ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

12 GENNAIO 2022

Moderazione e rimozione dei contenuti illegali online nel diritto dell'UE

di Giuseppe Morgese
Professore associato di Diritto dell'Unione europea
Università degli Studi di Bari Aldo Moro

Moderazione e rimozione dei contenuti illegali online nel diritto dell'UE*

di Giuseppe Morgese
Professore associato di Diritto dell'Unione europea
Università degli Studi di Bari Aldo Moro

Abstract [It]: Il contributo ha a oggetto la disciplina dell'UE sulla moderazione e rimozione (o disabilitazione) dei contenuti illegali *online*. Premessi brevi cenni alla questione (par. 1), il par. 2 si occupa della disciplina generale dettata dalla direttiva *eCommerce*, come interpretata negli anni dalla Corte di giustizia. I paragrafi da 3.1 a 3.7, invece, si concentrano sulle regole applicabili ai contenuti terroristici, pedopornografici, lesivi del diritto d'autore, lesivi di altri diritti di proprietà intellettuale, relativi a prodotti non sicuri o pericolosi, d'odio e disinformativi. I paragrafi da 4.1 a 4.3 esaminano le rilevanti disposizioni della proposta di *Digital Services Act* del 15 dicembre 2020. Nelle conclusioni, si dà conto dell'andamento della procedura legislativa per l'approvazione della proposta DSA.

Abstract [En]: This paper focuses on the EU framework on moderation and removal (or disabling) of illegal content online. After a brief outline of the issue (Para. 1), Para. 2 deals with the general framework of the *eCommerce* directive, as interpreted over the years by the European Court of Justice. Paras. 3.1 to 3.7, on the other hand, focus on rules applicable to terrorist contents, child pornography contents, copyright infringing contents, contents infringing other IPRs, unsafe or dangerous products, hate speech contents and misinformation contents. Paragraphs 4.1 to 4.3 go into detail of the relevant provisions of the *Digital Services Act* proposal of 15 December 2020. In conclusion, progress of the legislative procedure for the approval of the DSA proposal is reported.

Parole chiave: Contenuti illegali; rimozione; disabilitazione; direttiva *eCommerce*; proposta di *Digital Services Act*
Keywords: Illegal content; removal; disabling; *eCommerce* directive; DSA proposal

1. Introduzione

La risonanza che ha avuto la diffusione di documenti interni di Facebook a opera di una sua ex *data scientist* e la relativa inchiesta giornalistica "*The Facebook Files*"[1] sono l'occasione per esaminare la disciplina

* Articolo sottoposto a referaggio. L'articolo è una versione significativamente ampliata, diversamente organizzata e più aggiornata di un contributo destinato al volume di G. CAGGIANO – G. CONTALDI – P. MANZINI (a cura di), Verso una legislazione europea su mercati e servizi digitali, Bari, in corso di pubblicazione.

[1] L'inchiesta del Wall Street Journal ha messo in luce, tra l'altro, l'esistenza di un nutrito gruppo di utenti "vip" esentati dalla normale *policy* di moderazione (con la conseguenza di non procedere nei confronti di loro contenuti discutibili), le conseguenze della modifica dell'algoritmo del *newsfeed* operata nel 2018 (che ha dato rilevanza ai contenuti d'odio ed estremamente polarizzanti, in quanto generatori di traffico per il social network), la mancata rimozione o disabilitazione dei contenuti diffusi da esponenti della criminalità organizzata, o riguardanti il traffico di esseri umani e l'incitamento alla violenza contro minoranze etniche soprattutto nelle aree geografiche (Medioriente, Africa) sprovviste di moderatori

dell'UE sulla moderazione[2] e la rimozione (o disabilitazione) dei contenuti illegali[3] generati dagli utenti (*user-generated content*).

La necessità di predisporre norme dirette a regolamentare il diligente svolgimento delle attività di moderazione e rimozione/disabilitazione dei contenuti *online* da parte dei fornitori di servizi su Internet (*Internet Service Providers*, ISP o prestatori intermediari) è, da tempo, uno degli obiettivi più rilevanti e sensibili del mercato unico digitale[4]. La rilevanza dipende dal fatto che i contenuti *online* sono sempre più numerosi[5] e appartengono a categorie anche molto diverse tra loro[6]. La delicatezza, invece, risiede nella necessità di individuare il miglior bilanciamento possibile tra due diverse esigenze: quella di proteggere i beni giuridici colpiti dalla diffusione *online* di quei contenuti, beni che spesso si ricollegano a diritti fondamentali garantiti, tra gli altri, dalla Carta dei diritti fondamentali dell'UE (c.d. "Carta di Nizza" o "Carta")[7] e l'altrettanto importante esigenza che tali attività non comprimano oltre lo stretto indispensabile altri diritti fondamentali quali quelli alla libera manifestazione del pensiero e alla libera informazione (artt. 10 e 11 Carta)[8].

---

in grado di comprendere la lingua o i dialetti utilizzati; e il mancato efficace intervento contro i numerosissimi contenuti disinformativi soprattutto dei c.d. "no-vax".

[2] Secondo l'art. 2, lett. p), della proposta di *Digital Services Act* (*infra*, nota 9), la "moderazione dei contenuti" consiste in "attività svolte dai prestatori di servizi intermediari al fine di individuare, identificare e contrastare contenuti illegali e informazioni incompatibili con le loro condizioni generali, forniti dai destinatari del servizio, comprese le misure adottate che incidono sulla disponibilità, sulla visibilità e sull'accessibilità di tali contenuti illegali o di dette informazioni, quali la loro retrocessione o rimozione o la disabilitazione dell'accesso agli stessi, o sulla capacità dei destinatari di fornire tali informazioni, quali la cessazione o la sospensione dell'account di un destinatario del servizio". V. l'approfondito lavoro di A. DE STREEL e al., *Online Platforms' Moderation of Illegal Content Online. Law, Practices and Options for Reform*, giugno 2020.

[3] Per "contenuto illegale" si intende qualsiasi informazione che, di per sé o in relazione ad un'attività, non è conforme alle disposizioni normative dell'UE o di uno Stato membro, indipendentemente dalla natura o dall'oggetto specifico di tali disposizioni: questa è la definizione accolta, ad es., dall'art. 2, lett. g), della proposta di *Digital Services Act* (*infra*, nota 9).

[4] Una ricognizione del quadro generale è compiuta da G. CAGGIANO, *Il quadro normativo del Mercato unico digitale*, in *Eurojus*, fascicolo speciale "Mercato Unico Digitale, dati personali e diritti fondamentali", a cura di F. ROSSI DAL POZZO, 2020, p. 13 ss.

[5] Cfr. il *Flash Eurobarometer on Illegal Content online*, n. 469, settembre 2018.

[6] Si pensi, ad es., alla vendita di merci pericolose o beni contraffatti; alla diffusione di contenuti piratati; ai discorsi diffamatori e a quelli d'odio (*hate speech*); ai contenuti e materiali pedopornografici, terroristici, razzisti e xenofobi; nonché, per certi versi, ai contenuti (non illegali ma) ingannevoli di tipo disinformativo.

[7] La Carta è stata proclamata a Nizza il 7 dicembre 2000 dal Parlamento europeo, dal Consiglio e dalla Commissione, nonché riproclamata a Strasburgo il 12 dicembre 2007 (qui). Essa reca un nutrito catalogo di diritti fondamentali, in parte corrispondenti a quelli della Convenzione europea dei diritti dell'uomo (CEDU) o risultanti dalle tradizioni costituzionali comuni degli Stati membri, in parte completamente nuovi. In dottrina, per tutti, v. R. MASTROIANNI – O. POLLICINO – S. ALLEGREZZA – F. PAPPALARDO – O. RAZZOLINI (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017. Tra le norme rilevanti ai nostri fini ricordiamo quelle sul divieto di discriminazioni (art. 21) nonché sulla tutela dei minori (art. 24), della sicurezza pubblica (art. 6) e della proprietà intellettuale (art. 17).

[8] Sulla generale necessità di assicurare il rispetto dei diritti fondamentali *online* v. B. SANDER, *Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of a Human Rights-Based Approach to Content Moderation*, in *Fordham International Law Journal*, 2020, p. 939 ss.; e R. JANAL, *Eyes Wide Open. Adapting the Digital Services Act to the Realities of Intermediary Service Provision*, in *Verfassungsblog*, 7.09.2021.

Non è dunque un caso che l'individuazione di tale bilanciamento sia alla base della proposta di *Digital Services Act* (DSA)[9] la quale, assieme a quelle di *Digital Markets Act* e *Data Governance Act*[10], rappresenta una delle iniziative della "impetuosa" attività di regolamentazione del mercato unico digitale portata avanti dall'UE negli ultimi anni. La proposta DSA prevede norme più rigorose di quelle attualmente in vigore sulla moderazione dei contenuti svolta dagli ISP, e in specie dagli *hosting providers* soprattutto se gestori di piattaforme *online*, al dichiarato fine di instaurare "un ambiente online sicuro, prevedibile e affidabile, in cui i diritti fondamentali sanciti dalla Carta siano tutelati in modo effettivo"[11].

Ciò è diretta conseguenza del ripensamento di Internet come ambiente contenutisticamente favorevole agli ISP, che ha caratterizzato la prima fase dello sviluppo della Rete. Infatti, a fronte di un (lungo) periodo in cui ai prestatori è stato concesso un regime di responsabilità non particolarmente stringente[12], di recente anche nell'UE (e nei suoi Stati membri) si sta provando a disciplinare la materia con maggior rigore in considerazione dell'affermazione di nuovi servizi e del notevole incremento del numero dei contenuti illegali *online*. In particolare, si è ormai affermata l'idea per cui ciò che è vietato *offline* deve esserlo anche *online*, senza che la Rete rappresenti un "porto franco" per la circolazione di qualsivoglia contenuto illegale. Non è un caso, quindi, che in alcuni settori (quali quello dei contenuti audiovisivi) le nuove e più rigide norme di responsabilità hanno avuto come conseguenza il rafforzamento delle attività di moderazione e rimozione a beneficio dei titolari dei diritti delle opere diffuse illegalmente *online*.

Prima di esaminare il contenuto della proposta DSA, nella parte di nostro interesse, approfondiremo il quadro normativo vigente non solo perché i fondamenti di quest'ultimo non sono messi in discussione

[9] Proposta di regolamento del Parlamento europeo e del Consiglio, del 15 dicembre 2020, relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, COM(2020)825 final.

[10] Sul DMA v. G. CONTALDI, *Il DMA (*Digital Markets Act*) tra tutela della concorrenza e protezione dei dati personali*, in *Ordine internazionale e diritti umani*, 2021, p. 292 ss., e P. MANZINI, *Equità e contendibilità nei mercati digitali: la proposta di* Digital Market Act, in *I Post di AISDUE*, 25.01.2021,; sul DSA v. F. CALOPRISCO, *Data Governance Act. Condivisione e "altruismo" dei dati*, in *I Post di AISDUE*, 5.05.2021.

[11] Così l'art. 1, par. 2, proposta DSA.

[12] Sulla responsabilità dei *providers* v. P. BAISTROCCHI, *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, in *Santa Clara High Technology Law Journal*, 2002, p. 111 ss.; B. KLEINSCHMIDT, *An International Comparison of ISP's Liabilities for Unlawful Third Party Content*, in *International Journal of Law and Information Technology*, 2010, p. 332 ss.; G. B. DINWOODIE (ed.), *Secondary Liability of Internet Service Providers*, Cham, 2017; J. B. NORDEMANN, *Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?*, novembre 2017; G. SARTOR, *Providers Liability: From the eCommerce Directive to the future*, settembre 2017, pp. 8-9; M. TADDEO – L. FLORIDI (eds.), *The Responsibilities of Online Service Providers*, Cham, 2017; G. F. FROSIO, *Why keep a dog and bark yourself? From intermediary liability to responsibility*, in *International Journal of Law and Information Technology*, 2018, p. 1 ss.; M. L. MONTAGNANI – A. Y. TRAPOVA, *Safe harbours in deep waters: a new emerging liability regime for Internet intermediaries in the Digital Single Market*, in *International Journal of Law and Information Technology*, 2018, p. 294 ss.; K. T. O'SULLIVAN, *Copyright and Internet Service Provider "Liability": The Emerging Realpolitik of Intermediary Obligations*, in *IIC - International Review of Intellectual Property and Competition Law*, 2019, p. 527 ss.; M. C. BUITEN – A. DE STREEL – M. PEITZ, *Rethinking liability rules for online hosting platforms*, in *International Journal of Law and Information Technology*, 2020, p. 139 ss.; D. MAC SÍTHIGH, *The road to responsibilities: new attitudes towards Internet intermediaries*, in *Information & Communications Technology Law*, 2020, p. 1 ss.; e A. BERTOLINI – F. EPISCOPO – N.-A. CHERCIU, *Liability of online platforms*, febbraio 2021.

dalla proposta di cui si tratta, ma anche al fine di metter in luce le novità che quest'ultima introdurrebbe qualora approvata nei termini prefigurati.

2. Le disposizioni a carattere generale e la giurisprudenza della Corte di giustizia

La disciplina dell'UE concernente la moderazione e la rimozione/disabilitazione dei contenuti illegali *online* si compone di misure legislative, non legislative e volontarie di carattere sia generale (applicabili a tutti i contenuti) sia speciale (in ragione di specifici obiettivi da raggiungere).

La direttiva 2000/31 sul commercio elettronico (*eCommerce*)[13], adottata nella prima fase di sviluppo di Internet, detta ancor oggi il regime normativo di base applicabile ai prestatori intermediari e contiene una disciplina particolarmente favorevole quanto alle loro attività di moderazione e rimozione. L'atto prevede non un obbligo ma solo un "onere" di svolgere tali attività per avvalersi della clausola di esonero dalla responsabilità per attività di terzi (responsabilità indiretta o *secondary liability*). Più che per i prestatori *mere conduit*[14] e *caching*[15], nei confronti dei quali è meno probabile che sorga tale responsabilità[16], la questione rileva per gli *hosting providers*[17]. Questi ultimi, ai sensi dell'art. 14 direttiva *eCommerce*, godono dell'esonero alla duplice condizione che non siano effettivamente al corrente di attività o informazioni illecite e che, non appena ne vengano al corrente, agiscano immediatamente per rimuoverle o per disabilitarne l'accesso (sistema c.d. *notice-and-take-down*).

Dalla richiesta ai prestatori di *hosting*, per avvalersi dell'esonero dalla responsabilità, di attivarsi per la rimozione o disabilitazione dei contenuti illegali solo *ex post* – cioè, solo dopo che siano stati resi disponibili sui loro servizi – discende *l'assenza di generali obblighi di moderazione ex ante* e, per l'appunto, *solo oneri di successiva rimozione o disabilitazione* alle condizioni specificate.

L'esonero, tuttavia, opera solo a patto che i prestatori si limitino a svolgere un ruolo di ordine meramente tecnico, automatico e passivo ("*intermediari passivi*")[18], lasciando che gli utenti carichino e diffondano

[13] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000. Di recente v. A. DE STREEL – M. HUSOVEC, *The e-commerce Directive as the cornerstone of the Internal Market - Assessment and options for reform*, maggio 2020.

[14] Si tratta di quei prestatori che, ai sensi dell'art. 12, forniscono servizi di mera trasmissione sulle o di mero accesso alle reti di comunicazione, senza memorizzare le informazioni fornite dai destinatari dei servizi a meno che ciò sia funzionale alla trasmissione e limitato allo stretto necessario. Costoro non hanno oneri di moderazione e rimozione per usufruire dell'esonero dalla responsabilità.

[15] Questi ultimi, che svolgono attività di memorizzazione automatica, intermedia e temporanea delle informazioni fornite dai destinatari dei servizi con la finalità di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta, non possono essere ritenuti responsabili per la memorizzazione temporanea di contenuti illegali se, tra l'altro, agiscono prontamente per rimuoverli o per disabilitarne l'accesso non appena vengano a conoscenza di analoga rimozione o disabilitazione dal luogo dove si trovavano inizialmente oppure in base ad apposita inibitoria di un'autorità amministrativa o giurisdizionale (art. 13).

[16] Così, con riferimento all'attività di *mere conduit* consistente nell'offerta gratuita al pubblico di una rete wi-fi da parte del gestore di un negozio, v. la sentenza della Corte di giustizia del 15 settembre 2016, causa C-484/14, *Mc Fadden*, ECLI:EU:C:2016:689.

[17] Si definiscono tali i prestatori di servizi di memorizzazione di informazioni fornite da terzi.

[18] Così il considerando 42 della direttiva *eCommerce*.

contenuti senza "trattarli" in qualche modo. La possibilità di agire come intermediari passivi è senz'altro ammessa dall'art. 15, par. 1, che peraltro contiene il divieto per gli Stati di imporre obblighi di sorveglianza *ex ante* sui contenuti memorizzati e di accertamento attivo di fatti o circostanze che indichino la presenza di attività illecite (art. 15, par. 1)[19]. Al contrario, però, se gli *hosting providers* svolgono in maniera volontaria attività idonee a identificare contenuti illegali prima che siano memorizzati[20] o segnalati[21] dagli utenti o dalle autorità nazionali – così qualificandosi come *intermediari "attivi"* – incorrono in responsabilità qualora, rispettivamente, non si astengano dal memorizzare i contenuti "incriminati" oppure non agiscano con celerità per rimuoverli o disabilitarne l'accesso[22]. Ciò vale ancor più nel caso in cui i contenuti illegali siano trasmessi o memorizzati sotto la loro autorità o controllo (art. 14, par. 2), essendo in quel caso in presenza non di prestatori intermediari bensì di veri e propri editori[23].

Giova sottolineare che l'impostazione seguita dalla direttiva *eCommerce*, come interpretata dalla Corte di giustizia, risulta conforme alla giurisprudenza della Corte EDU. Nel caso *Delfi* c. *Estonia*, la Camera[24] e la Grande Camera[25] hanno ritenuto che il riconoscimento della responsabilità di un portale di notizie *online* per alcuni commenti offensivi postati dagli utenti sotto un articolo da esso pubblicato non violasse l'art. 10 CEDU sulla libertà di espressione, essendo quei commenti altamente offensivi e non essendo stati rimossi dal portale prima che diventassero pubblici, permettendo inoltre ai loro autori di rimanere anonimi. Qui la Corte EDU, pur non esaminando la direttiva *eCommerce*, ha affermato la responsabilità dei prestatori che svolgono un ruolo attivo ma non contrastano la diffusione di contenuti manifestamente illeciti, caricati da terzi, di cui hanno il controllo[26]. Al contrario, laddove l'illiceità dei contenuti non sia

[19] Nella sentenza del 24 novembre 2011, causa C-70/10, *Scarlet Extended*, ECLI:EU:C:2011:771, la Corte di giustizia ha escluso la possibilità per i giudici nazionali di imporre a un ISP l'obbligo di predisporre un sistema di filtraggio generale per prevenire scaricamenti illegali di file. Analogamente, nella sentenza del 16 febbraio 2012, causa C-360/10, *SABAM* c. *Netlog*, ECLI:EU:C:2012:85, si è escluso che possa essere imposto a un *social network* l'obbligo di predisporre un sistema di filtraggio generale per prevenire l'utilizzo illecito di opere musicali e audiovisive.

[20] Ad es. qualora svolgano volontariamente una sorveglianza generale dei contenuti caricati attraverso meccanismi automatizzati di riconoscimento preventivo.

[21] Ad es. nel caso in cui gli *hosting providers* assistano gli utenti per l'ottimizzazione della presentazione dei contenuti caricati (cfr. G. RUOTOLO, *Digital Services Act e Digital Markets Act tra responsabilità dei fornitori e rischi di bis in idem*, in *SIDIBlog*, 29.03.2021) oppure si avvalgano del controllo dei c.d. *trusted flaggers* (segnalatori attendibili esterni indipendenti).

[22] In tal senso, quanto alla prestazione di un servizio di posizionamento su Internet, v. la sentenza della Corte di giustizia del 23 marzo 2010, cause riunite da C-236 a 238/08, *Google France* e *Google*, ECLI:EU:C:2010:159.

[23] Sentenza dell'11 settembre 2014, causa C-291/13, *Papasavvas*, ECLI:EU:C:2014:2209, in cui la Corte di giustizia ha affermato che "i limiti alla responsabilità civile previsti agli articoli da 12 a 14 della direttiva 2000/31 non riguardano il caso di una casa editrice che disponga di un sito Internet sul quale venga pubblicata la versione on line di un giornale (…) qualora sia a conoscenza delle informazioni pubblicate ed eserciti un controllo sulle stesse" (punto 46). Gli editori, infatti, esercitano un controllo preventivo sui contenuti diffusi: v. 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*, 18.02.2021, p. 8.

[24] Sentenza del 10 ottobre 2013, *Delfi* c. *Estonia*, ECLI:CE:ECHR:2013:1010JUD006456909.

[25] Sentenza del 16 giugno 2015, *Delfi* c. *Estonia*, ECLI:CE:ECHR:2015:0616JUD006456909.

