ambiti o comunque che non lo abbracciano nella sua interezza⁵.

Il presente contributo, dopo aver brevemente richiamato i principali strumenti adottati nell'ambito del mercato interno al fine di regolamentare la condotta dei PSI, si concentra sull'azione dell'Unione europea diretta alla lotta contro l'*hate speech* attraverso l'adozione di norme incriminatrici, avviata con l'adozione della decisione quadro 2008/913/GAI del Consiglio del 28 novembre 2008 sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale (nel seguito, "Decisione Quadro")⁶ e recentemente portata avanti tramite la proposta di inserire le condotte di *hate speech* e di *hate crime* tra le sfere di criminalità suscettibili di regolamentazione da parte di Parlamento europeo e Consiglio, mediante norme minime relative alla definizione dei reati e delle sanzioni di sensi dell'art. 83 TFUE⁷, svolgendo alcune riflessioni critiche con riferimento a tale iniziativa.

1. Il contrasto all'*hate speech* attraverso le regole circa la moderazione dei contenuti *online*

Le prime norme in tema di regolamentazione della condotta dei PSI nell'ordinamento dell'Unione si ritrovano in strumenti funzionali alla realizzazione del mercato interno piuttosto che alla tutela dei diritti fondamentali, secondo il paradigma tipico dell'integrazione comunitaria. Tali strumenti,

⁴ Sono considerati tali i servizi della società dell'informazione, ai sensi della Direttiva sul Commercio elettronico e del DSA (come definiti nel testo), su cui vedi *infra*.

⁵ Si veda il documento dell'Unesco che ha evidenziato i principali elementi che contraddistinguono questa peculiare forma di propagazione del discorso di odio: Unesco, *Countering online hate speech*, Parigi, 2015, spec. p. 13. Cfr. anche A. F. SELLARS, *Defining Hate Speech*, Berkman Klein Center Research Publication No. 2016-20, Boston Univ. School of Law, Public Law Research Paper No. 16-48 e *Study to support the preparation of the European Commission's initiative to extend the list of EU crimes in Article 83 of the Treaty on the Functioning of the EU to hate speech and hate crime*, commissionato dalla Commissione europea, novembre 2021, reperibile *online*, spec. p. 32 ss.

⁶ Decisione quadro 2008/913/GAI del Consiglio del 28 novembre 2008 sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale, in *GUUE*, L 328 del 6 dicembre 2008.

⁷ Commissione europea, Un'Europa più inclusive e protettiva: estendere l'elenco dei reati riconosciuti dall'UE all'incitamento all'odio e ai reati generati dall'odio, COM(2021)777 final.

nell'indirizzarsi ad aziende informatiche, piattaforme, *social network* e, in generale, ai prestatori di servizi nel mondo digitale, hanno avviato la regolamentazione della gestione dei contenuti *online*, in prima battuta, per incentivare gli scambi nel mondo digitale mantenendo un *level playing field*, per poi concentrarsi su aspetti strettamente attinenti alla tutela della persona. È in tali strumenti che si possono ravvisare norme fondamentali per il contrasto all'*online hate speech*, fenomeno disciplinato con sempre maggiore consapevolezza dal legislatore comunitario, in un percorso ideale che va dalla 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 (nel seguito, la "Direttiva sul commercio elettronico")⁸, al recente regolamento del Parlamento europeo e del Consiglio relativo ad un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE (nel seguito, "*Digital services act*" o "DSA")⁹, passando per strumenti settoriali, anche di *soft law*, con norme specifiche sul punto.

1.1 Alle origini della disciplina in tema di *online hate speech*: la Direttiva sul commercio elettronico

Pur trattandosi di uno strumento ormai risalente a più di venti anni fa, la Direttiva sul commercio elettronico rimane, ancora oggi, lo strumento di riferimento in tema di regolamentazione delle piattaforme *online*, almeno finché sarà applicabile il *Digital Services Act* (su cui v. *infra*). Detta direttiva, nata con l'obiettivo di incoraggiare lo sviluppo del commercio elettronico nell'Unione europea, in un'epoca in cui l'utilizzo di *internet* a questo fine era piuttosto limitato, era diretta a stabilire un quadro comune, ravvicinando le legislazioni, per l'attuazione della libera circolazione dei servizi della società dell'informazione, nonché per creare certezza giuridica e fiducia dei consumatori nel commercio *online*. Le basi giuridiche della Direttiva sono infatti, l'art. 95 TCE, corrispondente all'attuale art. 114 TFUE, norma sul ravvicinamento delle

⁸ 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 («Direttiva sul commercio elettronico»), in *GUUE* L 178 del 17 luglio 2000, p. 1 ss. È stata trasposta in Italia dal 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, in Suppl. ordinario n. 61 a *GURI*, 14 aprile, n. 87. Sull'evoluzione della normativa dell'Unione sul tema si veda G. MORGESE, *Moderazione e rimozione dei contenuti illegali online nel diritto dell'Unione europea*, in *Federalismi.it*, 12 gennaio 2022, p. 80 ss.

⁹ Cfr. Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), in *GUUE* L 277 del 27 ottobre 2022, p. 1 ss.

legislazioni, e gli artt. 47, par. 2 (oggi art. 53, par. 1, TFUE), e 55 TCE (oggi art. 62 TFUE), che consentono l'azione delle istituzioni per agevolare l'accesso alle attività autonome e il loro esercizio, in regime di stabilimento e libera prestazione di servizi.

La Direttiva è principalmente diretta a disciplinare i servizi della società dell'informazione, definiti in maniera piuttosto ampia, utilizzando una definizione già contenuta nella direttiva 98/34/CE che prevede una procedura di informazione nel settore delle norme e delle regolamentazioni tecniche¹⁰ nonché nella direttiva 98/84/CE sulla tutela dei servizi ad accesso condizionato e dei servizi di accesso condizionato¹¹. Ai sensi di tale direttive, i servizi della società dell'informazione comprendono ogni servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica, attraverso apparecchiature elettroniche e su richiesta del destinatario, come riportato dal considerando n. 17 e dalla definizione sub art. 2, lett. a). La Corte di giustizia ha chiarito, tuttavia, che il legame tra servizio e retribuzione non deve essere necessariamente diretto, affermando la responsabilità di editori di notizie *online* per i commenti diffamatori e il materiale illegale pubblicato sul loro sito *web*, indipendentemente dal fatto che il contenuto sia gratuito o a pagamento per gli utenti, quando la piattaforma riceve un reddito generato da un'attività di *marketing*¹². Inoltre, La Corte di giustizia è intervenuta per precisare i confini di tale nozione, includendovi la piattaforma Airbnb Ireland, riscontrando un sufficiente collegamento tra il controllo fornito dalla piattaforma ed il servizio offerto¹³, escludendo al contrario Uber, ritenendolo unicamente un prestatore di servizio di trasporto, ma non un servizio della società dell'informazione¹⁴.

La direttiva si fonda, sostanzialmente, su tre principali elementi: (i) il principio dello Stato di origine, ai sensi del quale i prestatori di servizi devono rispettare le regole del loro Stato di origine, ovvero dello Stato in cui sono stabiliti; (ii) un regime di esenzione da responsabilità per gli intermediari *online* con riferimento ai contenuti che veicolano (in presenza di determinate condizioni); (iii) il divieto per gli Stati di imporre agli intermediari *online* un obbligo generale di monitorare le informazioni che trasmettono o conservano per non violare i diritti fondamentali degli utilizzatori (*in primis* diritto alla *privacy* e diritto alla libertà di espressione).

La direttiva prevede, infatti, una sostanziale esenzione di responsabilità per i prestatori di servizi della società dell'informazione in caso di semplice

¹⁰ In *GUCE* L 204 del 21 luglio 1998, p. 37 ss.

¹¹ In *GUCE* L 320 del 28 novembre 1998, p. 54.

¹² Cfr. Corte giust., 11 settembre 2014, C-291/13, *Papasavvas*.

¹³ Cfr. Corte giust. (grande sez.), 19 dicembre 2019, C-390/18, *Airbnb Ireland UC*, ECLI:EU:C:2019:1112.

¹⁴ Cfr. Corte giust. (grande sez.), 20 dicembre 2017, C-434/15, *Uber*, ECLI:EU:C:2017:981.

trasporto («mere conduit») ove il prestatore non dia origine alla trasmissione, non selezioni il destinatario della stessa, né scelga o modifichi in qualche modo le informazioni trasmesse. C'è un'esenzione da responsabilità anche per il caso di memorizzazione temporanea delle informazioni («caching»), sempre che il prestatore non modifichi le informazioni e non interferisca con l'uso della tecnologia per ottenere dati sull'impiego delle stesse.