[26] In dottrina v. H. J. MCCARTHY, *Is the Writing on the Wall for Online Service Providers? Liability for Hosting Defamatory User-Generated Content under European and Irish Law*, in *Hibernian Law Journal*, 2015, p. 16 ss., spec. p. 37 ss.; R. NIGRO, *La responsabilità degli* Internet service providers *e la Convenzione europea dei diritti umani: il caso* Delfi AS, in *Diritti umani e diritto*

così manifesta e richieda un'analisi contestuale, oppure qualora il prestatore non ne abbia il controllo, il giudice di Strasburgo ritiene che la responsabilità sorga solo per omissioni a sèguito di segnalazioni sufficientemente motivate o ingiunzioni specifiche[27]. Il tutto, però, alla luce del principio di proporzionalità: in quattro recenti casi concernenti la Russia, infatti, le misure di disabilitazione dell'accesso a interi siti web per impedire la diffusione di specifici contenuti considerati illegali dalle autorità nazionali sono state ritenute eccessive e arbitrarie, risultando in violazione dell'art. 10 CEDU e, in quanto assunte senza le necessarie salvaguardie procedurali, anche dell'art. 13 CEDU[28].

Ritornando alla direttiva *eCommerce*, la regola del controllo *ex post* attraverso misure di *notice-and-take-down*[29] risulta particolarmente favorevole per gli intermediari passivi, i quali hanno così tutto l'interesse a non moderare (e censurare) i contenuti ospitati. Tale circostanza, se da un lato ha permesso di tutelare la libertà di manifestazione del pensiero su Internet salvaguardando anche la libera iniziativa economica dei prestatori, ha però agevolato (se non incentivato) un'ampia "irresponsabilità" dei *providers* per i contenuti illegali.

L'esonero dalla responsabilità indiretta per gli intermediari passivi e la mancanza di specifici obblighi di moderazione e rimozione/disabilitazione non esclude però la possibilità per gli Stati di imporre a tutti gli intermediari, attivi e passivi, l'obbligo di impedire o porre fine a specifiche violazioni (art. 14, par. 3)[30]. Questa disposizione è di primaria importanza, atteso che le ingiunzioni nazionali dirette alla rimozione o alla disabilitazione di specifici contenuti illegali possono essere rivolte anche i prestatori che soddisfano le condizioni dell'art. 14, par. 1: costoro, infatti, non vengono "colpiti" in conseguenza di loro azioni od

internazionale, 2015, p. 681 ss; e L. BRUNNER, *The Liability of an Online Intermediary for Third Party Content. The Watchdog Becomes the Monitor: Intermediary Liability after Delfi v Estonia*, in *Human Rights Law Review*, 2016, p. 163 ss.

[27] V. le sentenze del 2 febbraio 2016, *Magyar Tartalomszolgáltatók Egyesülete* e *Index.hu Zrt* c. *Ungheria*, ECLI:CE:ECHR:2016:0202JUD002294713; del 19 marzo 2019, *Høiness* c. *Norvegia*, ECLI:CE:ECHR:2019:0319JUD004362414; e del 4 giugno 2020, *Jezior* c. *Polonia*, ECLI:CE:ECHR:2020:0604JUD003195511.

[28] V. le quattro sentenze pubblicate il 23 giugno 2000, nei casi *Vladimir Kharitonov* c. *Russia*, ECLI:CE:ECHR:2020:0623JUD001079514; *OOO Flavus* e *altri* c. *Russia*, ECLI:CE:ECHR:2020:0623JUD001246815; *Bulgakov* c. *Russia*, ECLI:CE:ECHR:2020:0623JUD002015915; ed *Engels* c. *Russia*, ECLI:CE:ECHR:2020:0623JUD006191916.

[29] In argomento v., tra gli altri, G. N. YANNOPOULOS, *The Immunity of Internet Intermediaries Reconsidered?*, in M. TADDEO – L. FLORIDI (eds.), *The Responsibilities*, *cit.*, p. 43 ss. Sulla differenza tra misure *ex ante* ed *ex post* si rinvia a K. PARTI – L. MARIN, *Ensuring Freedoms and Protecting Rights in the Governance of the Internet: A Comparative Analysis on Blocking Measures and Internet Providers' Removal of Illegal Internet Content*, in *Journal of Contemporary European Research*, 2013, p. 138 ss., spec. pp. 139-140.

[30] A ciò si aggiungono gli obblighi di informare senza indugio le autorità nazionali competenti di presunte attività o informazioni illecite a loro conoscenza, e di comunicare, su richiesta, le informazioni utili per l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati (art. 15, par. 2).

omissioni, non essendone appunto responsabili, ma per il solo fatto di trovarsi in una posizione idonea a porre fine alle attività illecite dei loro utenti[31].

Negli ultimi tempi, il carattere più maturo della Rete e l'emergere di nuovi servizi delle piattaforme *online*[32], che non si limitano alla semplice offerta di spazio per il caricamento dei contenuti ma offrono una vasta gamma di servizi[33], hanno fatto emergere i limiti della direttiva *eCommerce* sotto almeno quattro profili.

Il primo concerne il fatto che essa lascia agli Stati la definizione degli aspetti sostanziali e procedurali delle misure di rimozione e disabilitazione, fermo restando il divieto di imporre obblighi generali di sorveglianza e accertamento attivo dei fatti. Ciò ha causato un'inevitabile frammentazione della disciplina da Stato a Stato[34] e ha impedito per lungo tempo di allontanarsi dalla regola dell'intervento *ex post* sui contenuti segnalati[35]. Vero è che la Commissione negli ultimi anni ha tentato di imporre agli ISP l'adozione di misure di sorveglianza preventiva, sebbene relative solo ad alcuni contenuti (quelli terroristici[36] e quelli protetti dal diritto d'autore[37]), ma è altrettanto vero che il tentativo non è andato a buon fine perché respinto dalle Istituzioni legislative[38].

Il secondo profilo, strettamente collegato al primo, si riferisce alle conseguenze della regola dell'esonero dalla responsabilità indiretta[39] e del divieto di imporre obblighi di sorveglianza generali *ex ante* (art. 15). Le due norme hanno non solo affidato all'autoregolamentazione degli *hosting providers* le attività di moderazione dei contenuti ma anche scoraggiato l'adozione volontaria di misure "proattive" per timore di perdere la qualifica di intermediario passivo.

In proposito, va detto però che la Corte di giustizia ha da tempo intrapreso un percorso di superamento almeno parziale di queste regole. Nella sentenza *L'Oréal SA* e *a.* c. *eBay* è stato chiarito, per un verso, che il gestore di un mercato *online* non può avvalersi dell'esonero dalla responsabilità qualora sia stato al corrente di fatti o circostanze in base ai quali un operatore economico diligente avrebbe dovuto constatare

[31] Così le sentenze della Corte di giustizia del 3 ottobre 2019, causa C-18/18, *Glawischnig-Piesczek c. Facebook Ireland Ltd.*, ECLI:EU:C:2019:821, punto 25, e più recentemente del 22 giugno 2021, cause riunite C-682 e 683/18, *YouTube* e *Cyando*, ECLI:EU:C:2021:503, punto 143.

[32] Sulle quali v. A. GAWER – N. SRNICEK, *Online platforms. Economic and societal effects*, marzo 2021.

[33] Cfr. G. M. RUOTOLO, *Scritti di diritto internazionale ed europeo dei dati*, Bari, 2021, spec. p. 256.

[34] Vedi N. LOMBA – T. EVAS, *Digital services act. European added value assessment*, ottobre 2020, spec. l'allegato I.

[35] Al vantaggio per i prestatori corrisponde, ovviamente, la penalizzazione degli utenti interessati alla rimozione dei contenuti illegali, i quali specie in passato erano soliti inviare più segnalazioni anche se relative allo stesso contenuto illegale reiteratamente caricato *online*.

[36] Art. 6 della proposta del 12 settembre 2018, COM(2018)640 final, non a caso intitolata alla "prevenzione" della diffusione di contenuti terroristici online.

[37] Art. 13 della proposta del 14 settembre 2016, COM(2016)593 final.

[38] Le versioni finali del regolamento 2021/784 (*infra*, par. 3.1) e della direttiva 2019/790 (*infra*, par. 3.4) prevedono solo obblighi di rimozione *ex post*.

[39] Sulla necessità di ripensare la regola della irresponsabilità dei prestatori intermediari, v. S. STALLA-BOURDILLON, *Internet Intermediaries as Responsible Actors? Why It Is Time to Rethink the E-Commerce Directive as Well*, in M. TADDEO – L. FLORIDI (eds.), *The Responsibilities*, *cit.*, p. 275 ss.

l'illiceità delle offerte in vendita e non abbia prontamente agito[40]; e, per altro verso, che le ingiunzioni a suo carico possono essere dirette non solo a far cessare le violazioni attuali, ma anche a prevenire quelle future della stessa natura[41]. Similmente, nella sentenza *UPC Telekabel Wien*, relativa a un'ingiunzione avverso un fornitore di accesso a Internet per bloccare l'accesso di tutti i suoi abbonati a un sito web lesivo del diritto d'autore, la Corte ha affermato che detta ingiunzione è compatibile col diritto UE, anche se non specifica le misure da assumere, purché permetta al fornitore di sottrarsi alla responsabilità dimostrando di avere adottato tutte le misure ragionevoli[42].

Tuttavia, è nella più recente giurisprudenza sui *contenuti diffamatori (e d'odio)*, presenti in quantità soprattutto sui *social network*, che appare chiaro il percorso argomentativo del giudice di Lussemburgo. Nella sentenza *Glawischnig-Piesczek*, avente a oggetto un contenuto di questo tipo diffuso su Facebook, il giudice sovranazionale ha ammesso la possibilità per i giudici nazionali di imporre misure di rimozione o blocco non solo dei contenuti d'odio dichiarati illeciti (*take-down*)[43], ma anche di tutti quelli successivi aventi contenuto identico (*stay-down*) nonché persino di quelli con un contenuto "equivalente" purché sostanzialmente invariato rispetto a quello illecito[44].

Questa pronunzia, per certi versi "rivoluzionaria", ha spostato il punto di equilibrio più a favore degli utenti danneggiati dai contenuti diffamatori, ampliando quindi gli obblighi a carico degli *hosting providers*: questi, pur continuando a godere del divieto di obblighi generali di sorveglianza preventiva, possono però essere destinatari di *obblighi specifici* di controllo *ex ante* dei contenuti identici o equivalenti a quelli illegali. Il fatto che gli *hosting providers* debbano ora comportarsi in maniera più diligente[45], senza potersi "nascondere" in ogni caso dietro lo schermo dell'art. 14, ha prodotto l'irrigidimento delle regole di moderazione e, soprattutto, il ricorso a misure "proattive" come i filtri delle parole-chiave e dei contenuti,

[40] Sentenza del 12 luglio 2011, causa C-324/09, *L'Oréal SA* e *a.* c. *eBay*, ECLI:EU:C:2011:474, punto 124.
[41] *Ivi*, punto 144.
[42] Sentenza del 27 marzo 2014, causa C-314/12, *UPC Telekabel Wien*, ECLI:EU:C:2014:192.
[43] Peraltro, con efficacia territoriale mondiale.
[44] V. la sentenza *Glawischnig-Piesczek c. Facebook Ireland Ltd*, punto 53. In altri termini, la Corte non richiede agli *hosting providers* di effettuare una valutazione autonoma di tale equivalenza. In dottrina O. POLLICINO, *L'"autunno caldo" della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in *Federalismi.it*, n. 19/2019; G. DE GREGORIO, *Moderazione dei contenuti in rete: poteri privati tra prospettive locali e prospettive globali*, in *Quaderni costituzionali*, 2020, p. 176 ss.; D. KELLER, *Facebook Filters, Fundamental Rights, and the CJEU's* Glawischnig-Piesczek *Ruling*, in *GRUR International*, 2020, p. 616 ss.; C. RAUCHEGGER – A. KUCZERAWY, *Injunctions to remove illegal online content under the eCommerce Directive:* Glawischnig-Piesczek, in *Common Market Law Review*, 2020, p. 1495 ss.; e D. VAIRA – G. M. RUOTOLO, *Responsabilità dei social network per* user generated content *e applicazione extraterritoriale delle misure inibitorie di lesioni dei diritti della personalità alla luce della recente giurisprudenza UE*, in *Ordine internazionale e diritti umani*, 2020, p. 187 ss.
[45] In proposito v. P. VALCKE – A. KUCZERAWY – P.-J. OMBELET, *Did the Romans Get It Right? What Delfi, Google, eBay, and UPC TeleKabel Wien Have in Common*, in M. TADDEO – L. FLORIDI (eds.), *The Responsibilities*, *cit.*, p. 101 ss.

i "segnalatori attendibili" e i modelli di apprendimento automatico rivolti a replicare il processo decisionale umano (sebbene spesso sotto il controllo finale dell'uomo)[46].

Il terzo profilo problematico riguarda, invece, l'assenza nella direttiva di obblighi di trasparenza e diligenza dei prestatori nei confronti dei destinatari dei servizi. Il quarto profilo si riferisce, infine, all'assenza di un potere di supervisione e controllo delle autorità nazionali (ed europee) sulla correttezza dell'attività di quegli intermediari.

Alle lacune qui evidenziate, ben presenti alla Commissione a partire dal 2015[47], si è provato a rimediare anzitutto con norme non vincolanti a carattere orizzontale, cui si sono aggiunte quelle (vincolanti, non vincolanti e volontarie) relative a settori specifici[48].

In particolare, dando sèguito a precedenti orientamenti[49], nel 2018 la Commissione ha adottato la raccomandazione 2018/334 sulle misure per contrastare efficacemente i contenuti illegali *online*[50]. Tale atto non vincolante, indirizzato prevalentemente agli *hosting providers*, contiene una definizione ampia di "contenuto illegale"[51] (poi transitata nella proposta DSA). La raccomandazione non mette in discussione (né potrebbe farlo) il divieto di imporre obblighi generali di sorveglianza e di accertamento attivo dei contenuti illegali, ma invita i prestatori di servizi di *hosting* a prendere ulteriori iniziative con riferimento a tutti i tipi di contenuti illegali. Sinteticamente, i *providers* dovrebbero prevedere meccanismi di facile accesso e utilizzo per la presentazione di segnalazioni motivate e precise (parr. 5-8); informare rapidamente e in maniera motivata i fornitori di contenuti delle decisioni di rimozione o disabilitazione[52] e dare loro diritto di replica, oltre che informare fornitori e segnalatori delle decisioni assunte (parr. 9-13); pubblicare descrizioni trasparenti della loro politica di rimozione nonché, almeno una volta l'anno, relazioni sull'attività in materia (parr. 16-17); adottare, se del caso, misure proattive al fine di individuare i contenuti illegali (par. 18); predisporre misure di salvaguardia per evitare la rimozione dei contenuti non

[46] Per approfondimenti v. A. DE STREEL e al., *Online Platforms' Moderation*, *cit.*, p. 43 ss., e H. ZECH, *General and specific monitoring obligations in the Digital Services Act*, in *Verfassungsblog*, 2.09.2021.

[47] V. la comunicazione del 6 maggio 2015, Strategia per il mercato unico digitale in Europa, COM(2015)192 final, la cui sezione 3.3.2 è dedicata al contrasto ai contenuti illeciti su Internet. V. anche le comunicazioni del 25 maggio 2016, Le piattaforme online e il mercato unico digitale - Opportunità e sfide per l'Europa, COM(2016)288 final, e del 10 maggio 2017, sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale - Un mercato unico digitale connesso per tutti, COM(2017)228 final.

[48] *Infra*, par. 3.

[49] V. la comunicazione della Commissione, del 28 settembre 2017, Lotta ai contenuti illeciti online - Verso una maggiore responsabilizzazione delle piattaforme online, COM(2017)555 final, in cui la Commissione si è riproposta di migliorare le azioni rivolte all'efficace rimozione della generalità dei contenuti illegali, a una maggiore trasparenza e alla tutela dei diritti fondamentali.

[50] Raccomandazione (UE) 2018/334 della Commissione, del 1° marzo 2018. In proposito v. D. MAC SÍTHIGH, *The road*, *cit.*, p. 10 ss.

[51] È tale "qualunque informazione non conforme al diritto dell'Unione o alle leggi di uno Stato membro interessato" (par. 1, lett. b), indipendentemente dalla natura o dall'oggetto delle norme considerate.

[52] A meno che risulti evidente che i contenuti in questione sono illegali e fanno riferimento a reati gravi che comportano una minaccia per la vita o la sicurezza delle persone.

illegali e, qualora vengano utilizzati strumenti automatizzati, prevedere verifiche e sorveglianza umane (parr. 19-20); adottare misure apposite per prevenire segnalazioni o repliche in malafede e altri comportamenti abusivi (par. 21); nonché, infine, migliorare la collaborazione tra di loro, con gli Stati membri e con i segnalatori attendibili (parr. 22-28).

In assenza di norme vincolanti se non per alcuni settori, gli auspici della Commissione in merito alla maggiore responsabilizzazione degli *hosting providers*[53] hanno sinora trovato solo parziale riscontro nelle "condizioni di servizio" cui gli utenti acconsentono al primo accesso ai servizi dei prestatori. Il carattere assai variegato di tali condizioni, pur legittima espressione della libertà di impresa[54], non solo ha determinato un'ulteriore frammentazione delle regole da prestatore a prestatore (e da Stato a Stato), ma – per via della sproporzione contrattuale tra intermediari e utenti – non fornisce neanche garanzie che le attività di moderazione (se previste) e rimozione o blocco dei contenuti illegali siano effettuate in maniera efficace e tempestiva, né che siano tenuti in adeguato conto i diritti di tutti gli utenti[55].

3.1. La regolamentazione di alcuni contenuti specifici: i contenuti terroristici

Nella disciplina generale appena descritta rientrano solo parzialmente alcuni contenuti specifici in ragione delle speciali finalità da perseguire.

Un primo àmbito è quello dei *contenuti terroristici*, ai quali si applicano norme più stringenti in ragione della estrema gravità degli atti perpetrati con la loro diffusione *online*: la propagazione del messaggio terroristico, il reclutamento di adepti, la facilitazione e la direzione delle attività terroristiche operative[56].

L'introduzione di norme per contrastare i contenuti terroristici *online* è una delle misure prese in conseguenza degli attacchi di Parigi nel 2015 e di Bruxelles nel 2016. Da quel momento, gli ISP sono stati sottoposti a crescenti pressioni per aumentare e rendere più celeri le loro decisioni di moderazione e rimozione, contribuendo ad es. alla creazione del *Global Internet Forum to Counter Terrorism* da parte di alcune piattaforme. Parallelamente, si è intensificata l'azione non legislativa attraverso la creazione

[53] Sul passaggio dalla "responsabilità" alla "responsabilizzazione", v. G. F. FROSIO, *Why keep*, *cit.*, p. 7 ss.

[54] Così anche G. CAGGIANO, *La proposta*, *cit.*, p. 12.

[55] E infatti, l'inchiesta *The Facebook Files* ha messo in luce proprio l'esistenza di utenti privilegiati ai quali non si applicano le usuali regole di moderazione dei contenuti.

[56] In generale v. F. GALLI, *Prevenzione del terrorismo nell'Unione Europea: un nuovo ruolo e responsabilità per le piattaforme informatiche?*, in *Rassegna di diritto pubblico europeo*, 2019, p. 309 ss.; N. KLOMPMAKER, *Censor Them at Any Cost? A Social and Legal Assessment of Enhanced Action Against Terrorist Content Online*, in *Amsterdam Law Forum*, 2019, n 3, p. 3 ss., spec. p. 5 ss., e V. SACHETTI, *The EU Response to Terrorist Content Online: Too Little, (Maybe not) Too Late?*, in *European Papers*, 2021, p. 967 ss.

dell'*EU Internet Forum*[57], del *Civil Society Empowerment Programme*[58] e del *Radicalisation Awareness Network*[59]. Rilevante è anche l'attività di identificazione e segnalazione di contenuti terroristici svolta dall'*European Union Internet Referral Unit* (EU IRU) di Europol[60].

Sul versante normativo, la direttiva 2017/541/UE sulla lotta contro il terrorismo[61] ha previsto l'obbligo per gli Stati di adottare misure di contrasto ai contenuti *online* riconducibili alla pubblica provocazione a commettere reati di terrorismo (art. 21). Essi, in specie, debbono assicurarsi che i contenuti propagandistici siano tempestivamente rimossi da Internet qualora ospitati su server posizionati sul loro territorio, nonché adoperarsi per ottenerne la rimozione se presenti al di fuori dei confini nazionali. In caso di impossibilità di rimozione alla fonte, ogni Stato può adottare misure di blocco dell'accesso da parte degli utenti localizzati sul proprio territorio. Il tutto senza pregiudizio della direttiva *eCommerce*: in specie, del divieto di imporre ai *providers* obblighi generali di sorveglianza e di accertamento attivo dei contenuti terroristici, e dell'esonero dalla responsabilità per la diffusione di questi ultimi operata da terzi (a patto che non siano già a conoscenza del fatto di ospitarli sui loro servizi). A garanzia dei diritti degli utenti, le misure debbono essere trasparenti, limitate allo stretto necessario, proporzionate, motivate e soggette a eventuale controllo giurisdizionale.

A questi obblighi si aggiungono le prescrizioni della citata raccomandazione 2018/334 rivolte specificamente ai contenuti terroristici. Esse concernono le indicazioni da inserire nelle condizioni di servizio, la presentazione e il trattamento delle segnalazioni qualificate, le misure proattive anche automatizzate e la cooperazione degli *hosting providers* tra di loro e con le autorità nazionali (parr. 29-40).