I contenuti illegali sulle piattaforme *online* possono però diffondersi in particolare tramite servizi che permettono il caricamento di contenuti di terzi (servizi di «hosting»). A tal proposito, l'art. 14 della direttiva stabilisce che i prestatori di servizi di *hosting* non possano essere considerati responsabili per le informazioni memorizzate su richiesta di terzi, a condizione che: a) non siano effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non siano al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione; o b) non appena al corrente di tali fatti, agiscano immediatamente per rimuovere le informazioni o per disabilitarne l'accesso. Inoltre, l'articolo 15 dispone che «nella prestazione dei servizi di cui agli artt. 12, 13 e 14, gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite». Allo stesso tempo, il considerando 47 della direttiva ricorda che ciò riguarda unicamente gli obblighi di sorveglianza di carattere generale e non «gli obblighi di sorveglianza in casi specifici e, in particolare, lascia impregiudicate le ordinanze emesse dalle autorità nazionali secondo le rispettive legislazioni».

Questa direttiva ha, dunque, concesso una grande libertà ai prestatori di servizi *online*, impedendo agli Stati di imporre loro obblighi di sorveglianza, creando significative esenzioni di responsabilità. La direttiva, inoltre, diretta principalmente all'incentivazione del commercio elettronico, pare consentire una certa espansione della libertà di espressione attraverso *internet*: al considerando n. 9 viene, infatti, affermato che «la libera circolazione dei servizi della società dell'informazione può in numerosi casi riflettere specificamente nel diritto comunitario un principio più generale, e cioè la libertà di espressione prevista dall'art. 10, paragrafo 1, della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali [...]» e che sono possibili restrizioni soltanto conformemente all'art. 10, par. 2 della CEDU (ovvero purchè siano previste dalla legge e costituiscano misure necessarie, in una società democratica, alla sicurezza nazionale, all'integrità territoriale o alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario) e all'art. 46, par. 1, TCE [oggi art.

52, par. 1, TFUE] (ovvero per motivi di ordine pubblico, pubblica sicurezza e sanità pubblica). All'esenzione di responsabilità dei PSI corrisponde, quindi, una libertà di espressione concepita in termini piuttosto ampi, non essendovi un obbligo di autorizzazione preventiva per la diffusione delle informazioni *online*, ma al contrario solo di rimozione quando il PSI abbia la consapevolezza dell'illiceità dei contenuti trasmessi o ospitati.

La Direttiva sul commercio elettronico, inoltre, parla genericamente di informazioni o contenuti illegali, ma senza darne una precisa definizione: tale categoria pare ricomprendere ciò che è contrario al diritto nazionale e dell'Unione europea, ivi incluso le violazioni *online* del diritto d'autore, dei marchi e dei segreti commerciali, la contraffazione e la distribuzione parallela non autorizzata via *internet*, le violazioni della tutela dei consumatori, della *privacy*, delle norme circa la diffamazione e la calunnia nonché della protezione dei dati, i discorsi di odio e incitamento alla violenza (ad esempio, contenuti terroristici), la diffusione di materiale pedopornografico nonché di immagini sessuali private senza consenso. Non vi rientrano, invece, i c.d. *harmful contents*, ovvero quei contenuti che, pur non essendo espressamente vietati per legge, possono avere in ogni caso effetti nocivi, quali molestie verbali, messaggi di bullismo o diffusione di *fake news* (pur rimanendo all'interno dei limiti della libertà di espressione)¹⁵.

La Corte di giustizia è intervenuta interpretando la direttiva in modo da ridurre lo spazio di libertà dei PSI a favore di una maggiore protezione degli utenti dai contenuti di odio *online*: con la pronuncia *Glawisching-Piesczek*, ad esempio, ha sancito il potere dei giudici nazionali di imporre agli ISP di rimuovere le informazioni memorizzate e il cui contenuto sia identico a quello di un'informazione precedentemente dichiarata illecita o di bloccare l'accesso alle medesime, qualunque sia l'autore della richiesta di memorizzazione di siffatte informazioni¹⁶.

Nonostante l'opera di modernizzazione della Corte di giustizia, improntata ad una maggiore sensibilità nei confronti degli utenti delle piattaforme digitali e in generale dei PSI, la Direttiva rivela ormai la necessità di un importante aggiornamento, affidato al *Digital services act* (su cui v. *infra*).

1.2 La responsabilizzazione dei PSI attraverso gli strumenti di *soft law*

In tempi più recenti, l'azione dell'Unione europea è stata indirizzata alla promozione della responsabilizzazione dei PSI attraverso l'invito all'adozione di

¹⁵ Cfr. Lo studio del Parlamento europeo *Reform of the EU liability regime for online intermediaries*, maggio 2020, p. 10.

¹⁶ Cfr. Corte giust., 3 ottobre 2019, causa C-18/18, *Glawischning-Piesczek c. Facebook Ireland Limited*, ECLI:EU:C:2019:821. Sul punto si veda la ricostruzione di G. MORGESE, *op. cit.*, spec. p. 83 ss.

codici di autoregolamentazione e altri strumenti di *soft law*.

Nel dicembre del 2015, ovvero subito dopo gli attentati terroristici di matrice islamica avvenuti a Parigi il 13 novembre dello stesso anno, la Commissione ha avviato un progetto, l'*EU Internet Forum*, per unire forze politiche, istituzioni e aziende informatiche nella lotta contro la diffusione di contenuti terroristici e di odio *online*¹⁷.

Successivamente, il 31 maggio 2016, la Commissione ha promosso l'adozione, da parte di quattro tra le principali aziende informatiche (Facebook, Twitter, YouTube e Microsoft), di un codice di condotta per lottare contro forme illegali di incitamento all'odio *online*. Tale strumento è stato adottato, in seguito, anche da Google, Instagram, Snapchat, Dailymotion e Webedia.

Secondo questo codice di condotta, le aziende, in prima battuta, sono tenute ad adottare regole per la censura dell'istigazione alla violenza e a comportamenti improntati all'odio. Esse, inoltre, hanno l'obbligo di predisporre procedure chiare ed efficaci per esaminare eventuali segnalazioni riguardanti forme illegali di incitamento all'odio nei servizi da loro offerti, in modo da poter rimuovere tali contenuti o disabilitarne l'accesso.

In caso di segnalazione da parte degli utenti, i PSI interessati procedono ad un attento esame delle stesse, entro 24 ore, alla luce delle regole predisposte e delle disposizioni di legge applicabili (in particolare, per quanto riguarda il recepimento della Decisione Quadro, su cui v. *infra*). Ove necessario, i PSI provvedono alla rimozione dei contributi o al blocco dell'accesso agli stessi.

La Commissione effettua un monitoraggio periodico dell'applicazione di questi codici di condotta. Da quanto emerge dalla settima valutazione, relativa al 2022, la media delle segnalazioni riviste entro le 24 ore, pari al 64,4% del 2022, è decisamente diminuita rispetto agli anni precedenti, ovvero pari all' 81% nel 2021 e al 90,4% nel 2020. Soltanto la piattaforma Tik Tok ha migliorato la propria performance nella gestione della risposta alle segnalazioni. La rimozione dei contenuti si è poi verificata nel 63,6% dei casi, in continuità rispetto a quanto avvenuto nel 2021 (ove la media è stata del 62,5%), ma comunque in calo rispetto ai precedenti del 2019 e del 2020¹⁸.

Sebbene l'adozione di tali codici di condotta rappresenti un segnale positivo circa la volontà degli ISP di avere un ruolo attivo nella lotta all'odio *online* nonché alla diffusione di contenuti illegali o nocivi, si tratta pur sempre di un impegno del tutto volontario da parte delle aziende coinvolte, senza che possa esservi alcuno strumento di coercizione da parte delle pubbliche autorità. Inoltre, come evidenziato ripetutamente dalla più attenta dottrina, in questo

¹⁷ Cfr. *EU Internet Forum: Bringing together governments, Europol and technology companies to counter terrorist content and hate speech online*, Press Release, 3 dicembre 2015.

¹⁸ Cfr. Settimo monitoraggio dell'applicazione del Codice di condotta, Comunicato Stampa della Commissione europea, 24 novembre 2022, IP/22/7109.

modo aziende private sono chiamate a svolgere, in completa autonomia, il compito di un vero e proprio censore, ovvero ad effettuare un bilanciamento tra la tutela della libertà di espressione e gli altri diritti in gioco, al momento di decidere se rimuovere o meno un contenuto, finendo per agire quali pubbliche autorità¹⁹.

Sempre in ambito di *soft law*, il 28 settembre 2017 è stata pubblicata una Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, dal titolo «Lotta ai contenuti illeciti *online*. Verso una maggiore responsabilizzazione delle piattaforme *online*», seguita poi dalla Raccomandazione 2018/334 del 1° marzo 2018 sulle misure per contrastare efficacemente i contenuti illegali *online*. La Comunicazione del 2017 è una prima riflessione sul punto, mentre la raccomandazione è indirizzata agli Stati per promuovere l'adozione di misure specifiche da porre a carico degli operatori di *internet* che forniscono servizi di *hosting*.

L'obiettivo di questi strumenti è una forte responsabilizzazione dei prestatori di servizio, affinché questi agiscano per esaminare tutte le segnalazioni e rimuovere i contenuti illegali ed estendano la possibilità di segnalare eventuali contenuti illegali a tutti, non solo agli utenti di un determinato servizio o *social* registrati, quando si tratti di un contenuto visibile al pubblico. Gli ISP sono, inoltre, chiamati ad informare l'utente (autore della segnalazione) delle misure che sono state adottate e a dare la possibilità all'autore del contenuto di presentare un reclamo: tale possibilità si rivela sempre più importante, in quanto attualmente la rimozione di contenuti presunti illegali avviene tramite strumenti di intelligenza artificiale e algoritmi. Infine, grava sui PSI l'obbligo di segnalare alle autorità eventuali contenuti che si configurano come un reato.

1.3 La nuova direttiva sui media audiovisivi ed il regolamento relativo al contrasto della diffusione di contenuti terroristici *online*

Nel 2018 l'Unione europea è tornata ad utilizzare uno strumento normativo di *hard law* per rendere cogenti alcuni obblighi contenuti nei codici di condotta: si tratta della direttiva 2018/1808 che ha modificato la direttiva sui media audiovisivi²⁰. Tale strumento, il quale ha per base giuridica gli artt. 53, par. 1, e 62 TFUE, ovvero norme dirette a consentire l'adozione di strumenti per

¹⁹ Cfr. M. BASSINI, *Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione*, in *Rivista italiana di informatica e diritto*, 2021, p. 43 ss.

²⁰ Direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato, in *GUUE* L 303 del 28 novembre 2018, p. 69 ss.

il coordinamento delle disposizioni legislative, regolamentari e amministrative degli Stati membri relative all'accesso alle attività autonome e all'esercizio di queste, in regime di stabilimento o prestazioni di servizi, ha obiettivi più ampi rispetto alla lotta all'*hate speech*, ma detta importanti norme in tema, in modo da imporre giuridicamente obbligazioni assunte, fino a quel momento, in maniera solo volontaria dalle grandi piattaforme.

Il novellato art. 6 prevede ora che: «[f]ermo restando l'obbligo degli Stati membri di rispettare e proteggere la dignità umana, gli Stati membri assicurano mediante appositi mezzi che i servizi di media audiovisivi erogati dai fornitori di servizi di media soggetti alla loro giurisdizione non contengano: a) istigazione alla violenza o all'odio nei confronti di un gruppo di persone o un membro di un gruppo sulla base di uno dei motivi di cui all'articolo 21 della Carta; b) alcuna pubblica provocazione a commettere reati di terrorismo di cui all'articolo 5 della direttiva (UE) 2017/541. 2. Le misure adottate ai fini del presente articolo devono essere necessarie e proporzionate e rispettare i diritti e i principi sanciti dalla Carta». Dunque, gli Stati sono tenuti ad assicurarsi che le piattaforme per la condivisione di video adottino strumenti contro l'incitamento all'odio sulla base dei motivi di cui all'art. 21 della Carta, concretizzando molte delle indicazioni fornite dagli strumenti di *soft law*, con riferimento all'obbligo di adottare meccanismi di segnalazione e reclamo trasparenti e di facile uso.

Si tratta, tuttavia, di uno strumento settoriale, principalmente dedicato ai servizi che forniscono programmi al grande pubblico, sotto la responsabilità editoriale di un fornitore di servizi di media al fine di informare, intrattenere o istruire, attraverso reti di comunicazioni elettroniche, in radiodiffusione o a richiesta.

Nel richiamare le norme dirette a contrastare l'*hate speech* nell'ambito del diritto dell'Unione europea, occorre da ultimo ricordare uno strumento che prende in considerazione un particolare tipo di discorso di odio, quello legato alla diffusione di contenuti terroristici nonché all'istigazione di reati di terrorismo, ovvero il regolamento (UE) 2021/784 relativo al contrasto della diffusione di contenuti terroristici *online*²¹. Anche tale strumento ha come base giuridica l'art. 114 TFUE: in particolare, nel primo considerando, si fa riferimento al mercato unico digitale, il cui funzionamento dovrebbe essere migliorato rafforzando «la certezza del diritto per i prestatori di servizi di *hosting* e la fiducia degli utilizzatori nell'ambiente *online*, nonché potenziando le salvaguardie per la libertà di espressione, compresa la libertà di ricevere e

²¹Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio, del 29 aprile 2021, relativo al contrasto della diffusione di contenuti terroristici *online*, in *GUUE* L 172 del 17 maggio 2021, p. 79 ss.

comunicare informazioni e idee in una società aperta e democratica, e per la libertà e il pluralismo dei media». Il regolamento prevede, pertanto, norme comuni dirette al contrasto di contenuti terroristici *online*, fornendo una definizione piuttosto ampia di tale tipo di contenuti, considerando tali i materiali che « a) istigano alla commissione di uno dei reati di cui all'articolo 3, paragrafo 1, lettere da a) a i), della direttiva (UE) 2017/541 [ovvero, i reati di terrorismo]²², se tali materiali, direttamente o indirettamente, ad esempio mediante l'apologia di atti terroristici, incitano a compiere reati di terrorismo, generando in tal modo il pericolo che uno o più di tali reati siano commessi; b) sollecita[no] una persona o un gruppo di persone a commettere o a contribuire a commettere uno dei reati di cui all'articolo 3, paragrafo 1, lettere da a) a i), della direttiva (UE) 2017/541; c) sollecita[no] una persona o un gruppo di persone a partecipare alle attività di un gruppo terroristico, ai sensi dell'articolo 4, lettera b), della direttiva (UE) 2017/541; d) impartisca[no] istruzioni per la fabbricazione o l'uso di esplosivi, armi da fuoco o altre armi o sostanze nocive o pericolose, ovvero altri metodi o tecniche specifici allo scopo di commettere o contribuire alla commissione di uno dei reati di terrorismo di cui all'articolo 3, paragrafo 1, lettere da a) a i), della direttiva (UE) 2017/541; e) costituisca[no] una minaccia di commissione di uno dei reati di cui all'articolo 3, paragrafo 1, lettere da a) a i), della direttiva (UE) 2017/541».

Dovendo occuparsi di un fenomeno transfrontaliero, il regolamento detta poi norme dirette a regolare la competenza degli Stati (art. 16). Infine, detto regolamento prevede anche la possibilità di un ricorso giurisdizionale per il destinatario del provvedimento di censura statale.

²² In particolare, l'art. 3, par. 1, della direttiva (UE) 2017/541 prevede i seguenti reati: «a) attentati alla vita di una persona che possono causarne il decesso; b) attentati all'integrità fisica di una persona; c) sequestro di persona o cattura di ostaggi; d) distruzioni di vasta portata di strutture governative o pubbliche, sistemi di trasporto, infrastrutture, compresi i sistemi informatici, piattaforme fisse situate sulla piattaforma continentale ovvero di luoghi pubblici o di proprietà private che possono mettere in pericolo vite umane o causare perdite economiche considerevoli; e) sequestro di aeromobili o navi o di altri mezzi di trasporto collettivo di passeggeri o di trasporto di merci; f) fabbricazione, detenzione, acquisto, trasporto, fornitura o uso di esplosivi o armi da fuoco, comprese armi chimiche, biologiche, radiologiche o nucleari, nonché ricerca e sviluppo di armi chimiche, biologiche, radiologiche o nucleari; g) rilascio di sostanze pericolose o il cagionare incendi, inondazioni o esplosioni i cui effetti mettano in pericolo vite umane; h) manomissione o interruzione della fornitura di acqua, energia o altre risorse naturali fondamentali il cui effetto metta

in pericolo vite umane; i) interferenza illecita relativamente ai sistemi, ai sensi dell'articolo 4 della direttiva 2013/40/UE del Parlamento e del Consiglio (1) nei casi in cui si applica l'articolo 9, paragrafo 3 o l'articolo 9, paragrafo 4, lettere b) o c), di tale direttiva in questione e interferenza illecita relativamente ai dati, di cui all'articolo 5 di tale direttiva nei casi in cui si applica l'articolo 9, paragrafo 4, lettera c), di tale direttiva».

1.4 Il futuro della regolamentazione dell'*online hate speech*: il *Digital Services Act*

Attualmente, la lotta all'*hate speech* è sull'agenda della Commissione europea che ha adottato diverse iniziative, sia sul versante della regolamentazione dei contenuti, sia su quello dell'adozione di norme incriminatrici delle condotte penalmente rilevanti.