Con riguardo ai fornitori di piattaforme per la condivisione di video[62], poi, la direttiva (UE) 2018/1808[63] ha apportato modifiche alla direttiva 2010/13/UE sui servizi di media audiovisivi[64]: il nuovo art. 28-*ter*,

[57] Il Forum – istituito in base a uno degli impegni presi dalla Commissione nell'Agenda europea per la sicurezza del 28 aprile 2015, COM(2015)185 final – riunisce i Ministri degli interni degli Stati, il Parlamento europeo, Europol, il Coordinatore antiterrorismo dell'UE e i rappresentanti delle principali società su Internet, con la finalità di dare attuazione al partenariato pubblico-privato per individuare e affrontare i contenuti terroristici *online*.

[58] Si tratta di un'iniziativa assunta nell'àmbito dell'*EU Internet Forum*, con lo scopo di sostenere la società civile, le organizzazioni di base e le "voci credibili" affinché forniscano alternative efficaci ai messaggi violenti e terroristici e propongano idee che contrastino la propaganda estremista e terroristica.

[59] Il network mette in contatto gli operatori di prima linea di tutta Europa tra di loro e con accademici e responsabili politici, in modo da agevolare lo scambio di conoscenze, esperienze e approcci diretti a prevenire e contrastare l'estremismo violento in tutte le sue forme, compresa quella terroristica.

[60] L'unità è stata avviata nel luglio 2015. V. il dossier *Online Jihadist Propaganda - 2020 in Review*, 2021.

[61] Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, su cui v. S. SANTINI, *L'Unione europea compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della direttiva 2017/541*, in *Diritto penale contemporaneo*, 2017, n. 7-8, p. 13 ss.

[62] Per approfondimenti v. la comunicazione della Commissione, del 7 luglio 2020, Orientamenti relativi all'applicazione pratica del criterio di funzionalità essenziale della definizione di "servizio di piattaforma per la condivisione di video" a norma della direttiva sui servizi di media audiovisivi, 2020/C 223/02.

[63] Direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018. Cfr. D. MAC SÍTHIGH, *The road*, *cit.*, p. 6 ss. Sulla proposta v. M. L. MONTAGNANI – A. Y. TRAPOVA, *Safe*, *cit.*, p. 306 ss.

[64] Direttiva 2010/13/UE del Parlamento europeo e del Consiglio, del 10 marzo 2010.

par. 1, lett. c), di quest'ultimo atto chiede ora agli Stati di fare in modo che i fornitori rientranti nella loro giurisdizione prendano misure adeguate per tutelare il grande pubblico dalla visione, tra l'altro, di contenuti terroristici, senza violare le regole della direttiva *eCommerce* (art. 28-*bis*, par. 5). I parr. 3-10 dell'art. 28-*ter* disciplinano l'attività di *procedural accountability* per l'adeguatezza delle misure in questione[65], che possono consistere in specifiche prescrizioni all'interno delle condizioni di servizio oppure nella predisposizione di sistemi trasparenti di segnalazione dei contenuti terroristici e di gestione degli eventuali reclami. Trattandosi di servizi di trasmissione televisiva tradizionale oppure *on-demand*, posti sotto il controllo dei relativi fornitori di contenuti, viene meno la necessità di intervenire nei confronti degli utenti; gli Stati, tuttavia, hanno la possibilità di adottare meccanismi di valutazione e imporre misure più dettagliate e/o rigorose[66], dovendo anche assicurare meccanismi di risoluzione giudiziale e stragiudiziale delle controversie.

La necessità di introdurre disposizioni più efficaci per contrastare i contenuti terroristici sulle piattaforme degli *hosting providers*[67] ha, da ultimo, portato all'adozione del regolamento (UE) 2021/784[68], applicabile dal 7 giugno 2022. Quest'atto mantiene l'impostazione della direttiva 2017/541, fa salve le norme della direttiva 2010/13 e approfondisce gli aspetti procedurali e sanzionatori conseguenti alle decisioni nazionali di rimozione, così cercando di conciliare la rapidità di esecuzione delle misure inibitorie con la tutela dei diritti di prestatori e utenti.

Va anzitutto detto che l'art. 2, par. 7, del regolamento innova rispetto alla direttiva del 2017 stabilendo cosa si debba intendere per "contenuti terroristici": sono tali quelli che istigano alla commissione di reati di terrorismo, sollecitano qualcuno a compiere o a partecipare a tali reati, impartiscono istruzioni per fabbricare o usare oggetti a fini terroristici oppure costituiscono una minaccia di commissione di uno di quei reati[69].

---

[65] Le misure debbono essere determinate alla luce della natura del contenuto, del danno che possono causare, delle persone da tutelare nonché dei diritti e interessi legittimi di tutti i soggetti coinvolti e dell'interesse pubblico; essere praticabili e proporzionate; tener conto delle dimensioni delle piattaforme coinvolte e della natura dei servizi offerti; e non consistere in obblighi *ex ante* contrari alla direttiva *eCommerce*.

[66] Salvo, anche qui, il divieto di stabilire obblighi generali *ex ante*.

[67] Necessità evidenziata anche dal Parlamento europeo nella risoluzione del 15 giugno 2017 sulle piattaforme online e il mercato unico digitale, P8_TA(2017)0272.

[68] Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio, del 29 aprile 2021. Sulla genesi e il contenuto della già citata proposta del 12 settembre 2018, COM(2018)640 final, v. F. GALLI, *Prevenzione*, *cit.*, p. 312 ss., e N. KLOMPMAKER, *Censor Them*, *cit.*, p. 13 ss.

[69] Sono esclusi da questa definizione i materiali diffusi per scopi educativi, giornalistici, artistici o di ricerca o a fini di prevenzione o di lotta al terrorismo, compresi quelli che rappresentano l'espressione di opinioni polemiche o controverse nell'ambito di dibattiti pubblici (art. 1, par. 3).

Il regolamento stabilisce due procedure a seconda che il *provider* destinatario di un ordine di rimozione sia o meno localizzato nello Stato membro di emissione del provvedimento[70]. Ai sensi dell'art. 3, le autorità nazionali competenti possono emettere ordini di rimozione a carico dei *providers* presenti sul loro territorio[71], che dovranno essere eseguiti al massimo entro un'ora dal loro ricevimento. In caso di procedura transfrontaliera *ex* art. 4[72], invece, l'ordine andrà trasmesso anche all'autorità nazionale competente per territorio la quale potrà esaminarlo entro 72 ore per stabilire se viola in modo grave o manifesto il regolamento o la Carta di Nizza. Per gli stessi motivi, gli *hosting providers* colpiti dall'ordine di rimozione e i fornitori dei contenuti considerati terroristici hanno facoltà di ricorrere all'autorità competente per territorio entro 48 ore affinché adotti una decisione entro le successive 72 ore. L'accertamento della contrarietà dell'ordine di rimozione transfrontaliero con il regolamento 2021/784 o la Carta di Nizza comporta la cessazione dei suoi effetti giuridici e il ripristino dei contenuti prima rimossi o disabilitati.

L'introduzione di termini così brevi per l'esecuzione delle misure inibitorie va salutata con favore, perché tiene conto della necessità di intervenire rapidamente prima che i contenuti terroristici si diffondano senza controllo. Va però detto che il regolamento si muove pur sempre nell'ottica dell'intervento *ex post*: vero è che nella raccomandazione 2018/334 era emersa l'opportunità che gli ISP introducessero un regime volontario di identificazione *ex ante* dei contenuti terroristici, così come è vero che nella proposta di regolamento del settembre 2018 la Commissione aveva fatto un passo in più, prevedendo una norma diretta a incentivare e, in alcuni casi, imporre ai prestatori l'adozione di misure proattive[73]; tuttavia, nella versione finale del regolamento – e al pari di quanto si è verificato in materia di diritto d'autore[74] – tali misure sono state ritenute troppo "dirompenti" rispetto all'impostazione tradizionale della direttiva *eCommerce*.

Il regolamento in esame prevede anche obblighi di autoregolamentazione a carico degli *hosting providers* particolarmente esposti a contenuti terroristici (art. 5)[75] nonché l'obbligo di conservare per 6 mesi i dati

[70] Il prestatore che invece non ha il proprio stabilimento principale nell'UE ha l'obbligo di designare una persona fisica o giuridica quale suo rappresentante legale ai fini del ricevimento, dell'attuazione e dell'esecuzione degli ordini di rimozione nonché di tutte le altre decisioni emesse dalle autorità competenti (art. 17, par. 1).

[71] In caso di primo ordine rivolto a uno specifico *hosting provider*, le autorità nazionali debbono però fornire informazioni su procedure e termini applicabili almeno 12 ore prima dell'emissione dell'ordine di rimozione, salvo in casi di emergenza debitamente giustificati.

[72] È tale quella in cui il *provider* ha lo stabilimento principale o il rappresentante legale in uno Stato membro diverso da quello dell'autorità emittente.

[73] Si veda l'art. 6 della proposta COM(2018)640 final e gli autori citati *supra* in nota 68.

[74] *Infra*, par. 3.3.

[75] Un *provider* identificato come "esposto" da parte dell'autorità nazionale competente (in quanto, nei 12 mesi precedenti, ha ricevuto due o più ordini di rimozione definitivi) deve introdurre nelle proprie condizioni di servizio e applicare disposizioni per contrastare l'uso improprio dei servizi per la diffusione al pubblico di contenuti terroristici. Le misure specifiche di protezione possono includere misure o capacità tecnico-operative, meccanismi di segnalazione da parte degli utenti, meccanismi di moderazione dei contenuti e qualsiasi altra misura idonea. Tali misure vanno comunicate

sui contenuti rimossi che sono necessari per procedimenti amministrativi o giurisdizionali oppure per finalità di prevenzione, accertamento, indagine o perseguimento di reati di terrorismo (art. 6). A essi si aggiungono obblighi di trasparenza in capo sia ai *providers* (art. 7) sia alle autorità competenti (art. 8), così come un opportuno obbligo per i *providers* di informare immediatamente le autorità di contenuti terroristici che comportano una minaccia imminente per la vita delle persone (art. 14, par. 5).

Gli *hosting providers* e gli utenti fornitori di contenuti considerati terroristici hanno il diritto a un ricorso effettivo dinanzi alle giurisdizioni dello Stato competente avverso tutte le decisioni assunte dalle autorità nazionali (art. 9). A loro volta, gli utenti fornitori dei contenuti rimossi o disabilitati debbono anche ricevere informazioni sui motivi di siffatte decisioni assunte dai *providers* (art. 11) e poter presentare un reclamo interno diretto alla reintegrazione di quanto rimosso o disabilitato, il cui rifiuto non osta all'avvio di procedimenti amministrativi o giurisdizionali di impugnazione (art. 10).

Per garantire l'efficacia delle disposizioni sin qui esaminate, l'art. 18 regolamento 2021/784 consente agli Stati di imporre sanzioni a carico degli *hosting providers* per la violazione delle principali decisioni delle autorità nazionali. Come sempre nel diritto UE, tali sanzioni debbono essere effettive, proporzionate e dissuasive, e la loro entità deve tener conto di una serie di circostanze. Infine, in caso di sistematica o persistente inosservanza delle decisioni di rimozione, molto efficace sembra la possibilità di imporre sanzioni pecuniarie a carico del prestatore inadempiente fino al 4% del fatturato mondiale del precedente esercizio finanziario.

3.2. ***Segue*: i contenuti pedopornografici**

Altro settore "sensibile" è quello dei *contenuti pedopornografici*, data la particolare gravità del fenomeno degli abusi sessuali di minori *online*[76]. Simili pratiche, che esistono da quando esistono i mezzi di comunicazione *online*, sono aumentate con la pandemia da coronavirus in ragione del maggior tempo trascorso dai minori su Internet a casa[77].

all'autorità nazionale competente, la quale, se le ritiene insufficienti, gliene impone di proprie (senza tuttavia poter stabilire obblighi generali di sorveglianza e di accertamento attivo dei contenuti terroristici nonché l'obbligo di utilizzare strumenti automatizzati). La decisione di esposizione e quelle contenenti le misure ritenute necessarie dall'autorità nazionali possono essere riesaminate, modificate o revocate.

[76] Come le estorsioni a sfondo sessuale e il c.d. *cyber-grooming*, consistente nel fingere un legame di amicizia con un minore allo scopo di commettere abusi sessuali.

[77] Cfr. i dati di Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2020*, 5.10.2020. V. anche l'*Annual Report 2020* della *Internet Watch Foundation* (IWF).

La direttiva 2011/93 relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile[78] stabilisce all'art. 25 le misure nella disponibilità degli Stati[79]. Questi debbono procedere alla tempestiva rimozione (non dei contenuti bensì) delle pagine web ospitate nel loro territorio che contengono o diffondono materiale pedopornografico nonché adoperarsi per la loro rimozione qualora ospitate al di fuori del territorio nazionale (par. 1). Se ciò non è possibile[80], possono essere adottate misure di blocco dell'accesso degli utenti localizzati sul proprio territorio alle pagine web "incriminate": esse però vanno prese con procedure trasparenti, limitate allo stretto necessario, proporzionate, motivate e soggette a ricorso per via giudiziaria (par. 2).

Misure specifiche sono stabilite anche nell'art. 28-*ter* della citata direttiva 2010/13, introdotto con la citata direttiva 2018/1808, secondo cui gli Stati si debbono assicurare che i fornitori di piattaforme per la condivisione di video soggetti alla loro giurisdizione adottino misure adeguate per tutelare il grande pubblico dalla visione, tra l'altro, di video che incitino a commettere reati di pedopornografia (par. 1, lett. c). Analogamente a quanto succede per i contenuti terroristici, si applicano anche qui tutte le prescrizioni dei parr. 3-10.

Infine, la specifica necessità di consentire ai fornitori dei servizi di comunicazione interpersonale (servizi di webmail, chat, messaggistica istantanea, ecc.) di continuare a svolgere, nonostante la piena applicazione del codice europeo delle comunicazioni elettroniche[81], attività volontaria proattiva di contrasto e segnalazione degli abusi sessuali *online* sui minori che si verificano tramite i loro servizi[82] è alla base dell'adozione del recente regolamento 2021/1232[83].

L'atto in questione introduce una deroga temporanea[84] e limitata agli artt. 5, par. 1 (riservatezza delle comunicazioni) e 6 (dati sul traffico) della direttiva *ePrivacy*[85], in modo da permettere ai fornitori di quei servizi di continuare a utilizzare tecnologie proattive per l'individuazione degli abusi sessuali *online* sui minori, la segnalazione alle autorità competenti e la rimozione del materiale pedopornografico. Al fine di

[78] Direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011. Cfr. A. VERRI, *Contenuto ed effetti (attuali e futuri) della direttiva 2011/93/UE*, in *Diritto penale contemporaneo*, 28.03.2012, reperibile *online*.

[79] *Amplius* v. K. DEMEYER – E. LIEVENS – J. DUMORTIER, *Blocking and Removing Illegal Child Sexual Content: Analysis from a Technical and Legal Perspective*, in *Policy & Internet*, 2012, n. 3-4, p. 1 ss.

[80] Ad es. perché lo Stato ospitante non coopera oppure perché il processo di rimozione si rivela particolarmente lungo.

[81] Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018.

[82] Coerentemente, peraltro, con la strategia dell'UE per una lotta più efficace contro gli abusi sessuali su minori (comunicazione del 24 luglio 2020, COM(2020)607 final).

[83] Regolamento (UE) 2021/1232 del Parlamento europeo e del Consiglio, del 14 luglio 2021.

[84] Fino al 3 agosto 2024, in attesa che venga adottato, come si è proposta la Commissione anche nel programma di lavoro 2021 (comunicazione del 19 ottobre 2020, COM(2020)690 final), un quadro giuridico a più lungo termine per contrastare gli abusi sessuali sui minori. Secondo il *Joint Statement* della *Ministerial Conference on the Prevention and Investigation of Child Sexual Abuse*, 11-12 novembre 2021, la proposta dovrebbe essere pubblicata a breve.

[85] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002.

limitare il più possibile il carattere intrusivo della deroga[86], l'art. 3 regolamento 2021/1232 stabilisce alcune prescrizioni a carico dei fornitori. Si richiede, in specie, che il trattamento sia strettamente necessario alle finalità previste, che sia proporzionato e limitato alle tecnologie utilizzate, e circoscritto ai dati sul contenuto e ai dati sul traffico strettamente necessari[87]. Le tecnologie utilizzabili[88], preventivamente esaminate dalle autorità nazionali (par. 1, lett. c) e d)[89], debbono essere conformi allo stato dell'arte (lett. b) e limitare il più possibile il tasso di errori (lett. e)[90]. Si richiede, inoltre, la garanzia del controllo e dell'intervento umano sulle tecnologie in parola (lett. g), *sub* ii); la previsione di procedure e meccanismi per la presentazione dei reclami da parte degli utenti (*sub* iv); l'informazione a questi ultimi dell'uso e delle conseguenze di siffatti mezzi tecnologici (*sub* v); e, in caso di rimozione di specifici contenuti, la comunicazione agli utenti circa le modalità di presentazione dei ricorsi, la possibilità di presentare un reclamo all'autorità di controllo e il diritto al ricorso giurisdizionale (*sub* vi).

3.3. ***Segue*: i contenuti protetti dal diritto d'autore**

Per quanto riguarda la rimozione dei *contenuti protetti dal diritto d'autore*, il regime normativo è stato da poco modificato, nei confronti dei prestatori di servizi di condivisione di contenuti *online*, dalla direttiva 2019/790 sul diritto d'autore nel mercato unico digitale[91].

La direttiva 2001/29[92], che tutela il diritto d'autore e i diritti connessi nel mercato interno, prevede alcuni diritti che gli Stati debbono riconoscere agli autori (e ad altri soggetti). In particolare, l'art. 3 afferma che i titolari dei diritti hanno "il diritto esclusivo di autorizzare o vietare qualsiasi comunicazione al pubblico, su filo o senza filo, delle loro opere, compresa la messa a disposizione del pubblico delle loro opere in maniera tale che ciascuno possa avervi accesso dal luogo e nel momento scelti individualmente". La Corte

[86] Si noti che il Garante europeo per la protezione dei dati personali, nel suo parere del 10 novembre 2020, si era espresso negativamente sulla proposta del 10 settembre 2020, COM(2020)568 final, paventando rischi di violazione generalizzata dei dati personali degli utenti.
[87] Sotto questo profilo, l'art. 1, par. 2, esclude la propria applicazione alle comunicazioni audio.
[88] In genere, il materiale pedopornografico *online* viene rilevato con tecnologie specifiche che analizzano il contenuto (immagini e testo) o i dati sul traffico. La tecnologia di *hashing* è rivolta a identificare immagini e video, mentre testi e dati sono analizzati con i classificatori e l'intelligenza artificiale. Vedi M. NEGREIRO, *Curbing the surge in online child abuse. The dual role of digital technology in fighting and facilitating its proliferation*, novembre 2020, e J. P. MIFSUD BONNICI – M. TUDORICA – K. MODH – H. HAILU ABRAHA, *Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse. Targeted substitute impact assessment*, febbraio 2021, p. 14 ss. Si ricorda anche l'intenzione della società Apple di scansionare tutti gli iPhone degli Stati Uniti alla ricerca di immagini di abusi sessuali su minori.
[89] L'esame viene condotto ai sensi degli artt. 35 e 36 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (regolamento generale sulla protezione dei dati).
[90] Nel caso in cui si verifichino errori, bisogna correggerli senza indugio.
[91] Direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019. In generale v. V. BOCCHETTI, *La direttiva dell'Unione europea sul diritto d'autore*, in *DUE online*, 19.06.2019; D. MAC SÍTHIGH, *The road*, *cit.*, p. 9 s.; G. M. RUOTOLO, *Scritti*, *cit.*, p. 179 ss.; e l'ampio commento di I. STAMATOUDI – P. TORREMANS, *The Digital Single Market Directive*, in ID., *EU Copyright Law. A Commentary*, Cheltenham-Northampton, 2021, p. 651 ss.
[92] Direttiva 2001/29/CE del Parlamento europeo e del Consiglio, del 22 maggio 2001.

di giustizia si è occupata di verificare se le attività degli *hosting providers* possano qualificarsi come "atti di comunicazione al pubblico" non autorizzati per via dell'esistenza di contenuti protetti caricati illegalmente dagli utenti, escludendo la loro responsabilità diretta ogni qualvolta si limitino a svolgere un ruolo passivo[93] o, in taluni casi, attività senza fini di lucro[94]. In senso conforme anche la più recente sentenza *YouTube* e *Cyando*, in cui si ribadisce che gli *hosting providers* non sono responsabili diretti per la diffusione di contenuti protetti dal diritto d'autore se si limitano a mettere a disposizione le loro piattaforme e non contribuiscono a dare accesso ai contenuti che i loro utenti mettono illecitamente in rete[95].

Quanto alla *secondary liability*, è stato ritenuto pienamente applicabile, anche per i contenuti in esame, il regime della direttiva *eCommerce* facendo così salvi sia il divieto a carico degli Stati di imporre misure generali di sorveglianza e accertamento attivo *ex* art. 15[96], sia la possibilità per i prestatori di usufruire dell'esenzione da quella responsabilità alle condizioni stabilite nell'art. 14. Non a caso, nella pronunzia *YouTube* e *Cyando* viene confermata l'esenzione qualora gli intermediari svolgano un ruolo tecnico, automatico e passivo, senza avere conoscenza o controllo dei contenuti ospitati sulle loro piattaforme e senza essere al corrente di atti illeciti concreti compiuti dai loro utenti[97].