Nel dicembre 2020 la Commissione europea ha, infatti, pubblicato la comunicazione sul piano d'azione per la democrazia europea²³ (*European Democracy Action Plan*) e la proposta del *Digital Services Act* (DSA)²⁴, che costituiscono un punto di svolta nella disciplina europea del mercato dell'informazione digitale. Sul punto dei "discorsi d'odio", entrambi i documenti sembrano infatti muoversi nella direzione di un maggior rigore sotto due profili. Il primo profilo, su cui si concentra lo *European Democracy Action Plan*, si riflette nel progetto di estendere il raggio d'azione della criminalizzazione dei fenomeni d'odio a livello di Unione europea. Il secondo profilo, oggetto specifico della riforma proposta dal DSA, è, invece, quello relativo a una maggiore responsabilizzazione dei *provider* di servizi di intermediazione *online*. La proposta del DSA è stata pubblicata insieme a quella di regolamento relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali), il c.d. DMA²⁵. L'ambizioso progetto della Commissione è quello di ridisegnare con completezza il mercato unico digitale, con una disciplina che vada dalla regolazione dei servizi, alla concorrenza e alla tutela dei diritti fondamentali. Entrambi i regolamenti sono stati oggetto di un accordo tra Parlamento e Consiglio, il 25 marzo 2022 per il DMA e il 23 aprile 2022 per il DSA, e sono stati recentemente pubblicati in Gazzetta Ufficiale e sono ora una realtà nell'ordinamento dell'Unione europea²⁶.

Occorre ricordare che il DSA è stato fortemente voluto dal Parlamento

²³ Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni sul piano d'azione per la democrazia europea, 3 dicembre 2020, COM(2020) 790 final.

²⁴ Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, Bruxelles, 15 dicembre 2020, COM(2020)825 final, 2020/361 (COD).

²⁵ Proposta di regolamento del Parlamento europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali), Bruxelles, 15 dicembre 2020, COM(2020) 842 final, 2020/374 (COD).

²⁶ Cfr. Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali), in *GUUE* L, 265 del 12 ottobre 2022, p. 1 ss. e Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), cit.

europeo, che sulla base dell'art. 225 TFUE nel 2020 ha approvato due risoluzioni: la Risoluzione del PE recante raccomandazioni alla Commissione sulla legge sui servizi digitali: migliorare il funzionamento del mercato unico²⁷ e quella sull'atto sui servizi digitali e le questioni sollevate in materia di diritti fondamentali²⁸.

Molto interessante è – ai fini del presente contributo – la seconda risoluzione citata, la quale ha messo in luce, da un lato, che «la disinformazione e l'incitamento all'odio *online* si sono sempre più diffusi negli ultimi anni a causa di persone e soggetti perturbatori che utilizzano le piattaforme online per aumentare la polarizzazione, che a sua volta è sfruttata a fini politici; che le donne, le persone di colore, le persone appartenenti o percepite come appartenenti a minoranze etniche o linguistiche e le persone LGBTIQ sono spesso prese di mira da incitamenti all'odio discriminatorio, bullismo, minacce e ricerca di capri espiatori online» (par. F) e che «tale tendenza è stata favorita da piattaforme online il cui modello commerciale si basa sulla raccolta e l'analisi dei dati degli utenti finalizzate a generare più traffico e visualizzazioni nonché, di conseguenza, più dati di profilazione e quindi più profitto; che ciò porta all'amplificazione dei contenuti sensazionalistici; che l'incitamento all'odio e la disinformazione danneggiano l'interesse pubblico compromettendo il dibattito pubblico rispettoso e onesto e pongono minacce alla sicurezza pubblica dal momento che possono suscitare violenza nel mondo reale; che contrastare tali contenuti è fondamentale per garantire il rispetto dei diritti fondamentali e difendere lo Stato di diritto e la democrazia nell'UE» (par. G). Dall'altro lato, il Parlamento europeo ha evidenziato che «finora l'approccio politico volto a contrastare i contenuti illegali *online* nell'UE si è concentrato principalmente sulla cooperazione volontaria e su rimozioni autorizzate da provvedimenti giudiziari, ma che un numero crescente di Stati membri sta adottando ulteriori normative a livello nazionale che affrontano i contenuti illegali in maniera non armonizzata; che disposizioni volte a far fronte a taluni tipi di contenuti illegali sono state inserite nella recente normativa settoriale a livello dell'UE». Dunque, una prassi di autoregolamentazione non è sufficiente e attribuisce agli operatori privati un ruolo di autorità giudiziaria che non è opportuno affidare ai privati per i rischi di interferenza con il diritto alla libertà di espressione (lettera M). Inoltre «la sorveglianza e la supervisione a livello normativo sono settoriali nell'UE» mentre sarebbe utile un ulteriore coordinamento più globale tra i diversi organismi di sorveglianza in tutta l'UE (lettera N). La prospettiva è, quindi, quella di introdurre uno strumento orizzontale per la disciplina di tutte le

²⁷ 2020/2018 INL.

²⁸ 2020/2022 INI.

categorie di contenuti, prodotti, servizi e attività sui servizi intermediari.

Nel dicembre 2020²⁹, dunque, la Commissione europea ha scelto di proporre un regolamento, il DSA, per avere una sostanziale uniformizzazione delle regole, sulla base dell'art. 114 TFUE. Tale norma è in linea di principio utilizzata quale base giuridica di direttive, ai fini dell'armonizzazione, più che della "uniformizzazione" nell'ambito del mercato interno. Come rilevato nel secondo considerando dell'approvato regolamento, la presenza di diverse legislazioni nazionali per disciplinare un fenomeno tipicamente transfrontaliero, quale è quello di *internet*, incide negativamente sul mercato interno³⁰. In ogni caso, come rilevato in dottrina l'obiettivo dichiarato del DSA è il rafforzamento delle garanzie dei diritti fondamentali nel settore dei servizi digitali³¹: una prospettiva diametralmente opposta a quella della Direttiva sul commercio elettronico, che dimostra l'evoluzione delle sensibilità del legislatore comunitario (e non solo) sul tema.

Pur non essendo questa la sede per un'analisi compiuta delle norme del DSA e/o del DMA³², occorre sottolineare, ai fini del presente contributo, che il DSA, nello stabilire norme armonizzate sulla prestazione di servizi intermediari nel mercato interno³³, contiene norme dirette al contrasto all'*hate speech online* e, pur confermando in linea generale il regime di responsabilità limitata già delineato dalla direttiva 2000/31/CE per i servizi di *mere conduit*, *caching* e *hosting*, prevede una serie di obblighi aggiuntivi in capo ai *providers*, differenziati a seconda delle dimensioni dell'azienda coinvolta. Come sottolineato dalla più autorevole dottrina, tramite il DSA e il DMA l'Unione europea «mira a ridisegnare la cornice normativa e, dunque, gli obblighi e le responsabilità in capo alle piattaforme digitali *online*, tentando di contrastare, [...]

²⁹ Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, cit.

³⁰ Cfr. Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), in *GUUE L*, 277 del 27 ottobre 2022, p. 1 ss.

³¹ G. CAGGIANO, *La proposta di Digital Service Act per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, in *I Post di Aisdue*, 18 febbraio 2021, p. 1 ss., spec. p. 4

³² Per un'analisi del DSA e del DMA si v. (senza pretesa di completezza): A. ENGEL, X. GROUSOT, *The Digital Markets Act, A new era for competition law and fundamental rights in the EU digital single market*, in *EU Law Live, Weekend Edition*, 22 novembre 2022; M. EIFERT, A. METZGER, H. SCHWEITZER, G. WAGNER, *Taming the giants: the DMA/DSA package*, in *CMLR*, 2021, p. 987 ss.; G. CAGGIANO, *La proposta di Digital Service Act per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, in *I Post di Aisdue*, cit.; M. LARCHÈ, *Le Digital Services Act : un pas européen supplémentaire dans la lutte contre l'incitation à la haine et la violence sur les réseaux sociaux*, in *RAE*, 2021, p. 139 ss.; S. TOMMASI, *The liability of internet service providers in the proposed Digital Services Act*, in *European Review of Private Law*, 2021, p. 925 ss.; M. INGLESE, *L'economia collaborativa tra la giurisprudenza della Corte di giustizia e le prime proposte di armonizzazione: verso il Digital Markets Act e il Digital Services Act*, in *DUE*, 2020, p. 843 ss.

³³ Cfr. Art. 1 del DSA.

in una prospettiva più procedurale che assiologico-sostanziale, il consolidamento del potere digitale privato»³⁴.

Il DSA prevede una nozione piuttosto ampia di «contenuto illegale», nell'ambito del quale va senz'altro ricompreso il discorso di odio, trattandosi di «qualsiasi informazione che, di per sé o in relazione a un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme al diritto dell'Unione o di qualunque Stato membro, indipendentemente dalla natura o dall'oggetto specifico di tale diritto» (art. 3, lett. g). In buona sostanza, il DSA si basa sulla logica per cui «what is illegal offline should be illegal online»³⁵, inserendo finalmente una definizione di ciò che deve essere considerato come «contenuto illegale» e dunque colmando la lacuna della Direttiva sul commercio elettronico. Da notare che la definizione adottata dal DSA non prende in considerazione gli *harmful content*, ovvero, come già ricordato, quei contenuti che, pur non essendo illegali, sono comunque nocivi per i destinatari degli stessi, probabilmente per la difficoltà di raggiungere il consenso sui contenuti di tale nozione, anche per la grande varietà di posizioni degli Stati membri sul punto.

Il DSA si applica ai servizi della società dell'informazione, al pari della Direttiva sul commercio elettronico, aggiungendo, rispetto a quest'ultima, la definizione di servizio intermediario, ovvero ogni servizio consistente nel *mere conduit*, *caching* e *hosting* di informazioni (art. 3, lett. g). In particolare, il regolamento si applica ai servizi intermediari offerti a destinatari il cui luogo di stabilimento si trova nell'Unione o che sono ubicati nell'Unione, indipendentemente dal luogo di stabilimento dei PSI (art. 2, par. 1).

Quanto alla responsabilità dei PSI, il DSA conferma l'impianto della Direttiva sul commercio elettronico, replicando le norme sull'esonero della responsabilità per il semplice trasporto, la memorizzazione temporanea e la memorizzazione di informazioni (artt. 4,5,6). Si conferma, inoltre, che eventuali indagini volontarie svolte in buona fede e in modo diligente o azioni per il contrasto e/o la rimozione di contenuti illegali non comportano la perdita dell'immunità per i PSI (art. 7), secondo una versione europea del principio del «buon samaritano»³⁶. Una delle principali innovazioni, rispetto alla disciplina precedente, consiste nella differenziazione di obblighi e responsabilità a seconda delle dimensioni dell'ISP coinvolto.

In prima battuta, il DSA stabilisce obblighi comuni a tutti i fornitori di servizi di intermediazione digitale, senza distinzione alcuna sulla base della tipologia del servizio fornito né della dimensione (capo III, sezione 1): tra

³⁴ Cfr. O. POLLICINO, *Potere Digitale*, in *Enciclopedia del diritto*, cit., par. 10.

³⁵ Cfr. Editorial Comment, *The DMA and the DSA*, in *EU Law Live*, 26 ottobre 2022.

³⁶ Cfr. lo studio del Parlamento europeo *Reform of the EU liability regime for online intermediaries*, cit. p. 17.

questi, vi sono l'obbligo di istituire un punto di contatto unico per agevolare la comunicazione con le autorità degli Stati membri, la Commissione e il comitato europeo per i servizi digitali³⁷ (art. 11), nonché l'obbligo di designare un rappresentante legale nell'Unione per i prestatori stabiliti in Stati terzi (art. 13).

La sezione 2 del capo III prevede poi obblighi supplementari per i prestatori di servizi di memorizzazione delle informazioni, comprese le piattaforme *online*: in particolare, vi è l'obbligo di predisporre meccanismi che consentano a terzi di notificare presunti contenuti illegali e di reazione (art. 16), nonché un preciso obbligo di fornire una motivazione nel caso in cui si proceda con la rimozione (art. 17). Chiude questa sezione un articolo rubricato «notifica di sospetti di reati», il quale prevede che ove il prestatore di servizi di memorizzazione «venga a conoscenza di informazioni che fanno sospettare che sia stato commesso o si stia commettendo o probabilmente sarà commesso un reato che comporta una minaccia per la vita o la sicurezza di una o più persone» sia tenuto a informare senza indugio le autorità giudiziarie o di contrasto dello Stato interessato (art. 18). Tale articolo nella proposta di regolamento del dicembre 2020 era collocato nella sezione n. 3, dedicata alle piattaforme *online*: lo spostamento nella sezione precedente comporta una maggiore platea di destinatari per tale obbligo.

La sezione successiva, la n. 3 del capo III, prevede poi disposizioni aggiuntive per i fornitori di piattaforme *online*, imponendo loro di istituire un sistema interno di gestione dei reclami relativi alle decisioni adottate in relazione a presunti contenuti o informazioni *online* (art. 20); devono poi rivolgersi a organismi certificati per la risoluzione stragiudiziale di controversie (art. 21). Particolare attenzione deve poi essere riservata ai «segnalatori attendibili», ossia enti, certificati come tali, che dimostrino capacità e competenze particolari ai fini dell'individuazione, dell'identificazione e della notifica di contenuti illegali, siano indipendenti e presentino la segnalazione in modo diligente, accurato e obiettivo (art. 22). L'ultimo articolo della sezione è dedicato alla protezione dei minori, disponendo che i fornitori di piattaforme *online* adottino misure adeguate a tal fine (art. 28). La sezione 4 del capo III è dedicata alle piattaforme *online* che consentono ai consumatori di concludere contratti a distanza con operatori commerciali, prevedendo specifici obblighi anche per rispettare il diritto dell'Unione in materia di tutela dei consumatori e sicurezza dei prodotti.

Il regolamento prevede, poi, nella sezione 5 del capo III, obblighi più stringenti per fornitori di piattaforme *online* e per motori di ricerca *online* di dimensioni molto grandi per la gestione dei rischi sistemici. Per essere

³⁷ Istituito dall'art. 61 dello stesso DSA.

considerati «molto grandi» le piattaforme e i motori di ricerca devono avere un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a 45 milioni ed essere designati come tali dalla Commissione (art. 33). Tali enti devono compiere valutazioni di rischio con riferimento a rischi sistemici derivanti dal funzionamento e dall'uso dei loro servizi o ad essi connessi (art. 34) e adottare misure di attenuazione degli stessi (art. 35). Essi dovranno, inoltre, sottoporsi «a proprie spese e almeno una volta l'anno» a revisioni indipendenti.

Molto importanti sono le norme di cui alla sezione 5 del capo III che consentono alla Commissione europea di favorire e promuovere lo sviluppo e l'attuazione di norme europee armonizzate (art. 44) nonché l'elaborazione dei codici di condotta (artt. 45, 46 e 47). Il Comitato *ex art.* 61 può anche raccomandare alla Commissione di avviare l'elaborazione di protocolli per affrontare situazioni di crisi che incidono sulla sicurezza e sulla salute pubblica (art. 48).

Il capo IV del DSA disegna un nuovo ruolo per gli Stati membri e per le competenti autorità nazionali, ivi compresi i coordinatori dei servizi digitali, e questa è una delle novità più significative della nuova disciplina. Tali soggetti godono di ampi poteri di indagine in merito alla condotta dei PSI che ricadono nella competenza del loro Stato, tra cui eseguire ispezioni in loco e interrogare il personale di tali fornitori. I coordinatori dei servizi digitali potranno anche accettare gli impegni offerti dai fornitori, ordinare la cessazione delle violazioni riscontrate, imporre misure correttive e sanzioni pecuniarie (art. 51). Gli Stati, infatti, dovranno stabilire le norme relative alle sanzioni applicabili in caso di violazione del regolamento: tali sanzioni potranno essere quantificate entro il limite del 6% del fatturato annuo mondiale del fornitore di servizi in questione (art. 52). I destinatari dei servizi potranno, inoltre, presentare dei reclami e richiedere un risarcimento per i danni o le perdite subiti a causa della violazione degli obblighi da parte del fornitore di servizi intermediari (artt. 52 e 53). La Commissione europea dispone, poi, di poteri esclusivi per la vigilanza e l'applicazione del regolamento con particolare riferimento alle piattaforme e ai motori di ricerca di grandi dimensioni (art. 56 ss.) e vi sono norme dedicate al coordinamento con le autorità nazionali.

In conclusione, si può affermare che il DSA ridisegna gli obblighi degli ISP mediante una maggiore responsabilizzazione, crescente in proporzione alle dimensioni dello stesso fornitore, prevedendo al tempo stesso maggiori poteri per le autorità nazionali e dell'Unione in modo da creare un quadro di riferimento e di controllo dei PSI, sperimentando nuovi intrecci di potere pubblico e privato.

Il nuovo regolamento, entrato in vigore il ventesimo giorno seguente alla

pubblicazione, sarà applicabile a partire dal 17 febbraio 2024³⁸. Spetta ora a Stati, istituzioni e ISP adeguarsi alle nuove regole e creare un nuovo volto del mercato unico digitale.

2. L'azione dell'Unione nei confronti delle condotte penalmente rilevanti

Dopo aver ricostruito il contenuto delle principali fonti di regolamentazione della condotta dei PSI nell'ambito del mercato interno, occorre ora analizzare gli strumenti per il contrasto all'odio *online* attraverso l'adozione di norme dirette all'incriminazione delle condotte penalmente rilevanti.