Resta ferma anche qui la possibilità per le autorità giurisdizionali e amministrative nazionali di adottare specifiche misure di rimozione e blocco a carico dei prestatori intermediari. In quest'ottica, l'art. 8, par. 3, direttiva 2001/29 sancisce il diritto dei titolari di "chiedere un provvedimento inibitorio nei confronti degli intermediari i cui servizi siano utilizzati da terzi per violare un diritto d'autore o diritti connessi"[98].

---

[93] Ragionando *a contrario*, nella sentenza del 14 giugno 2017, causa C-610/15, *Stichting Brein*, ECLI:EU:C:2017:456, la Corte ha precisato che la fornitura e la gestione di una piattaforma di condivisione *online* di opere protette quale "The Pirate Bay" poteva costituire una violazione del diritto d'autore in quanto, nonostante tali opere fossero caricate dagli utenti della piattaforma, quest'ultima svolgeva un ruolo attivo attraverso l'indicizzazione dei file torrent, la loro suddivisione in categorie e l'eliminazione di quelli obsoleti ed errati.

[94] Così la sentenza dell'8 settembre 2016, causa C-160/15, *GS Media*, ECLI:EU:C:2016:644, secondo cui il collocamento su di un sito web di un collegamento ipertestuale verso opere protette dal diritto d'autore e pubblicate senza l'autorizzazione dell'autore su altro sito web non costituisce una comunicazione al pubblico quando la persona che colloca detto link agisce senza fini di lucro e senza essere al corrente dell'illegittimità della pubblicazione di dette opere; se invece i collegamenti ipertestuali sono forniti a fini di lucro, la conoscenza dell'illegittimità della pubblicazione sull'altro sito Internet deve essere presunta.

[95] Sentenza *YouTube* e *Cyando*, punto 102. Sulle conclusioni dell'Avvocato generale del 16 luglio 2020, ECLI:EU:C:2020:586, v. G. SMITH, *Advocate General advises CJEU on copyright liability of online sharing platforms*, in *Journal of Intellectual Property Law & Practice*, 2020, p. 857 s. Simile condizione non è invece soddisfatta nel caso in cui i prestatori siano messi al corrente della presenza illecita di quei contenuti e ciò nonostante si astengano dal rimuoverli o disabilitarli; oppure, pur sapendo che la piattaforma viene generalmente utilizzata per diffondere in maniera illecita contenuti protetti, si astengano dal predisporre le idonee misure tecniche che ci si può attendere da operatori normalmente diligenti per contrastare tale diffusione; o, ancora, si rendano parti attive nelle condotte illecite (ad es. partecipando alla selezione di contenuti protetti comunicati illecitamente al pubblico, fornendo strumenti specificamente destinati alla condivisione illecita di quei contenuti, o promuovendo scientemente condivisioni del genere), specie se adottano un modello economico idoneo a incoraggiare gli utenti alla diffusione di contenuti protetti.

[96] Si veda in nota 19 quanto affermato nelle sentenze *Scarlet Extended* e *SABAM* c. *Netlog*.

[97] Sentenza *YouTube* e *Cyando*, punto 118.

[98] Così il considerando 59.

Si è già detto[99] che la possibilità di essere interessati da misure nazionali di rimozione e blocco deriva non tanto da specifiche responsabilità quanto piuttosto dalla posizione più idonea in cui si trovano i prestatori per porre fine agli illeciti altrui: ebbene, nella sentenza *YouTube* e *Cyando* la Corte ha sottolineato che provvedimenti di questo tipo possono essere ottenuti nei confronti degli *hosting providers*, anche se non responsabili, purché la violazione lamentata sia stata previamente notificata e i *providers* non siano intervenuti immediatamente sia per rimuovere o bloccare l'accesso ai contenuti protetti segnalati (*take-down*), sia per garantire il ripetersi di analoghe violazioni in futuro (*stay-down*)[100].

Come si anticipava, il regime sin qui descritto subisce una deviazione più restrittiva a opera della direttiva 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale[101], introdotta per adeguare l'ordinamento dell'UE all'evoluzione delle tecnologie digitali.

È importante ai nostri fini l'art. 17 sull'utilizzo dei contenuti protetti da parte dei prestatori di servizi di condivisione di contenuti *online*, intendendo per tali quei *providers* che si occupano prevalentemente di memorizzare e dare accesso al pubblico a grandi quantità di opere protette dal diritto d'autore o altri materiali protetti caricati dai loro utenti, a scopo di lucro[102]. Si tratta, in breve, dei grandi prestatori di servizi di *streaming* video e/o audio, i cui contenuti sono caricati direttamente dagli utenti (es. YouTube, Soundcloud, Pinterest) e ove la remunerazione proviene dalla vendita di spazi pubblicitari[103]. Scopo della disposizione è, infatti, quello di ridurre il *value gap* tra i considerevoli ricavi dei prestatori, derivanti dagli introiti pubblicitari, e gli scarsi proventi che a loro volta versano ai titolari dei diritti. La mancanza di chiarezza circa l'applicabilità o meno nei loro confronti dell'esenzione dalla responsabilità indiretta della direttiva *eCommerce*[104] aveva portato i prestatori a rifiutarsi di concludere accordi di licenza oppure a stipularli a condizioni non eque per i titolari.

L'art. 17 direttiva 2019/790 prevede ora che l'attività di concessione dell'accesso al pubblico a grandi quantità di opere o materiali protetti caricati dagli utenti integri, per ciò stesso, un atto di comunicazione al pubblico ai sensi dell'art. 3 direttiva 2001/29 e che, di conseguenza, i prestatori interessati debbano ottenere un'autorizzazione dai titolari dei diritti per poterli diffondere (par. 1)[105]. In questa maniera, il

[99] *Supra*, nota 31 e testo corrispondente.
[100] Sentenza *YouTube* e *Cyando*, punto 143.
[101] Deviazione che però, in virtù della giurisprudenza *YouTube* e *Cyando*, è oggi meno rilevante di quando la direttiva 2019/790 è stata approvata.
[102] Come specifica il considerando 62, da tale definizione esulano i servizi di comunicazione elettronica (es. i servizi di accesso a Internet, quelli di comunicazione interpersonale, quelli di diffusione circolare radiotelevisiva), i servizi *cloud* da impresa a impresa, i servizi *cloud* a disposizione degli utenti privati e i *marketplace* che non dànno accesso a contenuti protetti dal diritto d'autore.
[103] La questione, viceversa, non rileva per i servizi di *streaming* che diffondono contenuti ottenuti in base a licenze dei titolari dei diritti e messi *online* non da terzi bensì dal *provider* stesso (es. Spotify, Apple Music, ecc.).
[104] Circostanza riconosciuta anche nella comunicazione del 4 giugno 2021, Orientamenti relativi all'articolo 17, COM(2021)288 final.
[105] *Ivi*, p. 6 ss., per un approfondimento sui modelli di autorizzazione.

legislatore UE ha chiarito, seppur ai soli fini dell'applicazione dell'art. 17, che la nozione di "comunicazione al pubblico" va estesa *ex lege specialis* alle attività di quei prestatori e che questi ultimi non possono avvalersi dell'esonero dalla responsabilità indiretta di cui all'art. 14 direttiva *eCommerce* (par. 3).

La differenza rispetto al regime "normale" si apprezza nel momento in cui i prestatori dei servizi interessati non ottengono l'autorizzazione dei titolari dei diritti. In casi simili, l'art. 17, par. 4, stabilisce a loro carico una responsabilità diretta *sui generis* per la diffusione illecita di contenuti e materiali protetti da parte dei propri utenti, di cui i prestatori possono liberarsi solo dimostrando di aver compiuto i massimi sforzi per ottenere l'autorizzazione e per assicurarsi che, sulle loro piattaforme, non siano disponibili specifici contenuti illeciti per i quali abbiano ricevuto informazioni pertinenti e necessarie. Inoltre, essi debbono in ogni caso dimostrare di aver agito con tempestività per disabilitare l'accesso o rimuovere opere o altri materiali oggetto di segnalazione (*take-down*) nonché di aver compiuto i massimi sforzi per impedire il loro caricamento in futuro (*stay-down*)[106].

Al fine di bilanciare gli interessi dei soggetti coinvolti, l'art. 17 prevede una parziale esenzione da questo regime rafforzato di responsabilità per alcuni nuovi prestatori[107]; l'obbligo per gli Stati di garantire meccanismi di risoluzione giudiziale e stragiudiziale delle controversie nonché di non pregiudicare gli usi legittimi dei contenuti in esame, come anche la possibilità di introdurre eccezioni per gli utenti che diffondono materiali contenenti citazioni, critiche, rassegne, utilizzi a scopo di caricatura, parodie o *pastiche* (es. i *meme*); l'obbligo per i prestatori di introdurre meccanismi di reclamo e ricorso celeri ed efficaci, di trattare i reclami senza indebito ritardo e di sottoporre a verifica umana le decisioni automatizzate di rimozione o disabilitazione; nonché l'obbligo per i titolari di indicare debitamente i motivi della richiesta di rimozione o disabilitazione.

Riassumendo, l'art. 17 della direttiva 2019/790, rispetto a quanto disposto per la generalità dei prestatori sui cui servizi vengono diffusi contenuti protetti dal diritto d'autore (come specificato, da ultimo, nella sentenza *YouTube* e *Cyando*), prevede addirittura la responsabilità diretta a carico dei prestatori di servizi *streaming* di grandi dimensioni per i contenuti caricati dagli utenti, il cui esonero dipende dal soddisfacimento di stringenti condizioni. Così disponendo, la direttiva 2019/790 ha assegnato alle operazioni di moderazione e rimozione o disabilitazione (sia attuali sia future) un ruolo ancor più incisivo di prima. Ciò nonostante, la versione finale dell'art. 17 risulta meno onerosa per i prestatori della corrispondente previsione dell'art. 13 della proposta del 2016[108]. Se il regime proposto dalla Commissione fosse stato mantenuto nel testo finale, infatti, i prestatori si sarebbero ritrovati a svolgere controlli

[106] *Ivi*, p. 9 ss., per maggiori dettagli.
[107] Sono tali coloro i cui servizi sono disponibili da meno di tre anni e che hanno un fatturato annuo inferiore a 10 milioni di EUR.
[108] Proposta COM(2016)593, sulla quale v. G. COLANGELO – M. MAGGIOLINO, *ISPs' copyright liability in the EU digital single market strategy*, in *International Journal of Law and Information Technology*, 2018, p. 142 ss.

obbligatori *ex ante* con l'uso massivo e generalizzato di tecnologie di riconoscimento di tutti i contenuti illecitamente caricati (c.d. *upload filters*)[109], circostanza vigorosamente osteggiata durante l'*iter* legislativo dai prestatori e da una parte della società civile[110]: ciò avrebbe comportato un deciso cambiamento di prospettiva rispetto alla situazione attuale[111], rendendo in gran parte inutili le attività di moderazione e rimozione dei contenuti audio/video.

A ben vedere, se è vero che l'art. 17 della direttiva non riproduce il contenuto della proposta della Commissione e, anzi, fa salvo al par. 8 il divieto di imporre obblighi generali di sorveglianza, è altrettanto vero che l'ultima condizione del par. 4 in un certo qual modo impone (pur non esplicitamente) l'utilizzazione di strumenti tecnologici di riconoscimento di contenuto per evitare non ogni caricamento illecito (come previsto nella proposta e non accolto) bensì solo quello futuro dei contenuti già rimossi o disabilitati in base a precedente segnalazione[112]. In altri termini, la norma esaminata non stabilisce l'obbligo di utilizzare strumenti di controllo generalizzato preventivo, bensì – coerentemente con la giurisprudenza *YouTube* e *Cyando* – solo l'onere di adottare un efficace sistema di *notice-and-stay-down* per liberarsi della responsabilità, in questo caso, diretta. La conformità o meno di siffatto onere rispetto al diritto alla libertà di espressione e di informazione[113] è attualmente oggetto di valutazione da parte della Corte di giustizia, in una causa di annullamento proposta dalla Polonia sulla quale si è di recente espresso l'Avvocato generale[114].

Quanto agli impegni volontari, si segnala il *Memorandum d'intesa sulla pubblicità online e sui diritti di proprietà intellettuale* del 25 giugno 2018[115], promosso dalla Commissione e sottoscritto (al 7 luglio 2021) da 29 parti coinvolte a vario titolo nelle attività di collocamento, acquisto, vendita e/o facilitazione della pubblicità *online*. Il Memorandum prende in considerazione una delle forme più diffuse di violazione *online* dei diritti di proprietà intellettuale, consistente nell'attività di siti web e applicazioni che offrono scientemente e gratuitamente contenuti illegali (libri, film, musica, ogni tipo di merce contraffatta) e che capitalizzano l'alto volume di traffico di utenti così generato attraverso la vendita degli spazi pubblicitari. Ferma

[109] Sui quali G. F. FROSIO, *Why keep*, *cit.*, p. 20 ss, e G. SARTOR – A. LOREGGIA, *The impact of algorithms for online content filtering or moderation. "Upload filters"*, settembre 2020.
[110] In proposito v. M. L. MONTAGNANI – A. Y. TRAPOVA, *Safe*, *cit.*, p. 300 ss.
[111] *Ivi*, p. 299. Cfr. anche G. M. RUOTOLO, *Scritti*, *cit.*, p. 202.
[112] Questo perché, molto spesso, i contenuti rimossi venivano rimessi *online* poco dopo, il che di regola costringeva i titolari dei diritti a fare "ingiunzioni-fotocopia" l'una dietro l'altra.
[113] In ragione del rischio che gli *upload filters* blocchino anche contenuti che possono legittimamente essere diffusi *online*, ad es. perché non coperti da diritto d'autore o perché rientranti nelle eccezioni a quel diritto.
[114] Conclusioni del 15 luglio 2021, causa C-401/19, *Polonia* c. *Parlamento europeo* e *Consiglio*, ECLI:EU:C:2021:613, in cui il sistema dell'art. 17 è stato ritenuto conforme all'art. 11, par. 1, della Carta di Nizza. Cfr. B. J. JÜTTE – C. GEIGER, *Regulating freedom of expression on online platforms? Poland's action to annul Article 17 of the Directive on Copyright in the Digital Single Market Directive*, in *European Law Blog*, 3.02.2021, e L. WOODS, *Copyright and the Internet: Poland v Parliament and Council (Case C-401/19), Opinion of the Advocate General, 15 July 2021*, in *EU Law Analysis*, 10 agosto 2021.
[115] *Memorandum of understanding on online advertising and IPR*. Cfr. G. F. FROSIO, *Why keep*, *cit.*, p. 15, e A. BERTOLINI – F. EPISCOPO – N.-A. CHERCIU, *Liability*, *cit.*, pp. 39-40.

restando la possibilità per i titolari dei diritti di chiedere provvedimenti inibitori (secondo le regole note), il Memorandum si ripropone di limitare la pubblicità su tali siti e applicazioni con l'accordo di inserzionisti, intermediari pubblicitari e associazioni del settore. Le prime due categorie si sono impegnate, tra l'altro, ad adottare misure ragionevoli per assicurarsi di rimuovere la pubblicità non appena vengano a conoscenza della sua collocazione su siti e applicazioni "incriminati". Si tratta, a ben vedere, di una forma di rimozione "indiretta" dei contenuti protetti, sulla base dell'approccio *follow-the-money*[116] che si sta dimostrando particolarmente efficace[117].

La questione interessa, com'è noto, anche le trasmissioni sportive in diretta diffuse illegalmente *online*, data l'attività di numerosi siti web che diffondono tali contenuti in cambio di sottoscrizioni a pagamento e/o della vendita di spazi pubblicitari. Qui il problema è particolarmente acuto per due ragioni: da un lato, l'evento sportivo non rientra di per sé – a differenza della sua registrazione – tra le opere protette e di conseguenza i titolari dei diritti sulle trasmissioni non hanno possibilità di chiedere provvedimenti inibitori; dall'altro, la maggior parte del valore di quelle trasmissioni si esaurisce al termine della diretta, per cui le misure di rimozione dovrebbero essere effettuate quasi "in tempo reale" per essere efficaci. Ecco perché, a fronte dell'impegno sinora non rispettato dalla Commissione di valutare un intervento *ad hoc*[118], il Parlamento europeo le ha recentemente chiesto di avanzare una proposta legislativa[119] finalizzata a introdurre procedure per il blocco in tempo reale o la rimozione dei contenuti sportivi piratati[120] e a garantire che esse colpiscano solo i contenuti illegali[121].

3.4. *Segue*: i contenuti che violano altri diritti di proprietà intellettuale

Misure di rimozione e disabilitazione possono essere adottate anche come conseguenza dell'attività di moderazione dei *contenuti che violano diritti di proprietà intellettuale diversi dal diritto d'autore*.

---

[116] Diretto, cioè, a rendere economicamente svantaggiosa per i gestori di quei siti web e applicazioni la prosecuzione del modello di *business* intrapreso.

[117] Secondo la relazione della Commissione, del 14 agosto 2020, sul funzionamento del Memorandum, SWD(2020)167 final, nel primo anno di applicazione la quota di pubblicità delle imprese europee su siti web che violano i diritti di proprietà intellettuale è scesa del 12%, mentre la pubblicità delle grandi marche è diminuita dal 62% al 50% nel settore del gioco d'azzardo; tendenze al ribasso si sono registrate anche relativamente ai grandi marchi e agli intermediari pubblicitari dell'UE. V. anche il documento preparato da WHITE BULLET SOLUTIONS LIMITED, *Study on the impact of the Memorandum of Understanding on online advertising and intellectual property rights on the online advertising market - 2020 Ad Monitoring Exercise*, luglio 2021.

[118] Si veda l'allegato alla risoluzione legislativa del Parlamento europeo del 26 marzo 2019 sulla proposta di direttiva del Parlamento europeo e del Consiglio sul diritto d'autore nel mercato unico digitale, P8_TA(2019)0231.

[119] Risoluzione del Parlamento europeo del 19 maggio 2021 recante raccomandazioni alla Commissione sulle sfide per gli organizzatori di eventi sportivi nell'ambiente digitale, P9_TA(2021)0236.

[120] *Ivi*, par. 20. In argomento v. L. PANELLA, *Challenges facing sports event organisers in the digital environment. European added value assessment*, dicembre 2020.

[121] Risoluzione P9_TA(2021)0236, par. 21.

Il regime a carattere orizzontale è contenuto nella direttiva 2004/48, che contempla la possibilità di emettere misure provvisorie e cautelari, misure correttive e ingiunzioni. Anzitutto, l'art. 9, par. 1, lett. a), permette alle autorità giudiziarie di vietare provvisoriamente il proseguimento di violazioni dei diritti di proprietà intellettuale a carico sia dei presunti autori, sia degli intermediari i cui servizi siano utilizzati a questi scopi: tra queste, rientrano le misure di rimozione dei (e blocco dell'accesso *online* ai) contenuti illegali. Inoltre, ai sensi dell'art. 10, le autorità giudiziarie possono anche ordinare, per le merci sicuramente contraffatte, la loro rimozione ed esclusione definitiva dai circuiti commerciali anche *online*. Infine, in presenza di decisioni giudiziarie di accertamento di avvenuta violazione, l'art. 11 consente a quelle autorità di emettere ingiunzioni dirette a vietare agli autori il proseguimento delle stesse nonché provvedimenti ingiuntivi attuali e futuri a carico degli intermediari sui cui servizi si siano verificate[122].

Anche qui, la possibilità di emettere ingiunzioni interlocutorie e definitive, attuali e future, nei confronti degli intermediari *online* – tra cui rientrano gli *online marketplaces* e i *social networks*[123] – non dipende da una loro qualche responsabilità ma dall'esigenza che i titolari possano far valere in maniera efficace i propri diritti. Resta ferma, ovviamente, la possibilità di riscontrare anche la responsabilità indiretta qualora un prestatore non si limiti a un ruolo passivo, così come nel caso in cui sia al corrente di fatti o circostanze in base ai quali un operatore economico diligente avrebbe dovuto constatare l'illiceità dei contenuti offerti e non li abbia prontamente rimossi o disabilitati[124].

Le misure generali della direttiva 2004/48 si applicano laddove non vi siano disposizioni specifiche per singoli diritti di proprietà intellettuale. Ad es., in materia di marchio, mentre la direttiva 2015/2436[125] non contiene norme di *enforcement*, il regolamento 2017/1001 sul marchio UE ammette la possibilità di emettere misure (anche di rimozione) per vietare la prosecuzione di atti di contraffazione nonché misure provvisorie e cautelari[126]. Allo stesso modo, nella protezione dei disegni e dei modelli, la direttiva 98/71[127] non prevede norme sulla rimozione a differenza del regolamento 6/2002 che contempla misure dirette a impedire atti di contraffazione oltre a quelle provvisorie e cautelari[128].

---

[122] Come evidenziato nella sentenza *L'Oréal SA* e *a.* c. *eBay*, punto 144. Il tutto, però, senza sconfinare nel divieto di imporre gli obblighi generali *ex ante* dell'art. 15 direttiva *eCommerce*.

[123] Cfr. la comunicazione della Commissione, del 29 novembre 2017, Orientamenti in merito ad alcuni aspetti della direttiva 2004/48/CE del Parlamento europeo e del Consiglio sul rispetto dei diritti di proprietà intellettuale, COM(2017)708 final, p. 19.