2.1 La Decisione Quadro: la lotta contro le condotte di odio attraverso il diritto penale

Qualche anno dopo l'adozione della Direttiva sul commercio elettronico, l'Unione europea ha adottato la già ricordata Decisione Quadro che obbliga gli Stati membri a punire le condotte di odio, indipendentemente dal fatto che siano *online* o *offline*, ove essere siano forme ed espressioni di razzismo e xenofobia. L'obiettivo di questo strumento era, infatti, che i reati di stampo razzista e xenofobo fossero passibili di sanzioni penali efficaci, proporzionate e dissuasive in tutti gli Stati membri, secondo quanto riportato dal considerando n. 13.

La Decisione Quadro precisa, al considerando n. 9, che la nozione di «odio» dovrebbe essere intesa come riferita «all'odio basato sulla razza, il colore, la religione, l'ascendenza o l'origine nazionale o etnica», escludendo l'odio per motivi diversi da quelli indicati, come la disabilità, il sesso, l'identità di genere.

La Decisione Quadro è diretta a garantire che gravi manifestazioni di razzismo e xenofobia siano punibili con sanzioni effettive, proporzionate e dissuasive nell'Unione europea, tramite l'armonizzazione della legislazione penale. Tra le basi giuridiche utilizzate vi è l'art. 29 TUE, introdotto dal Trattato di Amsterdam per costruire uno spazio di libertà, sicurezza e giustizia sviluppando un'azione comune nel settore della cooperazione di polizia e giudiziaria in materia penale e prevenendo e reprimendo il razzismo e la xenofobia, nonché l'art. 31 e l'art. 34, par. 2, lett. b), diretti a consentire al Consiglio l'adozione di decisioni quadro per il ravvicinamento delle legislazioni nell'ambito della cooperazione giudiziaria penale.

All'art. 1, par. 1, lett. a) la Decisione Quadro sancisce il dovere per gli Stati di rendere punibili i comportamenti intenzionali consistenti nella «istigazione

³⁸ Il DSA non abroga la Direttiva sul commercio elettronico, ma la modifica: essa rimane vigente, tranne gli articoli da 12 a 15 (ovvero la disciplina in materia di responsabilità dei PSI) che vengono riscritti come riportato nel testo dal DSA.

pubblica alla violenza o all'odio nei confronti di un gruppo di persone, o di un suo membro, definito in riferimento alla razza, al colore, alla religione, all'ascendenza o all'origine nazionale o etnica», mentre all'art. 4 viene affermato che «per i reati diversi da quelli di cui all'art. 1 e 2 [ovvero i reati di istigazione all'odio e apologia, negazione o minimizzazione dei crimini di genocidio e contro l'umanità] gli Stati membri adottano le misure necessarie affinché la motivazione razzista o xenofoba sia considerata una circostanza aggravante o, in alternativa, affinché tale motivazione possa essere presa in considerazione dal giudice all'atto della determinazione della pena». In tali due articoli, sono state ravvisate le definizioni di *hate speech* ed *hate crime*³⁹, sebbene paiano ancora non del tutto complete e precise, soprattutto con riferimento alla seconda, poiché la decisione quadro pare riferirsi principalmente ad aggravanti piuttosto che alla definizione di reati compiuti per un motivo di odio.

Si tratta in ogni caso di uno strumento di armonizzazione minima, potendo gli Stati decidere di ampliare la sfera dei motivi di odio tali da giustificare una repressione penale⁴⁰. La Decisione Quadro opera, infatti, un delicato bilanciamento tra la libertà di espressione e la lotta contro il razzismo e la xenofobia, con una decisa preferenza per tale secondo obiettivo, inserendosi in un contesto di profonda divergenza quanto alle tradizioni culturali e giuridiche degli Stati membri.

La Decisione Quadro ha avuto una lunga gestazione, ben sette anni, dovuta principalmente alle differenze nazionali quanto al livello di tutela della libertà di espressione ed al bilanciamento con altri valori e diritti⁴¹. Parimenti, la trasposizione di tale strumento negli Stati membri si è rivelata piuttosto difficoltosa, al pari della sua adozione. Nel 2014, la Commissione europea ha evidenziato che diversi Stati membri non avevano recepito in pieno o correttamente le disposizioni della decisione quadro, in particolare quelle sui reati di negazione, apologia o minimizzazione grossolana di determinati crimini. Inoltre, secondo la Commissione, le disposizioni sull'istigazione all'odio, o alla violenza, di stampo razzista e xenofobo vigenti negli Stati membri non sono sempre del tutto conformi alla decisione quadro, sussistendo diverse lacune⁴². Per porre rimedio a tale situazione, la Commissione preannunciava

³⁹ Cfr. Study to support the preparation of the European Commission's initiative to extend the list of EU crimes in Article 83 of the Treaty on the Functioning of the EU to hate speech and hate crime, cit. spec. p. 32 e 36.

⁴⁰ *Ibidem*, pag. 28.

⁴¹ Cfr. Relazione della Commissione al Parlamento e al Consiglio sull'attuazione della decisione quadro 2008/913/GAI

⁴² Relazione della Commissione al Parlamento europeo e al Consiglio sull'attuazione della decisione quadro 2008/913/GAI del Consiglio sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale, 27 gennaio 2014, COM/2014/027 final.

una serie di colloqui bilaterali con gli Stati interessati. Lo Stato italiano ha provveduto alla trasposizione solo nel 2017, mediante la Legge europea di quell'anno, con notevole ritardo⁴³.

Nel 2020 la Commissione ha avviato una lettera di messa in mora *ex art.* 258 TFUE a Romania e ad Estonia per la non corretta trasposizione della decisione quadro: in particolare, l'Estonia non avrebbe qualificato come reato alcune forme specifiche di incitamento all'odio quali l'apologia pubblica e la negazione o la minimizzazione dell'Olocausto o di crimini internazionali ove tali condotte si rivelino istigatrici di violenza e odio. Inoltre, detto Stato non avrebbe qualificato correttamente come reato la condotta di istigazione alla violenza o all'odio nei confronti di gruppi, né inserito la motivazione razzista e xenofoba come circostanza aggravante nel proprio codice penale. La Romania, invece, non avrebbe fornito una definizione corretta di "incitamento all'odio" e avrebbe omesso altresì di incriminare tale condotta ove configurata nei confronti di un singolo appartenente ad un gruppo di persone definito con riferimento a razza, colore della pelle, religione, discendenza, origine nazionale o etnica⁴⁴. L'anno successivo, la Commissione europea ha inviato una lettera di messa in mora in altri cinque Stati, ovvero Polonia, Belgio, Svezia, Finlandia e Bulgaria, sempre per la non corretta trasposizione della Decisione Quadro⁴⁵.

Le difficoltà nell'adozione, nonché nell'attuazione di tale strumento, dimostrano la delicatezza del bilanciamento operato in presenza di tradizioni profondamente diverse tra gli Stati, ove la libertà di espressione trova tutela secondo diversi livelli.

2.2 L'inserimento di *hate speech* e *hate crime* tra i reati europei: una nuova proposta della Commissione europea

Recentemente, la Commissione europea è tornata ad indirizzare la propria azione verso l'utilizzo del diritto penale per il contrasto all'*hate speech* (non solo *online*).

Nel settembre del 2020, la Presidente della Commissione europea, Ursula Von Der Leyen annunciava il proprio obiettivo di estendere la lista dei reati "europei" per condannare «tutte le forme di crimini d'odio e incitamento all'odio»⁴⁶, ovvero *hate crimes* e *hate speech*, nella versione inglese dello stesso documento.

Successivamente, nel dicembre dello stesso anno, nella propria

⁴³ Legge 20 novembre 2017, n. 167, Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017 (artt. 5, 6, 24).

⁴⁴ Cfr. Commissione europea, comunicato stampa, 30 ottobre 2020, INF/20/1687.

⁴⁵ Cfr. Commissione europea, comunicato stampa, 18 febbraio 2021, INF/21/441.

⁴⁶ Cfr. State of the Union 2020, Bruxelles, 16 settembre 2020.

Comunicazione sul piano d'azione per la democrazia europea⁴⁷, la Commissione europea illustrava una vasta gamma di proposte e iniziative dirette a promuovere un più salubre ambiente digitale e informativo. In particolare, per quanto rileva ai fini del presente contributo, la Commissione europea, al fine di incoraggiare una più ampia ed eguale partecipazione democratica, prevedeva espressamente l'intenzione di compiere ulteriori sforzi nella lotta contro le fattispecie di *hate speech* digitale. Secondo il documento, la presenza in *internet* di forme di incitamento all'odio avrebbe, infatti, l'effetto di dissuadere le minoranze da esse colpite dall'esprimere le loro opinioni in rete e dal partecipare al discorso pubblico⁴⁸. La Commissione annunciava, pertanto, un'iniziativa per ampliare la sfera dei reati di cui all'art. 83, par. 1, TFUE per i quali è consentito a Parlamento e Consiglio stabilire norme minime di ravvicinamento delle legislazioni nazionali⁴⁹.

Secondo quanto stabilito dal primo comma di questa norma, l'intervento normativo del legislatore europeo è consentito quando si tratti di «sfere di criminalità particolarmente grave», vi sia una «dimensione transnazionale» di tali reati o, in ogni caso, una «particolare necessità di combatterli su basi comuni». Attualmente, la lista tassativa di cui all'art. 83, par. 1, comma 2, TFUE include i reati di terrorismo, tratta degli esseri umani e sfruttamento sessuale delle donne e dei minori, traffico illecito di stupefacenti, traffico illecito di armi, riciclaggio di denaro, corruzione, contraffazione di mezzi di pagamento, criminalità informatica e criminalità organizzata. Il terzo comma dell'art. 83, par. 1, TFUE prevede, tuttavia, che «in funzione dell'evoluzione della criminalità» il Consiglio possa individuare altre sfere di criminalità che rispondano ai criteri di cui al comma 1, mediante una decisione da adottare all'unanimità, previa approvazione del Parlamento europeo. La proposta della Commissione avrebbe, dunque, l'effetto di aggiungere al novero di tali «reati dell'Unione europea» anche i crimini d'odio e l'incitamento all'odio.

Nel dicembre 2021 la Commissione europea ha effettivamente adottato una nuova comunicazione e una proposta per avviare l'*iter* di inserimento di nuove fattispecie nell'elenco dei «reati europei» di cui all'art. 83, par. 1, TFUE⁵⁰. Il primo passo a tal fine è l'adozione, da parte del Consiglio, di una decisione che identifichi le condotte di *hate speech* e di *hate crime* come una sfera di criminalità tale da rendere necessaria una regolamentazione europea.

⁴⁷ Cfr. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni sul piano d'azione per la democrazia europea, cit.

⁴⁸ *Ibidem*, par. 2.4.

⁴⁹ Per un'analisi completa dell'art. 83 TFUE si v. C. AMALFITANO, *Art. 83 TFUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, Milano, 2014, p. 896 ss.

⁵⁰ Commissione europea, *Un'Europa più inclusive e protettiva: estendere l'elenco dei reati riconosciuti dall'UE all'incitamento all'odio e ai reati generati dall'odio*, cit.

Successivamente, la Commissione potrà adottare una proposta di direttiva diretta a stabilire regole minime per la definizione e l'incriminazione delle condotte di *hate speech* e *hate crime*.

La comunicazione illustra le motivazioni alla base di questa proposta.

In prima battuta, la Commissione sottolinea come la lotta all'*hate speech* e all'*hate crime* sia una delle priorità dell'Unione europea, richiamando le diverse iniziative già adottate: dalla Decisione Quadro, al Codice di Condotta per i PSI, dal Regolamento circa i contenuti terroristici *online* all'*EU internet forum* e al DSA⁵¹.

Nonostante gli strumenti già in essere, la Commissione ritiene che sia necessaria l'adozione di un atto per estendere la lista dei reati di cui all'art. 83 TFUE, in quando *hate speech* e *hate crime* si configurerebbero come un'area di criminalità particolarmente grave. Secondo la Commissione, infatti, questo tipo di fattispecie si porrebbe in netto contrasto con i valori ed i diritti fondamentali dell'Unione europea, racchiusi dall'art. 2 e dall'art. 6 TUE. La Commissione richiama anche la giurisprudenza della Corte EDU per rafforzare l'idea che si tratta di condotte particolarmente lesive dell'integrità fisica e morale di una persona⁵².

Hate speech e *hate crime* violerebbero, soprattutto, il diritto fondamentale alla dignità e all'uguaglianza delle persone nonché il diritto alla libertà di espressione, con un forte impatto sulla persona e sulla sua comunità di appartenenza⁵³.

Secondo la Commissione, tali condotte avrebbero una forte dimensione sociale, costituendo una seria minaccia per i valori democratici, la stabilità e la pace della società. Esse impatterebbero, inoltre, negativamente sulla libertà di espressione, poiché le vittime potrebbero essere dissuase dall'utilizzo dei *social media* in ragione dei contenuti di odio ivi riportati⁵⁴. Nella propria comunicazione, la Commissione riporta esempi di *hate speech* e di *hate crime* riferiti, *inter alia*, a persone LGBTIQ, di origine asiatica, rom o africana, nonché legati a fenomeni di antisemitismo⁵⁵.

La comunicazione analizza, poi, gli altri elementi per giustificare la proposta, ovvero l'attuale normativa penale degli Stati membri e la dimensione transazionale del fenomeno⁵⁶. Nell'analizzare l'evoluzione della criminalità, la Commissione riferisce che nel 2019 il Parlamento europeo ha invitato gli Stati membri a condannare le condotte di *hate speech* e di *hate crimes* dei politici,

⁵¹ *Ibidem*, par. 2.

⁵² *Ibidem*, par. 3.2

⁵³ *Ibidem*.

⁵⁴ *Ibidem*, par. 3.2.3.

⁵⁵ *Ibidem*, par. 3.2.4.

⁵⁶ *Ibidem*, parr. 3.2.5 e 3.3.

poiché rafforzerebbero il clima di odio nella società. Inoltre, sottolinea come la pandemia da Covid-19 abbia provocato «uno tsunami di odio xenofobia»⁵⁷.

La Commissione ritiene, dunque, che l'iniziativa diretta ad ampliare la lista di reati di cui all'art. 83 TFUE e quindi a consentire l'adozione di norme minime in materia penale da parte dell'Unione sia «la risposta più efficace, a livello dell'UE, alle sfide individuate» in quanto «solo un'iniziativa comune a livello dell'UE può proteggere efficacemente i valori comuni sanciti dall'art. 2 TUE che sono minacciati da tutte le forme di incitamento all'odio e di reati generati dall'odio»⁵⁸. Tale conclusione non sarebbe rimessa in discussione dalla possibile sovrapposizione con i reati già previsti dall'art. 83 TFUE, come i reati informatici o il terrorismo.

Le motivazioni illustrate dalla Commissione non appaiono del tutto del tutto convincenti, suscitando più di una perplessità.

In primo luogo, la Commissione non spiega in alcun modo come la nuova normativa in tema di *hate speech* e di *hate crime* dovrà essere coordinata con la Decisione Quadro. Vi sarà un'evidente sovrapposizione tra i due strumenti, in quanto entrambi sono diretti all'incriminazione delle medesime condotte: se la Decisione Quadro colpisce le condotte di odio di contenuto razzista o xenofobo, la nuova normativa dell'Unione europea dovrebbe comprendere una sfera più ampia, tale da includere i motivi legati all'orientamento sessuale, al sesso, alla disabilità, alla religione. La stessa Commissione pare contraddirsi nella misura in cui, nel registrare un aumento dei fenomeni di odio nei tempi recenti, come sopra ricordato, fa riferimento a episodi dal contenuto razzista o antisemita che dovrebbero già essere coperti dalla Decisione Quadro⁵⁹ e che pertanto non necessitano di una nuova normativa. Ciò potrebbe significare che tale strumento non è del tutto adeguato, ma in tal caso la Commissione dovrebbe precisare quali sono le fattispecie che non sono attualmente coperte dalla disciplina del 2008 con riferimento ai contenuti di odio razzista e xenofobo.

La Commissione, inoltre, non affronta il tema della tutela della libertà di espressione e di manifestazione del pensiero: l'unico cenno a tale diritto è fatto dalla Commissione con riferimento alla prospettiva delle potenziali vittime di *hate speech* e *hate crime*, che potrebbero essere dissuase dall'esprimersi liberamente, anche sui social, per il timore delle condotte di odio altrui. Al contrario, la Commissione non illustra in alcun modo il bilanciamento che sarà effettuato dalla nuova disciplina dell'Unione europea con la libertà di

⁵⁷ *Ibidem*, par. 3.4.

⁵⁸ *Ibidem*, par. 4.1

⁵⁹ Cfr. ancora il già menzionato par. 3.2.4.

espressione degli altri soggetti, ovvero il limite da non superare per non incorrere in sanzioni per condotte di *hate speech*, tradizionale dilemma in questo ambito⁶⁰.

Anche la valutazione della proporzionalità della proposta non pare effettuata in maniera esaustiva: trattandosi dell'introduzione di norme di carattere penale, la Commissione avrebbe dovuto spiegare con maggiore precisione le ragioni per cui gli attuali strumenti di contrasto alle condotte di odio non paiono sufficienti a raggiungere l'obiettivo prefissato.

La proposta della Commissione pare, almeno con riferimento all'*hate speech*, diretta all'introduzione di un reato di opinione⁶¹ a livello europeo difficilmente accettabile per la mancanza di precisione nella determinazione delle condotte oggetto di incriminazione e per le criticità legate al bilanciamento con la libertà di espressione effettuato in modo diverso in ogni ordinamento europeo.

Nella riunione del 3-4 marzo 2022, il Consiglio Giustizia e Affari interni ha accolto favorevolmente l'iniziativa della Commissione, impegnandosi a lavorare per raggiungere quanto prima l'unanimità richiesta.