[124] Sentenza *L'Oréal SA* e *a.* c. *eBay*, punti 133-134. La tendenza a restringere la nozione di intermediari passivi, come si è detto, è stata confermata in materia di diritto d'autore dall'art. 17 direttiva 2019/790 (*supra*, par. 3.3).

[125] Direttiva (UE) 2015/2436 del Parlamento europeo e del Consiglio, del 16 dicembre 2015.

[126] Regolamento (UE) 2017/1001 del Parlamento europeo e del Consiglio, del 14 giugno 2017, artt. 130 e 131.

[127] Direttiva 98/71/CE del Parlamento europeo e del Consiglio, del 13 ottobre 1998.

[128] Regolamento (CE) n. 6/2002 del Consiglio, del 12 dicembre 2001, artt. 89 e 90.

Quali misure di co-regolamentazione, infine, si ricordano il già citato Memorandum sulla pubblicità *online*[129] e il *Memorandum d'intesa sulla vendita delle merci contraffatte via internet*. Quest'ultimo, firmato sotto gli auspici della Commissione nel 2011 e, dopo una sua revisione, nel 2016, riunisce (al 7 ottobre 2021) 32 parti tra titolari di diritti, piattaforme *online* e associazioni di imprese. Esso contiene impegni relativi ai beni dei quali vengono vendute *online* versioni contraffatte e piratate e assegna un ruolo importante alle procedure di *notice-and-take-down*. In particolare, si stabilisce la possibilità per i titolari dei diritti di notificare in buona fede alle piattaforme *online* l'esistenza di venditori generalmente impegnati nella vendita di merci contraffatte, previa corretta identificazione delle offerte di tali beni. A loro volta, le piattaforme si impegnano a prendere in considerazione le informazioni nel quadro delle loro misure proattive e preventive; a mettere a disposizione procedure di rimozione efficienti, efficaci, facilmente accessibili e non eccessivamente onerose; nonché a procedere alla rapida rimozione o disabilitazione delle offerte notificate e ad adottare misure deterrenti in relazione ai venditori. Nei confronti di coloro che vendono sistematicamente beni contraffatti, inoltre, le piattaforme si impegnano a prendere misure deterrenti e a valutare, tra l'altro, la sospensione e la rimozione degli *account* interessati[130].

3.5. *Segue*: i prodotti non sicuri o pericolosi

Vi sono anche normative che prevedono la possibilità esplicita o implicita di disporre misure di rimozione di altro tipo di prodotti venduti *online*. Nell'impossibilità di esaminarle tutte in questa sede, ci soffermiamo sui *prodotti non sicuri (o pericolosi)*[131]. Il quadro regolatorio si compone essenzialmente di due parti: quella relativa alla sicurezza generale dei prodotti e quella sulla vigilanza del mercato. Entrambe prevedono la possibilità di disporre la rimozione dei prodotti non sicuri[132].

La prima parte è disciplinata dalla direttiva 2001/95, concernente per l'appunto la sicurezza generale dei prodotti[133], che si applica ai prodotti non oggetto di misure di armonizzazione a livello UE. Nel prescrivere il generale obbligo che quelli immessi in commercio siano sicuri, l'atto in esame stabilisce un obbligo di ritiro – evidentemente, anche dai circuiti commerciali *online* – dei prodotti non sicuri se

[129] *Supra*, par. 3.3.

[130] Per una valutazione degli aspetti positivi e negativi del Memorandum, v. il documento della Commissione del 14 agosto 2020, *Report on the functioning of the Memorandum of Understanding on the sale of counterfeit goods on the internet*, SWD(2020)166 final.

[131] Intendendo per tali i prodotti non-alimentari che, in condizioni di uso normali o ragionevolmente prevedibili, presentano rischi non di minima entità, non compatibili col loro impiego e considerati non accettabili nell'osservanza di un livello elevato di tutela della salute e della sicurezza delle persone. La definizione si ricava dall'art. 2 della direttiva 2001/95/CE del Parlamento europeo e del Consiglio, del 3 dicembre 2001.

[132] Per approfondimenti v. C. ULLRICH, *New Approach meets new economy: Enforcing EU product safety in e-commerce*, in *Maastricht Journal of European and Comparative Law*, 2019, p. 558 ss.

[133] La direttiva si riferisce a qualunque prodotto destinato ai (o suscettibile di essere utilizzato dai) consumatori, che sia nuovo o usato, che sia fornito gratuitamente o a titolo oneroso nell'ambito di un'attività commerciale.

necessario per evitare rischi per i consumatori, obbligo che grava sui produttori (art. 5, par. 1) e sui distributori (parr. 2 e 3). Dal canto loro, le autorità competenti degli Stati dispongono del potere di ordinare il ritiro effettivo e immediato di qualsiasi prodotto pericoloso già immesso in commercio (art. 8, par. 1, lett. f), anche qualora l'azione intrapresa da produttori e distributori risulti insoddisfacente o insufficiente (par. 2), nonché del potere di rimuovere celermente i prodotti che presentano un rischio grave per i consumatori (par. 3). L'ordine di rimozione dai circuiti commerciali dei prodotti non sicuri, ai sensi del par. 4, può essere diretta anche a qualunque altra persona, se necessario per la migliore riuscita delle azioni delle autorità nazionali.

Quanto alla vigilanza del mercato, le disposizioni del regolamento 765/2008[134] sono state sostituite, dal 16 luglio 2021, da quelle del regolamento 2019/1020 sulla vigilanza del mercato e la conformità dei prodotti[135]. Quest'atto, che si applica ai prodotti c.d. "armonizzati"[136], assegna alle autorità di vigilanza degli Stati membri, tra gli altri, il potere di imporre il ritiro dei prodotti non conformi o rischiosi dal mercato (art. 14, par. 4, lett. h). Da notare che il regolamento del 2019 prende in espressa considerazione anche la posizione dei prestatori che gestiscono *marketplaces online*: questi debbono cooperare con le autorità di vigilanza, in casi specifici, per agevolare l'eliminazione o l'attenuazione dei rischi presentati da un prodotto messo in vendita *online* attraverso i loro servizi (art. 7, par. 2); inoltre, in assenza di altri mezzi efficaci, le autorità possono imporre la rimozione dei contenuti dall'interfaccia *online*, ordinare la visualizzazione esplicita di un'avvertenza per gli utenti o ancora, in caso di mancata ottemperanza, disporre la limitazione dell'accesso all'interfaccia *online* anche chiedendo la collaborazione di terzi (art. 14, par. 4, lett. k).

Come è stato sottolineato[137], questa disposizione consacra nella normativa europea sulla vigilanza di mercato la procedura di "*notice-and-action*", che era già nella disponibilità di alcune autorità nazionali in base a disposizioni interne[138] ed era stata accolta nel regolamento 2017/2394 sulla cooperazione tra le autorità nazionali a tutela dei consumatori[139] in termini quasi sovrapponibili a quelli del regolamento 2019/1020[140]. La *notice-and-action*, che l'art. 14 proposta DSA generalizza nei confronti degli *hosting providers*

134 Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008.
135 Regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio, del 20 giugno 2019.
136 L'allegato I del regolamento reca l'elenco delle normative di armonizzazione.
137 Da A. BERTOLINI – F. EPISCOPO – N.-A. CHERCIU, *Liability*, *cit.*, pp. 60-61.
138 Comunicazione della Commissione, del 1° agosto 2017, sulla vigilanza del mercato dei prodotti venduti online, 2017/C 250/01, par. 5.2.
139 Regolamento (UE) 2017/2394 del Parlamento europeo e del Consiglio, del 12 dicembre 2017.
140 L'art. 9, par. 4, lett. g), regolamento 2017/2934 attribuisce alle autorità nazionali non solo i poteri di rimuovere i contenuti o limitare l'accesso all'interfaccia *online*, di imporre la visualizzazione esplicita di un'avvertenza rivolta ai consumatori e di imporre ai prestatori di servizi di hosting di rimuovere, disabilitare o limitare l'accesso a un'interfaccia *online*, ma anche – a differenza del regolamento 2019/1020 – quello di imporre ai registri o alle autorità di registrazione del dominio di rimuovere un nome di dominio completo.

relativamente a tutti i contenuti illegali, non si deve risolvere nell'imposizione di obblighi generali di sorveglianza *ex* art. 15 direttiva *eCommerce* e va inserita nel quadro della regola dell'art. 14 di quest'ultimo atto, dal momento che la notifica effettuata dalle autorità nazionali di vigilanza ai *marketplaces* che trattano sulla loro interfaccia prodotti non sicuri integra la "conoscenza dei fatti" propedeutica alle misure di rimozione e disabilitazione ivi previste[141]. Va da sé che l'esenzione dalla responsabilità secondaria non opera anche qualora i *marketplaces*, pur non ricevendo segnalazioni, svolgano un ruolo attivo rispetto ai prodotti non sicuri o comunque siano al corrente di fatti o circostanze in base ai quali un operatore economico diligente avrebbe dovuto constatare la loro pericolosità e non agiscano prontamente per rimuoverli o disabilitarne l'accesso[142].

Va ricordato, peraltro, che la possibilità per i *marketplaces* di limitare, sospendere o cessare la fornitura dei servizi agli utenti commerciali in base alle loro politiche di moderazione e rimozione (come esplicitate nelle condizioni di servizio) deve soddisfare le prescrizioni del regolamento 2019/1150[143]. L'art. 4 di quest'ultimo prevede che le decisioni di limitazione o sospensione siano motivate in dettaglio preventivamente o al momento in cui hanno effetto, salvo casi particolari; che le decisioni di cessazione della fornitura, invece, vengano comunicate almeno 30 giorni prima, a meno che non si versi in situazioni specifiche; e che sia data agli utenti commerciali la possibilità di esporre le proprie ragioni nell'àmbito del processo interno di gestione dei reclami.

Il regime sin qui descritto è completato da un'iniziativa volontaria, denominata *Product Safety Pledge*[144], stipulata il 25 giugno 2018 sotto gli auspici della Commissione europea da quattro grandi intermediari che gestiscono *marketplaces online*, ai quali se ne sono aggiunti altri negli anni successivi[145]. In maniera non dissimile dai Memorandum che abbiamo già esaminato[146], vi si prevedono impegni riguardanti i prodotti non sicuri venduti *online* da terzi sui servizi dei firmatari che, in alcuni casi, vanno oltre quanto previsto nella legislazione vigente. E infatti, oltre all'impegno di intraprendere azioni appropriate nei confronti dei prodotti non sicuri, qualora identificabili (tra cui vengono menzionate le misure di rimozione o di blocco della vendita nel territorio UE), vi sono quelli di istituire un meccanismo interno di *notice-and-take-down* per i prodotti pericolosi; di reagire entro 2 giorni lavorativi alle richieste delle autorità nazionali per rimuovere gli annunci di prodotti non sicuri; di fornire una modalità trasparente per permettere ai

141 Comunicazione 2017/C 250/01, par. 5.2.
142 In altri termini, ci pare applicabile per analogia la sentenza *L'Oréal SA* e *a.* c. *eBay*.
143 Regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio, del 20 giugno 2019.
144 V. il *Product Safety Pledge*. *Voluntary commitment of online marketplaces with respect to the safety of non-food consumer products sold online by third party sellers*, , sul quale C. ULLRICH, *New Approach*, *cit.*, pp. 578-579, e A. BERTOLINI – F. EPISCOPO – N.-A. CHERCIU, *Liability*, *cit.*, pp. 61-62.
145 I primi quattro firmatari sono Alibaba, Amazon, eBay e Rakuten. Nel 2020 si sono aggiunti Allegro, Cdiscount, Wish.com, Bol.com, eMAG; nel 2021, Joom ed Etsy.
146 *Supra*, parr. 3.3 e 3.4.

consumatori di segnalare annunci di prodotti pericolosi (ai fini della loro eventuale rimozione); di introdurre, se appropriato, misure proattive per la rimozione di gruppi di prodotti vietati; di disporre misure contro i venditori "recidivi" di prodotti pericolosi; di adottare decisioni per prevenire la ricomparsa di annunci precedentemente rimossi; e, infine, di valutare la possibile introduzione di misure tecnologiche per migliorare l'individuazione *ex ante* dei prodotti non sicuri[147].

Infine, va ricordato che l'esigenza di assicurare coerenza tra il regime per i prodotti non armonizzati (disciplinato dalla direttiva 2001/95) e quello dei prodotti armonizzati (di cui al regolamento 2019/1020) ha indotto recentemente la Commissione a presentare una proposta di modifica della direttiva del 2001[148]. Essa ribadisce l'obbligo dei produttori di prendere le misure necessarie in presenza di prodotti non sicuri, incluso il ritiro degli stessi (art. 8, par. 10); analogo obbligo grava in capo ai distributori (art. 11, par. 4). Carattere di novità riveste, invece, la disposizione dell'art. 20 che, analogamente a quanto previsto nel regolamento 2019/1020 e sulla base dell'esperienza del *Product Safety Pledge* del 2018, stabilisce poteri e obblighi riguardanti i *marketplaces online*. Anzitutto, rileva il potere delle autorità nazionali di ordinare la rimozione dall'interfaccia *online* gli specifici contenuti illegali che si riferiscono a prodotti pericolosi, di disabilitarne l'accesso o di mostrare un avvertimento esplicito agli utenti finali, ordini che i *marketplaces* debbono eseguire prendendo tutte le misure necessarie agendo non oltre 2 giorni lavorativi dalla notifica (par. 2). Inoltre, i mercati *online* debbono tener conto delle informazioni periodiche sui prodotti pericolosi al fine di applicare misure proattive volontarie per individuare, identificare, rimuovere o disabilitare i contenuti illegali relativi a prodotti pericolosi offerti tramite i loro servizi (par. 3). I *marketplaces* debbono anche fornire risposta entro 5 giorni alle segnalazioni presentate da qualsiasi persona o ente[149] (par. 4). Infine, l'art. 26 della proposta in esame prevede che la Commissione possa attivarsi in proprio, anche con misure di rimozione o disabilitazione, qualora venga a conoscenza di prodotti che presentano un grave rischio per la salute e la sicurezza dei consumatori.

3.6. ***Segue*: i contenuti d'odio (*hate speech*)**

Un settore in cui la moderazione dei contenuti e l'adozione di misure di rimozione o disabilitazione si fa particolarmente sensibile è quello dei *contenuti d'odio (hate speech)*.

[147] I sinora cinque *Progress Report on the implementation of the Product Safety Pledge* sono reperibili *online*.
[148] Proposta del 30 giugno 2021, COM(2021)346 final, sulla quale N. ŠAJN, *General product safety regulation*, settembre 2021, e S. VETTORAZZI, *Updating the framework for the safety of non- food consumer products on the internal market*, ottobre 2021.
[149] Ciò viene espressamente coordinato con l'art. 14 proposta DSA, su cui *infra*, par. 4.

La nozione fa riferimento a tutte le manifestazioni del pensiero che diffondono, incitano, promuovono o giustificano l'odio razziale, la xenofobia, l'antisemitismo o altre forme di odio basate sull'intolleranza[150]. Rispetto ai contenuti d'odio, si pone la necessità di contemperare il diritto alla libertà di espressione[151] con il divieto di incitamento all'odio e alla discriminazione[152], nella consapevolezza che la prima libertà non può ammettere forme di espressione basate su odio e intolleranza. Il problema, com'è noto, si è fatto pressante negli ultimi anni per l'ampia diffusione di *hate speech* attraverso i *social network*[153].

Il regime normativo dell'UE in materia[154] è meno dettagliato di quelli relativi ad altri contenuti illegali prima esaminati, in specie dal punto di vista delle procedure applicabili. Ciò dipende, in parte, dal fatto che l'Unione non ha seguito né la strada "cyberliberalista" degli Stati Uniti[155] né quella "cyberpaternalista" di Paesi come la Cina[156], scegliendo invece quella potremmo dire "mista"[157] di confermare la regola dell'art. 14 direttiva *eCommerce* ma di affiancarla con misure di diritto penale (decisione quadro 2008/913/GAI)[158], con l'imposizione di obblighi a carico di determinati *providers* (direttiva 2010/13) e con misure volontarie.

---

150 Così la raccomandazione del Comitato dei ministri del Consiglio d'Europa, del 30 ottobre 1997, sull'*hate speech*, n. 97/20. In generale v. S. ASSIMAKOPOULOS – F. H. BAIDER – S. MILLAR (eds.), *Online Hate Speech in the European Union*, Cham, 2017; J. BAYER – P. BÁRD, *Hate speech and hate crime in the EU and the evaluation of online content regulation approaches*, luglio 2020; e A. A. SIEGEL, *Online Hate Speech*, in N. PERSILY – J. A. TUCKER (eds.), *Social Media and Democracy*, Cambridge, 2020, p. 56 ss.

151 Sancito, tra gli altri, dall'art. 19 della Dichiarazione universale dei diritti dell'uomo (DUDI), dall'art. 19 del Patto sui diritti civili e politici (Patto), dall'art. 10 della CEDU e dall'art. 11 della Carta di Nizza.

152 Si vedano, ad es., l'art. 7 DUDU, l'art. 4 della Convenzione sull'eliminazione di ogni forma di discriminazione razziale, l'art. 20 Patto e l'art. 21 Carta di Nizza. La CEDU, invece, non contiene una norma *ad hoc* ma la Corte EDU ha avuto modo di limitare il diritto alla libertà di espressione dell'art. 10 applicando altri articoli della Convenzione (tra cui l'art. 17 sull'abuso del diritto): in argomento, v. M. SPATTI, Hate speech *e negazionismo tra restrizioni alla libertà d'espressione e abuso del diritto*, in *Studi sull'integrazione europea*, 2014, p. 341 ss.; M. CASTELLANETA – P. DE SENA, *La libertà di espressione e le norme internazionali, ed europee, prese sul serio: sempre su CasaPound c. Facebook*, in *SIDIBlog*, 20.01.2020; E. NALIN, *Libertà di espressione tramite facebook e* hate speech, in *Sud in Europa*, febbraio 2020, p. 13 s.; A. KUCZERAWY, *Does Twitter trump Trump? A European perspective*, in *Verfassungsblog*, 29.01.2021. Sulla recente vicenda dei calciatori inglesi oggetto di *hate speech* in conseguenza della sconfitta nella finale degli Europei 2020 con l'Italia, v. T. DE SOUZA DIAS – S. THAPA, *Tackling Football-Related Online Hate Speech: The Role of International Human Rights Law*, in *EJIL:Talk!*, parti 1 e 2, 30.07.2021.

153 Cfr. F. ABBONDANTE, *Il ruolo dei social network nella lotta all'hate speech: un'analisi comparata fra l'esperienza statunitense e quella europea*, in *Informatica e diritto*, 2017, n. 1-2, p. 41 ss.

154 Su cui tra gli altri E. PSAILA e al., *The European legal framework on hate speech, blasphemy and its interaction with freedom of expression*, settembre 2015; P. FALLETTA – L. DI DONATO, *Il difficile equilibrio tra libertà di espressione e protezione della dignità umana sulla rete: il caso del c.d.* hate speech online, in P. PASSAGLIA – D. POLETTI (a cura di), *Nodi virtuali, legami informali: Internet alla ricerca di regole*, Pisa, 2017, p. 167 ss.; V. NARDI, *I discorsi d'odio nell'era digitale: quale ruolo per l'internet service provider?*, in *Diritto Penale Contemporaneo. Rivista trimestrale*, 2019, n. 2, p. 268 ss.; F. CASAROSA, *L'approccio normativo europeo verso il discorso dell'odio online: l'equilibrio fra un sistema di "enforcement" efficiente ed efficace e la tutela della libertà di espressione*, in *Questione giustizia*, 8.07.2020; e G. RUOTOLO, *Scritti*, *cit.*, p. 229 ss.

155 Dove viene data preminenza alla libertà di espressione garantita dal Primo emendamento alla Costituzione e alla libertà di impresa degli *hosting providers* su Internet.

156 In cui, al contrario, la legge impone penetranti obblighi in capo agli *hosting providers*, affinché a loro volta controllino le manifestazioni del pensiero degli utenti *online*.

157 Su questi tre possibili modelli, v. Y. WENGUANG, *Internet Intermediaries' Liability for Online Illegal Hate Speech*, in *Frontiers of Law in China*, 2018, p. 342 ss.

158 Decisione quadro 2008/913/GAI del Consiglio, del 28 novembre 2008.

La normativa di riferimento è data dalla decisione quadro 2008/913/GAI sulla lotta contro alcune forme ed espressioni di razzismo e xenofobia attraverso il diritto penale[159]. Essa non fornisce una definizione di razzismo e xenofobia, limitandosi a stabilire l'obbligo per gli Stati di prendere le misure necessarie per punire i comportamenti indicati nell'art. 1. Tra questi, rilevano "l'istigazione 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" (lett. a) e "la perpetrazione di uno degli atti di cui alla lettera a) mediante la diffusione e la distribuzione pubblica di scritti, immagini o altro materiale" (lett. b). Quanto alle misure per contrastare i predetti comportamenti, l'art. 3 stabilisce l'obbligo di introdurre negli ordinamenti interni sanzioni penali efficaci, proporzionate e dissuasive che prevedano la reclusione per una durata massima da uno e tre anni[160].

Disposizioni specifiche si ritrovano, poi, nella più volte citata direttiva 2010/13 sui servizi di media audiovisivi, come modificata dalla direttiva 2018/1808[161]. L'art. 28-*ter* chiede agli Stati membri di assicurarsi che i fornitori di piattaforme per la condivisione di video prendano misure adeguate per tutelare il grande pubblico da programmi, video generati dagli utenti e comunicazioni commerciali audiovisive che, da un lato, istighino alla violenza o all'odio nei confronti di un gruppo di persone o un membro di un gruppo per motivi discriminatori (par. 1, lett. b)[162] e, dall'altro, includano contenuti la cui diffusione costituisce reato di stampo razzista o xenofobo ai sensi della decisione quadro 2008/913 (lett. c). Gli Stati restano comunque liberi di imporre misure più dettagliate o rigorose rispetto a quelle ritenute adeguate dal par. 3 (par. 6). Tutte le misure, però, devono rispettare le regole della norma in commento senza violare il divieto di imposizione di obblighi generali di sorveglianza attiva e la regola dell'esonero dalla responsabilità indiretta per quei fornitori (artt. 28-*bis*, par. 5, e 28-*ter*, par. 6).

Come si può notare, la diffusione degli *hate speech* nell'ambiente *online* non è disciplinata in quanto tale né dalla decisione quadro 2008/913 né dalla direttiva 2010/13. Se, dunque, le disposizioni prima esaminate non aggiungono nulla in termini di presentazione delle segnalazioni, di speditezza delle operazioni di rimozione ordinate dalle autorità nazionali e di garanzie per interessati e controinteressati, si ritiene che le attività di moderazione e rimozione/disabilitazione dei contenuti d'odio seguano le regole generali. In proposito si ricorda che, proprio con riferimento a un contenuto d'odio (e diffamatorio), nella sentenza

[159] Su cui T. M. MOSCHETTA, *La decisione quadro 2008/913/Gai contro il razzismo e la xenofobia: una «occasione persa» per l'Italia?*, in *Rivista di Diritto dell'Economia, dei Trasporti e dell'Ambiente*, 2014, p. 21 ss.

[160] La sentenza della Corte EDU del 2 settembre 2021, *Sanchez* c. *Francia*, ECLI:CE:ECHR:2021:0902JUD004558115, ha peraltro confermato la compatibilità con l'art. 10 CEDU di sanzioni pecuniarie a carico di individui che non cancellano tempestivamente i commenti d'odio pubblicati da altri sulle loro bacheche Facebook.

[161] *Supra*, parr. 3.1 e 3.2.

[162] La norma richiama l'art. 21 della Carta di Nizza, che stabilisce il divieto di discriminazione fondata sul sesso, la razza, il colore della pelle o l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, il patrimonio, la nascita, la disabilità, l'età o l'orientamento sessuale.

Glawischnig-Piesczek l'àmbito di applicazione delle misure di rimozione è stato esteso non solo ai contenuti identici ma anche a quelli equivalenti a contenuti precedentemente rimossi[163].

L'assenza di una disciplina specifica per gli *online hate speech* è solo in parte colmata dalle misure volontarie concordate con i principali *providers*. Nel 2016, la Commissione ha adottato un *Codice di condotta per contrastare l'illecito incitamento all'odio online*[164], sottoscritto volontariamente da alcune piattaforme *online*[165]. Nel Codice, i firmatari si sono tra l'altro impegnati a istituire procedure trasparenti ed efficaci per esaminare le segnalazioni; a chiarire agli utenti che sono vietati la promozione dell'istigazione alla violenza e a comportamenti improntati all'odio; a esaminare, alla luce delle norme nazionali e delle proprie *community rules*, la maggior parte delle segnalazioni in meno di 24 ore e, nel caso, a procedere alla rimozione o disabilitazione; a migliorare la cooperazione con le autorità nazionali, con gli esperti e con i segnalatori attendibili; e ad avviare azioni di educazione e sensibilizzazione sui contenuti non autorizzati e sulla lotta contro i discorsi di incitamento all'odio.

Nonostante la sua efficacia[166], il Codice non è esente da aspetti problematici. A parte il fatto di scontare i limiti tipici di uno strumento volontario, esso ha spinto le piattaforme a incrementare l'uso di strumenti automatizzati che, però, non riescono sempre a distinguere tra veri discorsi d'odio e legittime manifestazioni del pensiero[167]. Inoltre, la mancanza di riferimenti alla possibilità di ricorrere a mezzi stragiudiziali di risoluzione delle controversie lascia gli utenti la sola facoltà di rivolgersi ai sistemi di revisione istituiti dalle piattaforme, qualora esistenti, oltre che ovviamente ai giudici nazionali.

Proprio in materia di discorsi d'odio, si sono avute le prime decisioni del *Facebook Oversight Board* (FOB), organo di autoregolamentazione che dovrebbe assicurare un controllo ulteriore e indipendente sulle attività di rimozione e blocco degli *account* effettuate dal *social network* per violazioni delle proprie condizioni di servizio. Il 28 gennaio 2021, il FOB ha pubblicato le prime sei decisioni, affermando in quattro di esse che i contenuti rimossi perché ritenuti *hate speech* avrebbero dovuto ricevere una valutazione differente[168]. Si segnala anche la decisione del 5 maggio 2021 sulla precedente sospensione

---

163 *Supra*, nota 44 e testo corrispondente.

164 *Code of Conduct on Countering Illegal Hate Speech Online*, del 31 maggio 2016. Cfr. K. PODSTAWA, *Hybrid Governance or... Nothing? The EU Code of Conduct on Combatting Illegal Hate Speech Online*, in E. CARPANELLI – N. LAZZERINI (eds.), *Use and Misuse of New Technologies*, Cham, 2019, p. 167 ss.; G. CALIMÀ, *Il Codice di Condotta dell'Unione Europea contro l'incitamento all'odio online*, in *Ius in itinere*, 21.09.2020; e F. CASAROSA, *L'approccio*, *cit.*

165 Sinora hanno firmato Facebook, Google, Microsoft, Twitter, Instagram, Google+, Snapchat, Dailymotion, Jeuxvideo.com e ByteDance (TikTok).

166 Secondo la *6th Evaluation of the Code of Conduct*, 7.10.2021, le compagnie firmatarie hanno valutato l'81% delle segnalazioni entro 24 ore e rimosso il 62,5% dei contenuti segnalati. Il dato è però inferiore alla media registrata nel 2019-2020.

167 Cfr. F. CASAROSA, *When the Algorithm Is Not Fully Reliable. The Collaboration between Technology and Humans in the Fight against Hate Speech*, in H.-W. MICKLITZ – O. POLLICINO – A. REICHMAN – A. SIMONCINI – G. SARTOR – G. DE GREGORIO (eds), *Constitutional Challenges in the Algorithmic Society*, Cambridge, 2022, p. 298 ss.

168 Vedi D. GHOSH – J. HENDRIX, *Facebook's Oversight Board Takes on the Curious Case of Donald J. Trump*, in *Verfassungsblog*, 29.01.2021; A. IANNOTTI DELLA VALLE, *La giurisdizione privata nel mondo digitale al tempo della crisi della*

dal *social network* dell'ex Presidente degli Stati Uniti Trump, ritenuta sproporzionata perché a tempo indeterminato[169].

Merita, da ultimo, sottolineare che la necessità di conseguire una maggiore armonizzazione delle normative nazionali è alla base dell'intenzione della Commissione[170] di presentare entro la fine del 2021 un'iniziativa legislativa per includere nell'elenco dell'art. 83, par. 1, TFUE tutte le forme di reati generati dall'odio e di incitamento all'odio in modo da avanzare, in un secondo momento, una proposta per l'armonizzazione della definizione e delle sanzioni relative ai discorsi e ai crimini d'odio[171].

3.7. *Segue*: la specifica problematica dei contenuti disinformativi

Il quadro normativo dell'UE si fa scarno con riferimento alla moderazione e alla rimozione o disabilitazione dei *contenuti disinformativi*[172].

Nella comunicazione del 2018, la disinformazione è definita "un'informazione rivelatasi falsa o fuorviante concepita, presentata e diffusa a scopo di lucro o per ingannare intenzionalmente il pubblico, e che può arrecare un pregiudizio pubblico"[173]. Il pregiudizio pubblico, in specie, comprende le minacce ai processi politici democratici, ai processi di elaborazione delle politiche e ai beni pubblici (tutela della salute dei cittadini, dell'ambiente e della sicurezza dell'Unione). Così definita, la disinformazione va distinta da altri fenomeni simili, quali la cattiva informazione (o *misinformation*, ove i contenuti falsi o fuorvianti, seppur dannosi, vengono diffusi senza intenzione fraudolenta), le operazioni di influenza delle informazioni (in genere attuate da soggetti nazionali o esteri per influenzare il pubblico con una serie di mezzi

*sovranità: il "modello" dell'*Oversight Board *di Facebook*, in *Federalismi.it*, 26/2021, p. 144 ss.; J. MONTERO REGULES, *The Facebook Oversight Board and 'Context': Analyzing the first decisions on hate speech*, in *Verfassungsblog*, 16.02.2021; e O. POLLICINO – G. DE GREGORIO, *Shedding Light on the Darkness of Content Moderation: The First Decisions of the Facebook Oversight Board*, *ivi*, 5.02.2021.

169 Cfr. M. MILANOVIC, *The Facebook Oversight Board Made the Right Call on the Trump Suspension*, in *EJIL:Talk!*, 6.05.2021, e O. POLLICINO – G. DE GREGORIO – M. BASSINI, *Trump's Indefinite Ban: Shifting the Facebook Oversight Board away from the First Amendment Doctrine*, in *Verfassungsblog*, 11.05.2021.

170 Comunicazione COM(2020)690 final.

171 Risposta all'interrogazione scritta del 27 maggio 2021, E-001327/2021.

172 Sui quali v. in generale A. M. GUESS – B. A. LYONS, *Misinformation, Disinformation, and Online Propaganda*, in N. PERSILY – J. A. TUCKER (eds.), *Social*, *cit.*, p. 10 ss.; G. PITRUZZELLA – O. POLLICINO, *Disinformation and Hate Speech - A European Constitutional Perspective*, Milano, 2020, spec. p. 97 ss.; e G. CAGGIANO, *Il contrasto alla disinformazione tra nuovi obblighi delle piattaforme online e tutela dei diritti fondamentali nel quadro del Digital Service Act e della co-regolamentazione*, in *Papers di diritto europeo - Riflessioni e ricerche*, 2021, n. 1, pp. 45 ss.

173 Comunicazione della Commissione del 26 aprile 2018, Contrastare la disinformazione online: un approccio europeo, COM(2018)236 final, p. 4. Una definizione più sintetica la si ritrova nella comunicazione del 3 dicembre 2020 sul piano d'azione per la democrazia europea, COM(2020)790 final, p. 20.

ingannevoli)[174] e le vere e proprie ingerenze straniere (misure coercitive e ingannevoli poste in essere da soggetti statali stranieri al fine di ostacolare la libertà di informazione e di espressione degli individui)[175].

Va subito detto che i contenuti disinformativi *online*, di per sé, non sono illegali. Tenendo a mente la definizione accolta nella proposta DSA[176], infatti, la disinformazione non rientra di per sé tra le informazioni illegali in base alla normativa UE o degli Stati membri. Anche il Piano d'azione contro la disinformazione del 2018 riconosce che le azioni di contrasto in materia "riguardano esclusivamente i contenuti di disinformazione *che sono legali a norma del diritto dell'Unione o nazionale*"[177], non essendo sovrapponibili ad altri contenuti – questi sì illegali – come quelli diffamatori, d'odio, di incitamento alla violenza, ecc.[178].

Ciò dipende dal fatto che il confine tra libertà di espressione, cattiva informazione e disinformazione è sottile e che, al di fuori di un quadro regolatorio comune, c'è il rischio che si giunga alla compressione ingiustificata della prima libertà[179]. Eppure, la presenza di quei contenuti *online* pone un problema di moderazione e rimozione (o disabilitazione), vista la loro elevata capacità di trarre in inganno un pubblico numeroso e arrecare seri pregiudizi alla collettività[180]. Si pensi alla disinformazione sui processi elettorali che, grazie all'utilizzo delle nuove tecnologie[181], giunge alla manipolazione intenzionale del discorso politico sui *social network* (anche con la creazione di *deepfakes*)[182]: essa, pur se non sempre originata da campagne di influenza o ingerenza straniere, è idonea a pregiudicare la qualità del dibattito pubblico soprattutto in periodo preelettorale con chiari rischi per la tutela dello stato di diritto, della democrazia e

---

174 Ad es. attraverso la soppressione delle fonti di informazione indipendenti, spesso in combinazione con la disinformazione.

175 COM(2020)790 final, p. 20. Sulle influenze e ingerenze straniere v. E. BRESSANELLI e al., *Institutions and foreign interferences*, giugno 2020, ed E. BRESSANELLI, *Investing in destabilisation: How foreign money is used to undermine democracy in the EU*, aprile 2021.

176 *Supra*, nota 3 e testo corrispondente.

177 Comunicazione congiunta della Commissione e dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, del 5 dicembre 2018, JOIN(2018)36 final, p. 1 (corsivo nostro).

178 V. anche il rapporto dal titolo *A multi-dimensional approach to disinformation*, marzo 2018, p. 10.

179 V. ad es. la sentenza della Corte EDU del 25 luglio 2019, *Brzeziński* c. *Polonia*, ECLI:CE:ECHR:2019:0725JUD004754207, in cui è stata riscontrata la violazione dell'art. 10 CEDU sulla libertà di espressione nei confronti dello Stato polacco, i cui giudici avevano censurato (perché ritenuti disinformativi) i commenti fatti dal ricorrente, candidato sindaco, in un volantino diffuso nella comunità locale prima delle elezioni. Sulla possibilità di utilizzare l'art. 17 CEDU quale limite della libertà di espressione nei casi di disinformazione v. E. SHATTOCK, *Should the ECtHR Invoke Article 17 for Disinformation Cases?*, in *EJIL:Talk!*, 26.03.2021.

180 Cfr. M. MONTI, *Le "bufale"* online *e l'inquinamento del* public discourse, in P. PASSAGLIA – D. POLETTI (a cura di), *Nodi virtuali*, *cit.*, p. 179 ss. V. anche *Disinformation and freedom of opinion and expression*, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, 13.04.2021, doc. A/HRC/47/25.

181 Cfr. L. M. NEUDERT – N. MARCHAL, *Polarisation and the use of technology in political campaigns and communication*, marzo 2019.

182 Si tratta di contenuti foto, audio e video falsi, creati tramite le nuove tecnologie di intelligenza artificiale, economiche e facili da utilizzare. Vedi T. KIRCHENGAST, *Deepfakes and image manipulation: criminalisation and control*, in *Information & Communications Technology Law*, 2020, p. 308 ss., e M. VAN HUIJSTEE e al., *Tackling deepfakes in European policy*, luglio 2021.

dei diritti fondamentali dei soggetti coinvolti[183]. Ma si pensi anche alla c.d. "infodemia" da coronavirus, che fa riferimento alla sovrabbondanza di contenuti informativi su siti web e *social network* sulle cause e conseguenze della pandemia, tra i quali è difficile discernere quelli veri, quelli inaccurati, quelli disinformativi e quelli creati da campagne straniere[184]. Si ricordano anche le campagne di disinformazione contro i migranti e altre minoranze[185] e contro le persone LGBTI+[186].

In questo quadro, si comprende il ruolo-chiave dei media[187] e dei *social network*, atteso che in specie i servizi di questi ultimi fungono sempre più da cassa di risonanza e strumento di rapida diffusione delle informazioni (buone o cattive) a livello mondiale[188]. Il problema non consiste solo nella capacità tecnica di svolgere o meno la moderazione in maniera rigorosa, ma coinvolge il modello di *business* delle piattaforme *social*. Secondo una recente relazione speciale della Corte dei conti europea, la disinformazione *online* deriva in gran parte dal fatto che le informazioni false condivise dagli utenti sono considerate prioritarie e quindi messe in primo piano dagli algoritmi di visualizzazione, che dànno evidenza ai contenuti personalizzati e popolari perché maggiormente in grado di attrarre l'attenzione degli utenti[189]. Quanto ciò sia vero, del resto, è stato messo bene in luce dallo scandalo dei *Facebook Files*.

Parallelamente a quanto sta avvenendo negli Stati Uniti[190], dunque, l'azione UE di contrasto alla disinformazione si è fatta più intensa negli ultimi tempi[191]. In risposta alle conclusioni del Consiglio

183 Vedi J. SYROVÁTKA, *In Scrooge's boots: Lessons learned on disinformation from the 2019 European elections*, in *European View*, 2019, p. 203 ss.; J. BAYER e al., *Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States - 2021 update*, aprile 2021; e C. COLOMINA – H. SÁNCHEZ MARGALEF – R. YOUNGS, *The impact of disinformation on democratic processes and human rights in the world*, aprile 2021. Sulle possibili azioni contro la disinformazione intesa quale "minaccia ibrida" v. L. LONARDO, *EU Law Against Hybrid Threats: A First Assessment*, in *European Papers*, 2021, p. 1075 ss., spec. pp. 1078-1081.

184 Cfr. N. BENTZEN, *COVID-19 foreign influence campaigns - Europe and the global battle of narratives*, aprile 2020; N. BENTZEN – T. SMITH, *Countering the health 'infodemic'*, aprile 2020; ID., *The EU's response to the coronavirus 'infodemic'*, giugno 2020; S. L. VÉRITER – C. BJOLAB – J. A. KOOPS, *Tackling COVID-19 Disinformation: Internal and External Challenges for the European Union*, in *The Hague Journal of Diplomacy*, 2020, p. 569 ss.; ed É. BASSOT e al., *Towards a more resilient Europe post-coronavirus - Options to enhance the EU's resilience to structural risks*, aprile 2021, p. 121 ss.

185 Vedi J. SZAKÁCS – É. BOGNÁR, *The impact of disinformation campaigns about migrants and minority groups in the EU*, giugno 2021.

186 Cfr. C. STRAND – J. SVENSSON, *Disinformation campaigns about LGBTI+ people in the EU and foreign influence*, luglio 2021.

187 Su cui v. H. TUMBER – S. WAISBORD (eds.), *The Routledge Companion to Media Disinformation and Populism*, London-New York, 2021.

188 *Amplius* K. SHU – S. WANG – D. LEE – H. LIU (eds.), *Disinformation, Misinformation, and Fake News in Social Media. Emerging Research Challenges and Opportunities*, Cham, 2020.

189 Relazione speciale della Corte dei conti, *La disinformazione nell'UE: combattuta ma non vinta*, 9/2021, p. 33. Così già COM(2018)236, pp. 5-6.

190 Dove la c.d. "rivolta di Capitol Hill" del 6 gennaio 2021 ha provocato un sostegno bipartisan alla riforma della *Section 230* del *Communications Act* del 1934 (come modificato nel 1996) sull'immunità delle piattaforme web dalla responsabilità per i contenuti di terzi: per alcuni cenni v. N. BENTZEN – T. KRAUSE, *Regulation of the digital sector*, luglio 2021.

191 Cfr. N. BENTZEN, *Online disinformation and the EU's response*, febbraio 2019.

europeo del 19-20 marzo 2015[192], poi ribadite e approfondite[193], sono state adottate alcune comunicazioni da parte della Commissione, anche congiuntamente con l'Alto rappresentante per gli affari esteri e la politica di sicurezza[194], in cui si evidenziano i rischi strategici per l'UE e i suoi Stati membri derivanti dalla diffusione *online* dei contenuti disinformativi. In funzione di contrasto soprattutto alle campagne di disinformazione della Federazione russa, nel settembre 2015 è stata creata la task force *East StratCom* del Servizio europeo per l'azione esterna[195], mentre nel 2018 è stata prevista l'istituzione di un sistema di allarme rapido tra gli Stati e le istituzioni dell'UE al fine di assicurare risposte comuni alla disinformazione attraverso la condivisione delle informazioni e le tempestive segnalazioni sulle campagne di disinformazione[196].

Anche il Parlamento europeo, in alcune sue risoluzioni, ha avuto modo di evidenziare la pericolosità dei contenuti disinformativi[197], al punto di costituire nell'attuale legislatura una "Commissione speciale sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, inclusa la disinformazione"[198].

Tutto ciò non ha, però, sinora portato all'adozione di norme vincolanti in materia. Le piattaforme continuano, dunque, ad avere un potere pressoché assoluto nel decidere, in base alle loro condizioni di servizio, cosa è disinformazione e cosa non lo è. Ne deriva non solo una disciplina assai frammentata tra le diverse piattaforme ma soprattutto la possibilità che, all'esito di attività di moderazione non regolamentate, vengano rimossi contenuti non disinformativi (e cancellati specifici *account*) oppure, al contrario, che non si proceda alla rimozione di quelli chiaramente ingannevoli, spesso in base all'applicazione di algoritmi automatizzati senza successiva verifica umana e senza che gli utenti ricevano una motivazione e/o dispongano di efficaci mezzi di ricorso oltre quelli interni, ove previsti[199].

---

192 Doc. EUCO 11/15, par. 13.

193 V. ad es. le conclusioni del 28 giugno 2018, doc. EUCO 9/18, par. 13, e del 18 ottobre 2018, doc. EUCO 13/18, par. 9.