Recentemente, il Comitato economico e sociale (CESE)⁶² ed il Comitato delle Regioni (CdR)⁶³ hanno espresso un parere favorevole circa la proposta della Commissione, ritenendo che l'incitamento all'odio e i reati generati dall'odio costituiscano sfere di criminalità che rispondono ai criteri di cui all'art. 83, par. 1, TFUE.

In particolare, il CESE ritiene pertinente considerare tali fattispecie «come una sfera di criminalità che ha una “sostanza” comune, basata sull'odio motivato da pregiudizi che prende di mira persone o gruppi» e di chiara di attendere «con impazienza lo sviluppo di una definizione di incitamento all'odio e di reato generato dall'odio come prossimo passo [...]. Tale definizione è fondamentale per la certezza del diritto, ma anche per la tutela dei diritti fondamentali e per assicurare una solida comunicazione generale»⁶⁴. Viene inoltre evidenziata l'importanza, nel definire l'incitamento all'odio e i reati generati dall'odio, nonché le relative sanzioni, di chiarire la loro relazione con i diritti fondamentali nel loro insieme: correttamente, il CESE sottolinea il delicato rapporto con la libertà di espressione e di informazione⁶⁵. Considerando

⁶⁰ Cfr. M. PELISSERO, *La parola pericolosa. Il confine incerto del controllo penale del dissenso*, in *Questione Giustizia*, 2015, p. 1 ss.

⁶¹ Sulle criticità di questo tipo di norme incriminatrici si v. A. SPENA, *Libertà di espressione e reati di opinione*, in *Riv. It. Dir. e Proc. Penale*, 2007, p. 689 ss.

⁶² Cfr. Parere del Comitato economico e sociale europeo, in *GUUE* C 323 del 26 agosto 2022, p. 83 ss.

⁶³ Cfr. Parere del Comitato delle Regioni, in *GUUE* C 79 del 2 marzo 2023, p. 79 ss.

⁶⁴ Cfr. Parere del CESE cit, punti 3.5 – 3.7.

⁶⁵ *Ibidem*, punto 3.11.

l'esperienza della Decisione Quadro 2008/913/GAI, il CESE considera che le difficoltà nel recepimento e nell'attuazione potrebbero ripetersi, invitando ad una maggiore cooperazione con i governi, i parlamenti e gli attori della società civile degli Stati membri⁶⁶.

Sulla stessa linea il parere del CdR, che ha espresso il proprio favore circa la proposta della Commissione, rilevando la preoccupazione per l'istigazione all'odio scientemente propagata da Paesi Terzi⁶⁷ nonché constatando che «le norme attualmente in vigore [...] non sono sufficienti a garantire che i fornitori di servizi Internet facciano la loro parte nel combattere e prevenire efficacemente l'incitamento all'odio da parte degli utenti dei loro servizi»⁶⁸. Al tempo stesso, il CdR sottolinea che «tra la lotta contro l'incitamento all'odio e la censura il confine è spesso sottile. Nel preparare soluzioni giuridiche per combattere l'incitamento all'odio e i reati generati dall'odio, si dovrebbe fare attenzione a garantire il diritto alla libertà di espressione»⁶⁹. In maniera piuttosto singolare, infine, il CdR dopo aver osservato che a livello internazionale non esiste una definizione omogenea dei reati generati dall'odio «chiede di sviluppare la giurisprudenza in materia e, di conseguenza, accrescere l'efficacia del perseguimento penale dell'incitamento all'odio e dei reati generati dall'odio»⁷⁰, sebbene chiarimenti in tema dovrebbero essere forniti dal legislatore, più che dai giudici, in ossequio al principio di legalità.

3. Osservazioni conclusive

Nel presente contributo si è cercato di delineare l'evoluzione dei principali strumenti di diritto dell'Unione europea per il contrasto all'*online hate speech*, attraverso le direttrici della regolamentazione del mercato interno da un lato, dalla Direttiva sul commercio elettronico al DSA, ed il ricorso al diritto penale europeo dall'altro lato, dalla Decisione Quadro alla recente proposta della Commissione europea di estendere l'elenco dei reati riconosciuti dall'Unione europea ai sensi dell'art. 83 TFUE all'incitamento all'odio e ai reati generati dall'odio.

Gli sviluppi più recenti mostrano una rinnovata attenzione nei confronti del fenomeno: il DSA porterà ad una nuova responsabilizzazione per i PSI, con obblighi sempre più stringenti a seconda delle dimensioni e delle funzioni dell'ente coinvolto e per questa via vi sarà una maggiore attenzione alla moderazione dei contenuti e alla eventuale rimozione degli stessi, ove si concretizzino in un discorso d'odio. In questa attività di controllo, vi sarà anche un

⁶⁶ *Ibidem*, punto 3.15.

⁶⁷ Cfr. Parere Cdr, cit., punto 10.

⁶⁸ *Ibidem*, punto 16

⁶⁹ *Ibidem*, punto 39.

⁷⁰ *Ibidem*, punto 40.

ruolo rinnovato per gli Stati, chiamati – tra l'altro – ad introdurre delle sanzioni pecuniarie per la violazione del DSA, nonché per la Commissione e l'apposito comitato creato dallo stesso regolamento, con una nuova interazione tra potere pubblico e privato.

Meno convincente appare l'iniziativa legata all'estensione dei reati di cui all'art. 83 TFUE includendo le condotte di *hate speech* e *hate crime*. Se, da un lato, tale proposta costituisce un'importante testimonianza della volontà di proseguire il contrasto all'*hate speech* attraverso strumenti di *hard law* e addirittura mediante il ricorso all'adozione di fattispecie incriminatrici, in maniera da raggiungere obiettivi non sufficientemente perseguibili mediante atti di *soft law*, dall'altro lato non mancano aspetti problematici.

Una prima criticità è legata alla difficoltà definitoria del fenomeno, nonché alla sovrapposizione con altri strumenti europei (in particolare, con la Decisione Quadro), in quanto non appare sufficientemente definita la condotta oggetto delle possibili nuove fattispecie incriminatrici, né precisamente delineati i confini rispetto alla legislazione già vigente.

In secondo luogo, è dubbio che sussistano tutti i requisiti di cui all'art. 83, par. 1, TFUE ai fini dell'inserimento di *hate speech* e *hate crime* nella lista dei reati di cui al par. 2. Se non si può dubitare del carattere transazionale delle fattispecie, soprattutto per i reati di *hate speech online*, anche per la rapida diffusione di idee e contenuti, nonché della necessità di combatterli su basi comuni, maggiori criticità emergono con riferimento alla considerazione di tali reati come appartenenti alla sfera di criminalità particolarmente grave. Non vi è una definizione di tale concetto a livello europeo, sebbene possa ritenersi configurabile in presenza di elementi quali una forte disapprovazione sociale e un significativo impatto sull'ordine pubblico⁷¹. Appare evidente che le condotte di *hate speech* e di *hate crime* sono profondamente diverse da questo punto di vista, in particolare con riferimento all'impatto sull'ordine pubblico: non pare potersi parlare di «sfera di criminalità particolarmente grave» con riferimento all'*hate speech*, soprattutto se paragonato agli altri crimini di cui all'art. 83, par. 2, TFUE, quali, ad esempio, terrorismo, tratta degli esseri umani e sfruttamento sessuale di donne e minori.

Infine, non si può non rilevare che il reato di *hate speech* rischia di divenire un reato di opinione europeo, su cui appare particolarmente difficile raggiungere il consenso, anche per i diversi livelli di tutela della libertà di espressione nell'ordinamento europeo.

Sarebbe, forse, più opportuno separare l'*hate speech* dall'*hate crime* nel

⁷¹ Cfr. Study to support the preparation of the European Commission's initiative to extend the list of EU crimes in Article 83 of the Treaty on the Functioning of the EU to hate speech and hate crime, cit., pag. 19.

percorso verso l'adozione di una decisione del Consiglio ai sensi dell'art. 83, par. 3, TFUE.

L'esperienza della Decisione Quadro, inoltre, rivela la difficoltà di raggiungere il consenso per l'adozione e l'attuazione di questo tipo di norme incriminatrici, soprattutto con riferimento all'*hate speech*, stante le diverse tradizioni giuridiche ed il diverso patrimonio culturale degli Stati membri che incide sul bilanciamento tra la tutela della dignità delle persone offese e della libertà di espressione.

In ogni caso, nelle more dell'*iter* per l'approvazione della proposta della Commissione, il futuro della tutela contro l'*online hate speech* è al momento affidato al DSA, nella speranza che la nuova regolamentazione della condotta dei PSI e la nuova forma di collaborazione con le autorità nazionali ed europee si riveli efficace non solo per la tutela del mercato unico digitale, ma per la protezione dei diritti fondamentali dei cittadini.