194 Cfr. la comunicazione congiunta del 6 aprile 2016, Quadro congiunto per contrastare le minacce ibride - La risposta dell'Unione europea, JOIN(2016)18 final; la citata comunicazione sul contrasto alla disinformazione online, COM(2018)236 final; il citato piano d'azione contro la disinformazione, JOIN(2018)36 final; la comunicazione congiunta del 10 giugno 2020, Contrastare la disinformazione sulla Covid-19 - Guardare ai fatti, JOIN(2020)8 final; e il piano d'azione per la democrazia europea, COM(2020)790 final. Su alcuni di questi documenti v. M. LASTILLA, *Il virus della disinformazione online nell'UE*, in *Sud in Europa*, dicembre 2020, p. 17 s.

195 Il progetto di punta della task force è *EUvsDisinfo*, istituito per prevedere, affrontare e rispondere meglio alle campagne di disinformazione della Russia dirette verso l'UE, i suoi Stati membri e i Paesi confinanti.

196 Comunicazione JOIN(2018)36, p. 7 ss.

197 Tra le altre, si vedano le risoluzioni del 23 novembre 2016, Comunicazione strategica dell'Unione europea per contrastare la propaganda contro di essa a opera di terzi, P8_TA(2016)0441; del 13 marzo 2019, Seguito dato dal SEAE a due anni dalla relazione del PE sulla comunicazione strategica dell'UE per contrastare la propaganda nei suoi confronti da parte di terzi, P8_TA(2019)0187; e del 20 ottobre 2020, Atto sui servizi digitali e questioni sollevate in materia di diritti fondamentali, P9_TA(2020)0274, spec. parr. E, F, G, H, 6, 7 e 34.

198 Decisione del Parlamento europeo del 18 giugno 2020, P9_TA(2020)0161.

199 Conforme G. CAGGIANO, *Il contrasto*, *cit.*, p. 53. V. anche C. MARSDEN – T. MEYER, *Regulating disinformation with artificial intelligence*, marzo 2019., e P. M. BARRETT, *Who Moderates the Social Media Giants?*, NYU Stern Center for Business and Human Rights, New York, 2020.

Si assiste, quindi, a una sempre più marcata "privatizzazione della censura"[200] cui non si è riusciti a porre rimedio con l'adozione del *Codice di buone pratiche dell'UE sulla disinformazione* del 20 settembre 2018[201], strumento di co-regolamentazione firmato dalla Commissione, da alcune piattaforme (Facebook, Google, Microsoft, Mozilla, Twitter, ByteDance-TikTok) e da associazioni del settore. Nel Codice, i firmatari si sono limitati a riconoscere l'importanza di aumentare gli sforzi per chiudere i profili falsi e garantire l'integrità dei servizi riguardo ai profili il cui scopo e intento consistono nel diffondere la disinformazione (par. I, numeri v) e vi), senza però prendere impegni precisi. Anzi, si prevede che nessuno dovrebbe essere obbligato a cancellare o inibire l'accesso a contenuti o messaggi leciti per il solo fatto che siano ritenuti falsi, né ad adottare politiche volontarie in tal direzione (n. vii)[202], così rendendo palese – e forse addirittura rafforzando – la tendenza alla privatizzazione della censura di cui si parlava prima. Gli unici impegni, caratterizzati spesso dal compimento di meri "sforzi ragionevoli", riguardano il vaglio delle inserzioni pubblicitarie (par. II.A)[203], la presentazione trasparente di messaggi pubblicitari politici e campagne di sensibilizzazione (par. II.B)[204], un maggiore controllo dell'integrità dei servizi quanto all'uso di sistemi automatizzati ("bot") di diffusione delle notizie (par. II.C) e una maggiore responsabilizzazione dei consumatori (par. II.D) e della comunità dei ricercatori (par. II.E).

Non è quindi un caso, quindi, che la Commissione abbia recentemente rilevato la necessità di procedere al rafforzamento del Codice[205]. Pur riconoscendo che esso rappresenta un risultato unico nel suo genere, si sottolinea la persistenza di lacune in termini di qualità delle segnalazioni, di indicatori di prestazione, di valutazione indipendente, di mancanza di una copertura sufficiente per quanto riguarda la verifica dei fatti e di "monetizzazione della disinformazione" attraverso le inserzioni pubblicitarie[206]. Così, si propone di rafforzare il Codice prevedendo impegni più rigorosi, specifici e mirati, ampliando il suo àmbito di applicazione, incoraggiando la più ampia partecipazione e cooperando più intensamente con l'Osservatorio europeo dei media digitali (EDMO) e il citato sistema di allarme rapido[207].

---

[200] *Amplius* M. MONTI, *La disinformazione online, la crisi del rapporto pubblico-esperti e il rischio della privatizzazione della censura nelle azioni dell'Unione Europea* (Code of practice on disinformation), in *Federalismi.it*, n. 11/2020, p. 282 ss. V. anche M. BASSINI, *Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione*, in *Media Laws*, 2021, n. 1, p. 67 ss.

[201] Reperibile *online*.

[202] Su questo Codice v. M. MONTI, *Il* Code of Practice on Disinformation *dell'UE: tentativi* in fieri *di contrasto alle* fake news, in *Media Laws*, 2019, n. 1, p. 320 ss.; G. PAGANO, *Il Code of Practice on Disinformation. Note sulla natura giuridica di un atto misto di autoregolazione*, in *Federalismi.it*, n. 11/2019; M. MONTI, *La disinformazione*, *cit.*; e G. CAGGIANO, *Il contrasto*, *cit.*, p. 60 ss.

[203] Allo scopo di ridurre il profitto dei vettori della disinformazione, nei casi in cui essi si muovano per ragioni economiche.

[204] In modo che risulti chiaro agli utenti che non si tratta di contenuti editoriali.

[205] Comunicazione del 26 maggio 2021, Orientamenti della Commissione europea sul rafforzamento del codice di buone pratiche sulla disinformazione, COM(2021)262 final. V. anche il comunicato stampa dell'1.10.2021, IP/21/4945.

[206] COM(2021)262, pp. 4-5.

[207] Previsto nella comunicazione JOIN(2018)36.

4.1. Le disposizioni della proposta di *Digital Services Act*

È nell'ampio quadro sin qui decritto che si inserisce la proposta di regolamento *Digital Services Act*[208], pubblicata il 15 dicembre 2020 dopo un periodo di consultazione pubblica, numerosi contributi da ambienti accademici e soggetti interessati[209], nonché tre risoluzioni del Parlamento europeo[210].

La proposta mantiene i capisaldi della direttiva *eCommerce* e ne approfondisce alcuni aspetti, facendo propria l'esperienza maturata nell'applicazione degli strumenti prima esaminati e stabilendo obblighi di diligenza "a cerchi concentrici", che cioè si fanno più intensi all'aumentare del tipo di attività e dimensione degli ISP, oltre che prevedendo un articolato sistema di controllo da parte delle autorità nazionali e della Commissione. Così facendo, la proposta di regolamento segna, già dalla scelta del tipo di atto, un deciso passaggio dal *lasseiz-faire* della direttiva *eCommerce* – seppur "messo in crisi" da alcuni degli interventi normativi e giurisprudenziali prima esaminati – a un sistema maggiormente regolamentato (e co-regolamentato) ove soprattutto le piattaforme *online* di grandi dimensioni saranno interessate da obblighi più stringenti di quelli attuali. Tuttavia, la proposta lascia irrisolta tutta una serie di problemi, a cominciare dalla mancata disciplina di alcuni servizi digitali difficilmente riconducibili alle tre tradizionali categorie dei *mere conduit*, dei *caching* e degli *hosting providers*[211].

---

[208] Su cui in generale G. M. RUOTOLO, *Le proposte di disciplina di* digital services *e* digital markets *della Commissione del 15 dicembre 2020*, in *DPCE on line*, 2020, p. 5419 ss.; L. WOODS, *Overview of Digital Services Act*, in *EU Law Analysis*, 16.12.2020; BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS, *The Digital Services Act Proposal - BEUC position paper*, 2021; G. CAGGIANO, *La proposta*, *cit.*; G. DE GREGORIO, *The Digital Services Act: A Paradigmatic Example of European Digital Constitutionalism*, in *Diritti comparati*, 17.05.2021; G. DE GREGORIO – O. POLLICINO, *The European Constitutional Road to Address Platform Power*, in *Verfassungsblog*, 31.8.2021; M. EIFERT – A. METZGER – H. SCHWEITZER – G. WAGNER, *Taming the giants: The DMA/DSA package*, in *Common Market Law Review*, 2021, p. 987 ss.; F. ERIXON, *"Too Big to Care" or "Too Big to Share": The Digital Services Act and the Consequences of Reforming Intermediary Liability Rules*, ECIPE Policy Brief n. 5/2021; V. GOLUNOVA, *The Digital Services Act and freedom of expression: triumph or failure?*, 8.03.2021; A. SAVIN, *The EU Digital Services Act: Towards a More Responsible Internet*, Copenhagen Business School Law Research Paper Series No. 21-04; e i diversi contributi in G. CAGGIANO – G. CONTALDI – P. MANZINI (a cura di), *Verso una legislazione*, *cit.*

[209] La consultazione si è svolta dal 2 giugno all'8 settembre 2020. Tra le riflessioni che hanno preceduto la proposta, v. L. BELLULO, *Reflections in the Perspective of the European Digital Services Act*, marzo 2020; EUROPEAN DIGITAL SME ALLIANCE, *Position paper on the Digital Services Act (DSA)*, 8.09.2020; N. LOMBA – T. EVAS, *Digital services act*, *cit.*; T. MADIEGA, *Reform of the EU liability regime for online intermediaries - Background on the forthcoming digital services act*, maggio 2020; J. B. NORDEMANN, *The functioning of the Internal Market for Digital Services: responsibilities and duties of care of providers of Digital Services - Challenges and opportunities*, maggio 2020; A. PONCE DEL CASTILLO, *The digital services act package: Reflections on the EU Commission's policy options*, ETUI Policy Brief n. 12/2020; e R. WINGFIELD, *The Digital Services Act and Online Content Regulation: A Slippery Slope for Human Rights?*, in *The GNI Blog*, 15.07.2020.

[210] Risoluzioni del 20 ottobre 2020 recante raccomandazioni alla Commissione sulla legge sui servizi digitali: migliorare il funzionamento del mercato unico, P9_TA(2020)0272; recante raccomandazioni alla Commissione sulla legge sui servizi digitali: adeguare le norme di diritto commerciale e civile per i soggetti commerciali che operano online, P9_TA(2020)0273; e la citata P9_TA(2020)0274.

[211] Su questo e altri profili, qui non affrontabili, v. L. WIEWIORRA – I. GODLOVITCH (eds.), *The Digital Services Act and the Digital Markets Act: A forward-looking and consumer-centred perspective*, 26.05.2021, spec. i contributi di J. VAN HOBOKEN (p. 10 s.), T. RODRIGUEZ DE LAS HERAS BALLELL (p. 11 s.) e D. KELLER (p. 12 s.). V. anche R. JANAL, *Adapting*, *cit.*

Tra le principali questioni affrontate nella proposta DSA vi sono quelle della moderazione e della rimozione dei (o disabilitazione dell'accesso ai) contenuti illegali. Sono questioni che, nell'ottica della proposta, si ricollegano funzionalmente alla disciplina della responsabilità dei prestatori intermediari e tengono conto degli sviluppi tecnologici e dei nuovi modelli di *business* dei servizi digitali, al fine di stabilire alcuni obblighi di diligenza e così rafforzare le garanzie per gli individui coinvolti e la società nel suo complesso[212].

Come si è già detto, l'art. 2, lett. g), della proposta contiene una definizione di "contenuto illegale", inteso come "qualsiasi informazione che, di per sé o in relazione ad un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme alle disposizioni normative dell'Unione o di uno Stato membro, indipendentemente dalla natura o dall'oggetto specifico di tali disposizioni". A questa definizione si ricollega quella di "moderazione dei contenuti" (lett. p), attività che consiste nell'individuazione, identificazione e contrasto ai contenuti illegali e alle informazioni contrarie alle *community rules* diffusi dagli utenti: essa può sfociare sia nell'adozione di misure relative alla disponibilità, visibilità e accessibilità di contenuti o informazioni (rimozione e disabilitazione), sia nella capacità degli utenti di renderle disponibili (cessazione e sospensione degli *account*).

La proposta DSA non modifica le regole di base della direttiva *eCommerce* (art. 1, par. 5, lett. a). Gli artt. 3, 4 e 5, infatti, riproducono in maniera pressoché integrale gli artt. 12, 13 e 14[213] sull'esonero dalla responsabilità indiretta di *mere conduit*, *caching* e *hosting providers*[214], incluso l'onere di rimozione o disabilitazione. Rimane inoltre invariata, all'art. 7, la regola dell'assenza di obblighi generali di sorveglianza o di accertamento attivo dei fatti di cui già all'art. 15, par. 1, direttiva *eCommerce*[215]. La Commissione ha quindi deciso di non applicare il più stringente regime previsto per i prestatori di servizi di *streaming* audio-video (art. 17 direttiva 2019/790), permettendo alla generalità degli ISP di mantenere quello più favorevole della direttiva *eCommerce*[216].

Parimenti, la proposta DSA non incide sulle norme concernenti alcuni dei contenuti specifici prima esaminati, considerate *leges speciales*. Sono fatte esplicitamente salve le norme sulla rimozione dei contenuti terroristici di cui al regolamento 2021/784 (art. 1, par. 5, lett. d); il regolamento 2021/1232 sulla deroga

[212] V. anche G. CAGGIANO, *La proposta*, *cit.*, p. 4.
[213] Articoli che vengono di conseguenza soppressi (art. 71).
[214] A proposito di questi ultimi prestatori, l'art. 5 specifica che l'esonero dalla responsabilità indiretta non opera in tema di contratti conclusi dai consumatori, qualora la piattaforma *online* induca un consumatore medio e ragionevolmente informato a ritenere che le informazioni, o il prodotto o il servizio oggetto delle operazioni siano forniti dalla piattaforma stessa o da un destinatario del servizio che agisce sotto la sua autorità o il suo controllo (cioè, quando la piattaforma di cui si tratta non si palesi come un autentico *hosting provider*).
[215] Anche quest'ultimo viene soppresso dall'art. 71.
[216] Sull'opportunità di questa scelta v. M. EIFERT – A. METZGER – H. SCHWEITZER – G. WAGNER, *Taming*, *cit.*, p. 1005 ss.

temporanea della direttiva *ePrivacy* per contrastare i contenuti pedopornografici (lett. i)[217]; la direttiva 2010/13 sul divieto di contenuti terroristici, pedopornografici e di *hate speech* sulle piattaforme di condivisione di video (lett. b); le norme in materia di diritto d'autore, compreso il regime della direttiva 2019/790 (lett. c); la disciplina sulla protezione dei consumatori e la sicurezza dei prodotti (lett. h); e il regolamento 2019/1150 (lett. g). Quanto alle altre normative rilevanti, anch'esse continueranno ad applicarsi nella misura in cui la proposta DSA (o altri successivi atti) non vi apporteranno modifiche espresse o implicite.

Con la conferma dei regimi precedenti, impostati sul controllo *ex post* dei contenuti illegali, risulta chiaro come la Commissione abbia per ora abbandonato, anche su sollecitazione del Parlamento europeo[218], l'idea di imporre obblighi *ex ante* che, come sappiamo, è stata respinta per i contenuti terroristici e per quelli coperti dal diritto d'autore.

Piuttosto, l'Esecutivo UE si è mosso sulla strada degli incentivi "positivi" allo svolgimento volontario di attività di moderazione *ex ante*, prevedendo all'art. 6 una versione temperata del c.d. "principio del buon samaritano". La norma, confermando un'intenzione già espressa in passato[219], intende porre rimedio al circostanza[220] per cui gli ISP sono restii a svolgere attività di moderazione e adottare misure proattive per timore di perdere la qualifica di intermediari "passivi" e venire considerati responsabili indiretti per i contenuti illegali da loro individuati prima di apposita segnalazione o di un'ingiunzione nazionale[221].

Per questo motivo – ferma restando la giurisprudenza che ha già "incrinato" la distinzione tra intermediari attivi e passivi[222] e ha stabilito la possibilità di imporre obblighi specifici di sorveglianza[223] – viene stabilita una protezione *prima facie* per i prestatori: secondo l'art. 6, la semplice circostanza dello svolgimento di indagini volontarie o di altre attività dirette all'individuazione, identificazione e rimozione/disabilitazione dei contenuti illegali, così come l'adozione delle misure necessarie per conformarsi alle prescrizioni del diritto UE per quanto riguarda l'attuazione delle condizioni generali[224], non sarà sufficiente a escludere per quei prestatori la possibilità di avvalersi dell'esonero dalla responsabilità indiretta.

---

[217] In tema di contrasto all'abuso sessuale minorile, il Consiglio UE sta valutando il ruolo di specifiche misure proattive che, sul punto, vadano oltre le previsioni della proposta DSA (v. il doc. *The digital dimension of investigating child sexual abuse: challenges and way forward*, 28 settembre 2021, 12060/21).

[218] Si veda la risoluzione P9_TA(2020)0272, par. 6.

[219] Si vedano la comunicazione COM(2017)555, p. 14, e il considerando 26 della raccomandazione 2018/334. Sulla possibilità di introdurre il principio nell'ordinamento UE v. già J. BARATA, *Positive Intent Protections: Incorporating a* Good Samaritan principle *in the EU Digital Services Act*, 29.07.2020.

[220] *Supra*, nota 39 e testo corrispondente.

[221] In argomento A. BERTOLINI – F. EPISCOPO – N.-A. CHERCIU, *Liability*, *cit.*, p. 32.

[222] *Supra*, note 40 ss.

[223] Con le sentenze *Glawischnig-Piesczek* (contenuti diffamatori) e *YouTube* e *Cyando* (contenuti coperti dal diritto d'autore).

[224] Questa precisazione si ritrova nel considerando 25.

Si tratta, come detto, di una versione temperata del principio previsto nell'ordinamento degli USA[225], in quanto l'esonero opera solo se i prestatori eseguono misure proattive "in buona fede e in modo diligente"[226]: ciò significa che si applica anche in questo caso la regola del precedente art. 5 che, come sappiamo, esclude la possibilità per gli *hosting providers* di avvalersi dell'esonero qualora vengano a conoscenza della presenza di contenuti illegali – nel nostro caso, tramite attività "da buon samaritano" – e non agiscano immediatamente per rimuoverli o disabilitarne l'accesso.

Così formulato, l'art. 6 dovrebbe svolgere un ruolo abbastanza limitato[227]. Stabilendo – con formulazione inutilmente complicata – che non saranno inammissibili all'esonero dalla responsabilità indiretta "per il solo fatto" di adottare misure proattive, infatti, la Commissione intende circoscrivere la protezione del buon samaritano ai soli casi in cui gli ISP si limiteranno strettamente a svolgere le azioni indicate. Ragionando *a contrario*, dalla norma si ricava però anche la conferma che i prestatori potranno risultare responsabili in tutti gli altri casi di conoscenza di contenuti illegali[228] e, talvolta, anche qualora si mantengano nei limiti delle attività previste[229]. Detto altrimenti, le misure proattive volontarie né precluderanno né garantiranno l'esonero dalla responsabilità.

Se ciò è vero, è più che probabile che gli *hosting providers* di dimensione più ridotta faranno il più possibile a meno di simili misure per non fornire un'eventuale prova di conoscenza effettiva dell'esistenza di contenuti illegali diffusi sui loro servizi, la qual cosa pone un problema di effettività del principio. Al contrario, le piattaforme *online* specie se molto grandi – le quali, spesso, già oggi sono dotate di strumenti automatizzati sofisticati, risultano impegnate in attività estese di moderazione e andranno incontro a vincoli più incisivi nel futuro DSA – saranno più propense rispetto al passato a rimuovere i contenuti generati dagli utenti, rischiando però di non limitarsi solo a quelli chiaramente illegali ma lasciando che siano rimossi anche quelli "dubbi" per non risultare in qualche modo inadempienti[230].

---

[225] Ove invece è in vigore nella sua forma piena: in base alla *Section 230* del *Communications Act* del 1934, come modificato dal *Communications Decency Act* del 1996, i prestatori stabiliti negli Stati Uniti sono ritenuti sempre immuni da responsabilità anche se vengono a conoscenza di contenuti illegali diffusi tramite i loro servizi. Vedi D. KELLER, *US Developments and the DSA*, in L. WIEWIORRA – I. GODLOVITCH (eds.), *The Digital*, *cit.*, p. 12.

[226] Considerando 25.

[227] Per considerazioni sull'utilità di questa norma, v. G. CAGGIANO, *La proposta*, *cit.*, pp. 18-19.

[228] Ad es., quando assumeranno informazioni specifiche per trasmetterle alle autorità competenti in base all'art. 9, oppure nel momento in cui riceveranno notifiche anche non dettagliate da parte degli utenti *ex* art. 14. *Amplius* J. BARATA, *The Digital Services Act and the Reproduction of Old Confusions: Obligations, Liabilities and Safeguards in Content Moderation*, in *Verfassungsblog*, 2.03.2021.

[229] Ad es. qualora le misure proattive non si rivelino efficaci, oppure se vengano svolte in maniera non diligente. Ciò viene esplicitato nel considerando 25, il quale, con formulazione abbastanza "ipocrita", afferma che le attività volontarie non dovrebbero essere prese in considerazione ai fini della responsabilità indiretta, "senza che tale norma implichi tuttavia che il prestatore possa necessariamente avvalersene". Cfr. A. KUCZERAWY, *The Good Samaritan that wasn't: voluntary monitoring under the (draft) Digital Services Act*, *ivi*, 12.01.2021.

[230] Così anche J. BARATA, *The Digital*, *cit.* Sulla necessità che il DSA contenga una distinzione tra contenuti manifestamente illegali (soggetti a misure di rimozione in qualche modo automatiche), contenuti illegali "dubbi" (soggetti a rimozione solo dopo un'attenta attività di moderazione umana) e contenuti dannosi ma non illegali (per i quali la

Quest'ultima considerazione solleva un diverso problema di rispetto del principio di proporzionalità. Se è vero, infatti, che l'art. 6 tenta di conciliare la necessità di un intervento anticipato di moderazione con il regime di esenzione dalla responsabilità indiretta e con il divieto di obblighi generali di sorveglianza o ricerca attiva dei contenuti illegali, in un certo senso "invogliando" i *providers* a svolgere indagini volontarie, è altrettanto vero che la libertà di espressione degli utenti, che la proposta DSA pure si ripropone di tutelare, ne potrà risultare più facilmente lesa[231]. È dunque auspicabile, a fronte di una disposizione che rischia di rivelarsi non solo inutile ma anche dannosa, che il bilanciamento tra esonero dalla responsabilità e tutela della libertà di espressione sia al più presto individuato in un'apposita comunicazione interpretativa della Commissione, in attesa di una pronunzia della Corte di giustizia.

Carattere di novità rispetto alla direttiva *eCommerce* assume, poi, l'art. 8 della proposta che detta le disposizioni procedurali conseguenti agli ordini di contrastare i contenuti illegali emessi dalle autorità nazionali[232]. Questi andranno redatti nella lingua dichiarata dai prestatori e inviati al punto di contatto da questi nominato[233], oltre che al coordinatore nazionale dei servizi digitali[234] il quale a sua volta li trasmetterà alla rete dei coordinatori nazionali[235].

Gli ordini dovranno recare la motivazione per cui i contenuti sono ritenuti illegali (con indicazione della specifica disposizione europea o nazionale violata), gli elementi idonei alla loro identificazione (compreso uno o più indirizzi URL) e appropriate informazioni sui mezzi di ricorso. Inoltre, il loro àmbito di applicazione territoriale non dovrà eccedere quanto strettamente necessario per il conseguimento dell'obiettivo. Ricevuti gli ordini, gli ISP avranno l'obbligo di informare quanto prima l'autorità emittente in merito alle misure adottate e al momento in cui sono state eseguite.

4.2. ***Segue*: gli obblighi di diligenza delle diverse categorie di *provider* e le altre norme rilevanti**

Come si è anticipato, la proposta DSA stabilisce obblighi di diligenza via via più penetranti in ragione dei servizi offerti dai *providers* e della loro crescente dimensione economica. Tali obblighi, merita sottolinearlo, saranno applicabili indipendentemente dal regime di responsabilità applicabile e rappresentano la vera

rimozione non dovrebbe essere l'opzione preferibile), v. G. FROSIO – C. GEIGER, *Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime*, in *SSRN Electronic Journal*, dicembre 2020, spec. par. III.2. Sulla dubbia efficacia dei filtri automatizzati v. C. DOCTOROW, *Europe's Digital Services Act: On a Collision Course With Human Rights*, in *Electronic Frontier Foundation*, 27.10.2021.

[231] *Ibidem*.

[232] A questa norma si affianca quella dell'art. 9 sulle disposizioni procedurali conseguenti agli ordini di fornire informazioni, qui sinteticamente richiamata.

[233] L'art. 10 proposta DSA specifica che tutti gli ISP debbono istituire un punto di contatto unico per le comunicazioni con le autorità nazionali, la Commissione e il Comitato europeo per i servizi digitali dell'art. 47.

[234] Si tratta di una figura istituita dall'art. 38 della proposta, che ha la responsabilità di tutte le questioni relative all'applicazione e all'esecuzione del DSA a livello nazionale.

[235] Prevista dall'art. 67.

novità della proposta rispetto alla direttiva *eCommerce*. Mentre gli artt. da 10 a 13 riguardano tutti gli ISP, i successivi artt. 14 e 15 si rivolgono ai soli *hosting providers*; a loro volta, gli artt. da 16 a 24 interessano le sole piattaforme *online*; e infine gli artt. da 25 a 33 contengono obblighi per le sole piattaforme *online* di dimensioni molto grandi.

A) La moderazione dei contenuti e la loro eventuale rimozione o disabilitazione sono oggetto anzitutto degli *obblighi di trasparenza* degli artt. 12 e 13, che riguardano tutti gli ISP.

L'art. 12 impone a costoro di includere, nelle condizioni di servizio, appropriate *informazioni sulle restrizioni applicabili ai contenuti* forniti dai loro utenti. Esse andranno redatte in maniera chiara e comprensibile, rese disponibili in formato accessibile e dovranno illustrare, in specie, *le modalità con cui viene condotta la moderazione dei contenuti*, compresi i processi algoritmici utilizzati e la loro verifica umana (par. 1)[236]. La necessità di una politica trasparente sulle restrizioni emerge anche dall'obbligo degli ISP di agire in modo diligente, obiettivo e proporzionato nell'applicarle e farle rispettare, tenendo conto dei diritti e interessi legittimi di tutte le parti, compresi quelli sanciti dalla Carta di Nizza (par. 2)[237].

Si tratta di una significativa innovazione rispetto alla situazione attuale, in quanto i prestatori non sempre illustrano chiaramente la loro politica di moderazione e rimozione né sottopongono a verifica umana le decisioni automatizzate[238]. In specie, sarà così possibile accertare se la verifica umana dei processi automatizzati di moderazione si mantenga nei limiti della giurisprudenza *Glawischnig-Piesczek*[239]. Ciò posto, va però detto che la mancanza nella proposta di una definizione di "contenuto incompatibile con le condizioni generali"[240] ha la conseguenza di legittimare la rimozione di qualunque informazione solo perché ritenuta *a priori* inopportuna dagli ISP. Ciò solleva un rilevante problema di tutela della libertà di espressione nei confronti dei veri o presunti contenuti disinformativi: come è stato notato, invece di affidare una delega agli ISP a decidere cosa è disinformazione e cosa non lo è, sarebbe stato più opportuno rendere chiaramente illegali i contenuti disinformativi o almeno fornire una classificazione anche esemplificativa di quelli dannosi (ma non illegali)[241].

---

[236] Sulla necessità che i contenuti "dubbi" siano soggetti a un'attenta verifica umana, v. G. FROSIO – C. GEIGER, *Taking*, *cit.*, par. III.2.

[237] Per una critica relativa ai maggiori oneri in capo ai piccoli ISP, v. A. PEUKERT, *Five Reasons to be Skeptical About the DSA*, in *Verfassungsblog*, 31.8.2021.

[238] Tuttavia, l'art. 12 apre a tutta una serie di questioni, tra cui spicca quella dell'applicabilità dei diritti fondamentali nelle relazioni tra prestatori intermediari e destinatari dei servizi, su cui si rinvia a N. APPELMAN – J. P. QUINTAIS – R. FAHY, *Using Terms and Conditions to apply Fundamental Rights to Content Moderation: Is Article 12 DSA a Paper Tiger?*, in *Verfassungsblog*, 1.09.2021.

[239] E cioè del divieto di compiere una valutazione autonoma dei contenuti simili a quelli già dichiarati illegittimi: si tratta di un bilanciamento non agevole, come sottolineato da D. KELLER, *Facebook Filters, cit.*, p. 620 ss.

[240] Secondo la formula utilizzata nell'art. 2, par. p).

[241] Così R. JANAL, *Adapting*, *cit.* V. anche le considerazioni di M. EIFERT – A. METZGER – H. SCHWEITZER – G. WAGNER, *Taming*, *cit.*, pp. 1012-1014. In senso contrario invece A. PEUKERT, *Five*, *cit.*, secondo cui il DSA non dovrebbe contenere norme sulla rimozione diretta o indiretta dei contenuti dannosi ma non illegali.

A sua volta, l'art. 13 impone agli ISP (eccetto le micro e le piccole imprese) di pubblicare, almeno una volta l'anno, *relazioni chiare, facilmente comprensibili e dettagliate sulle attività di moderazione dei contenuti* svolte nel periodo di riferimento. Le relazioni dovranno indicare il numero di ordini ricevuti dalle autorità nazionali e le attività di moderazione avviate autonomamente (obbligo per tutti gli ISP), le notifiche presentate dagli utenti[242] (solo per gli *hosting providers*) e i reclami ricevuti per mezzo del sistema interno di gestione (obbligo che ricade solo sulle piattaforme *online*, anche molto grandi). In questa maniera, si dovrebbe assicurare un controllo *ex post* a carattere diffuso e la possibilità di correggere gli aspetti problematici da parte dei coordinatori nazionali dei servizi digitali[243] (e, per le piattaforme molto grandi, della Commissione)[244].

B) Gli *hosting providers* sono interessati da maggiori obblighi rispetto alla generalità degli ISP anche in merito alla moderazione e alla rimozione o disabilitazione dei contenuti illegali.

L'art. 14 afferma che essi dovranno predisporre *meccanismi di "notice-and-action"*, consentendo a persone o enti di presentare, facilmente e in via elettronica, notifiche precise e motivate sulla presenza di presunti contenuti illegali sui loro servizi[245]. Questa previsione si ricollega alla regola dell'art. 5: le notifiche "complete" – quelle cioè che soddisferanno le condizioni previste[246] – costituiranno *ex* art. 14, par. 3, la presunzione *juris et de jure* dell'avvenuta conoscenza o consapevolezza effettiva dell'esistenza di contenuti da verificare. Quindi, se vorranno avvalersi dell'esonero dalla responsabilità, gli *hosting providers* non avranno altra scelta che svolgere un'attenta attività di moderazione dei contenuti notificati e prendere decisioni sulla loro rimozione o disabilitazione in modo tempestivo, diligente e obiettivo, comunicandone l'esito ai notificanti assieme ai mezzi di ricorso esperibili.

Dubbi sorgono, invece, nel caso di notifiche "non complete": a nostro avviso, qui la presunzione assoluta non dovrebbe operare, dovendosi al contrario valutare con prove e controprove la diligenza dell'operatore economico in base alla giurisprudenza *L'Oréal SA* e *a.* c. *eBay*[247]. In altri termini, i maggiori oneri per gli *hosting providers* discenderanno dall'accuratezza con cui i notificanti redigeranno le denunce, essendo il regime *ex* art. 14 più restrittivo di quello delineato nella giurisprudenza ricordata.

---

[242] Queste andranno classificate per tipo di contenuto illegale, per eventuale azione intrapresa e per tempo medio di reazione.

[243] In base all'art. 41.

[244] *Ex* art. 51 ss. In riferimento all'analoga "opacità" delle procedure per la moderazione dei contenuti negli Stati Uniti, cfr. E. LEE, *Moderating Content Moderation: a Framework for Nonpartisanship in Online Governance*, in *American University Law Review*, 2021, p. 913 ss

[245] Sulla ruolo degli utenti come *platform prosecutors* v. Q. WEINZIERL, *Institutionalizing Parallel Governance: The Digital Services Act, Platform Laws, Prosecutors, and Courts*, in *Verfassungsblog*, 18.12.2020.

[246] Esse dovranno contenere la spiegazione dei motivi dell'illegalità dei contenuti, la chiara indicazione della loro ubicazione elettronica, le generalità del notificante e la dichiarazione della sua "buona fede".

[247] *Supra*, nota 40 e testo corrispondente.

L'art. 15 della proposta prevede un *obbligo di trasparenza* degli hosting providers nei confronti di *coloro che hanno fornito i contenuti considerati illegali*. La decisione di rimozione o disabilitazione andrà infatti comunicata, al più tardi al momento della sua esecuzione, all'utente che ha fornito i contenuti "incriminati", motivandola *ex* par. 2. La norma dovrebbe così porre un freno alla prassi "da far west" di numerosi prestatori (in specie, i *social network*) di rimuovere contenuti senza fornire motivazione e senza permettere agli utenti di accedere in maniera effettiva ai meccanismi interni di gestione dei reclami, ai mezzi di risoluzione extragiudiziale delle controversie e/o ai ricorsi per via giudiziaria.

C) Ulteriori obblighi interessano, poi, le sole piattaforme *online*. Queste ultime sono definite all'art. 2, lett. h) – in maniera forse un po' troppo riduttiva[248] – come *hosting providers* che, su richiesta degli utenti, memorizzano e diffondono al pubblico informazioni, a meno che tali attività siano di portata minore e puramente accessorie ad altri servizi.

Tranne le microimprese o le piccole imprese (art. 16), tutte le piattaforme *online* devono fornire agli utenti, *ex* art. 17, l'accesso a un *sistema interno di gestione dei reclami* per almeno 6 mesi dalla data dalle decisioni di rimozione o disabilitazione[249]. Il sistema dovrebbe permettere di sottoporre le motivazioni della liceità (e compatibilità con le condizioni di servizio) dei contenuti rimossi o disabilitati; se sufficienti, le decisioni saranno annullate senza indebito ritardo.

Gli utenti i cui contenuti sono stati rimossi o disabilitati potranno anche sottoporre doglianze ad *organismi esterni di risoluzione extragiudiziale delle controversie*, la cui attività sarà svolta previa certificazione del coordinatore dei servizi digitali dello Stato di stabilimento (art. 18). La norma risulta favorevole agli utenti per tre ragioni: vincola *ex lege* le piattaforme alle decisioni assunte da quegli organismi; non esclude un ricorso per via giudiziaria; e infine, in caso di decisione favorevole alle piattaforme, non impone agli utenti il pagamento di diritti e altre spese sostenute da queste ultime mentre, nel caso contrario, le piattaforme *online* saranno obbligate al rimborso della controparte[250].

Ora, non si può non rilevare l'ingiustificabile disparità di trattamento tra gli autori dei contenuti rimossi o disabilitati, che dispongono dei rimedi extragiudiziali degli artt. 17 e 18 (oltre che usufruire dell'obbligo informativo dell'art. 15), e gli utenti pregiudicati dalla presenza di contenuti illegali *online* (es. diffamatori). La situazione di questi ultimi utenti non è disciplinata dalla proposta DSA, il che lascia loro come uniche opzioni quelle di segnalare i contenuti, sperando che le piattaforme vi diano sèguito positivo, e di rivolgersi ai giudici nazionali per ottenere un provvedimento ingiuntivo[251].

---

[248] Conforme T. RODRIGUEZ DE LAS HERAS BALLELL, *Key Factors for Enhancing the Effectiveness of Enforcement: Analytical Framework and Proposals*, in L. WIEWIORRA – I. GODLOVITCH (eds.), *The Digital*, *cit.*, pp. 11-12.

[249] Per considerazioni sulla reale efficacia di tale norma, v. R. JANAL, *Adapting*, *cit.*

[250] Per una critica all'art. 18, v. D. HOLZNAGEL, *The Digital Services Act wants you to "sue" Facebook over content decisions in private de facto courts*, in *Verfassungsblog*, 24.06.2021.

[251] Conforme M. EIFERT – A. METZGER – H. SCHWEITZER – G. WAGNER, *Taming*, *cit.*, pp. 1010-1012.

Le piattaforme *online* dovranno anche adottare misure tecniche e organizzative per trattare in via prioritaria le *notifiche presentate dai segnalatori attendibili* (art. 19), che quindi svolgeranno in una cornice formale il loro attuale compito di "pre-moderazione" in vista delle successive decisioni delle piattaforme. In maniera opportuna, l'art. 20 stabilisce alcune *misure contro gli abusi*: i fornitori frequenti di contenuti manifestamente illegali dovranno essere sospesi dal servizio, per un periodo di tempo ragionevole e dopo un avviso preventivo; la sospensione opererà anche nei confronti del trattamento di notifiche e reclami presentati da persone o enti che hanno dimostrato in passato di presentare con frequenza notifiche o reclami manifestamente infondati.

Un altro obbligo di trasparenza è poi previsto dall'art. 23, in base al quale le piattaforme *online* dovranno includere *informazioni aggiuntive nella relazione di cui all'art. 13* sul numero di controversie sottoposte a organismi extragiudiziali (e sul loro esito), sul numero di sospensioni effettuate (evidenziando quelle sulla fornitura di contenuti illegali) e, soprattutto, su *qualsiasi uso di strumenti automatizzati per la moderazione dei contenuti*. Quest'ultimo obbligo ci sembra particolarmente importante, dovendo essere corredato dalla descrizione delle finalità delle attività di moderazione, dagli indicatori di accuratezza degli strumenti automatizzati e dall'indicazione delle eventuali garanzie applicate.

D) Infine, le sole piattaforme *online* di dimensioni molto grandi dovranno adempiere a obblighi ulteriori. Ci si riferisce ai c.d. "giganti tecnologici", cioè alle piattaforme che *ex* art. 25, par. 1, prestano i loro servizi a un numero medio mensile di destinatari attivi del servizio nell'UE pari o superiore a 45 milioni[252]. Queste sopporteranno, come si diceva, adempimenti più gravosi e controlli più intensi che, però, non è detto che siano in ultima analisi idonee a ridurre il loro dominio digitale[253].

L'art. 26 impone anzitutto l'obbligo di compiere annualmente una *valutazione degli eventuali rischi sistemici* riguardanti la diffusione dei contenuti illegali, gli eventuali effetti negativi per l'esercizio di alcuni diritti fondamentali[254] e la manipolazione intenzionale del servizio[255]. Quest'ultima ipotesi sarà di capitale importanza per l'attività dei *social network* a diffusione globale: essi, infatti, dovranno regolare il sistema di moderazione in modo da contrastare con rigore gli *account* falsi e l'uso di "bot" e altri sistemi automatizzati

[252] In base al medesimo art. 25, l'adeguamento del numero medio mensile dei destinatari e la definizione delle metodologie specifiche di calcolo spetteranno alla Commissione, mentre la designazione delle piattaforme *online* come "di dimensioni molto grandi" (o la revoca di tale designazione) sarà di pertinenza del coordinatore dei servizi digitali dello Stato alla cui giurisdizione sono soggette. Per una critica a questa soglia, ritenuta troppo alta, v. R. JANAL, *Adapting*, *cit.*; v. anche M. EIFERT – A. METZGER – H. SCHWEITZER – G. WAGNER, *Taming*, *cit.*, pp. 997-998.

[253] Anzi, secondo I. BURI – J. VAN HOBOKEN, *The DSA Proposal's Impact on Digital Dominance*, in *Verfassungsblog*, 30.08.2021, è possibile che queste piattaforme ne traggano addirittura un vantaggio competitivo.

[254] In particolare, quelli al rispetto della vita privata e familiare, alla libertà di espressione e di informazione, alla non discriminazione e alla tutela del minore.

[255] Sul trattamento dei contenuti disinformativi da parte delle piattaforme *online* di dimensioni molto grandi, v. P. CESARINI, *The Digital Services Act: a Silver Bullet to Fight Disinformation?*, 8.02.2021, e ID., *Regulating Big Tech to Counter Online Disinformation: Avoiding Pitfalls while Moving Forward*, in *Media Laws*, 2021, n. 1, p. 288 ss.

o semi-automatizzati idonei a diffondere in maniera rapida e ampia contenuti illegali o incompatibili con le condizioni di servizio[256], compresi quelli disinformativi. Ciò posto, valgono ancor più per le piattaforme molto grandi i rilievi critici in merito alla mancanza di definizione o classificazione dei contenuti legali ma "inopportuni" e al rischio che, per questa via, si giunga a violazioni della libertà di espressione[257].

A ogni modo, in presenza di rischi sistemici, l'art. 27 obbliga le piattaforme molto grandi ad adottare misure di attenuazione, in specie *adeguando il sistema di moderazione dei contenuti*, con possibilità per il Comitato europeo per i servizi digitali di individuare annualmente i rischi sistemici più rilevanti e le migliori pratiche per attenuarli, e per la Commissione di predisporre orientamenti generali in materia[258].

Le piattaforme molto grandi sopportano, in base all'art. 28, anche l'obbligo di sottoporsi annualmente ad *audit esterni indipendenti* diretti a valutare, tra l'altro, il rispetto di tutti gli obblighi concernenti la moderazione e la rimozione o disabilitazione dei contenuti illegali nonché degli impegni volontariamente assunti da quelle piattaforme attraverso la stipulazione di codici di condotta. In caso di *audit* non positivo, si dovranno adottare le misure correttive conseguenti.

Tra gli altri obblighi di diligenza, si segnalano infine gli artt. 34 e 35 dedicati alle *norme settoriali volontarie* e ai *codici di condotta*. Quanto alle prime, la Commissione intende sostenere e promuoverne lo sviluppo e l'attuazione per questioni connesse anche alla rimozione dei contenuti illegali: esse, infatti, riguarderanno almeno la presentazione elettronica delle notifiche degli utenti (art. 14) e dei segnalatori attendibili (art. 19), nonché gli *audit* indipendenti per le piattaforme molto grandi (art. 28). Con riguardo ai codici di condotta, si assiste alla definitiva generalizzazione della tendenza ad affiancare alla regolazione pubblica gli strumenti di co-regolazione: in presenza soprattutto di rischi sistemici, la Commissione potrà invitare tutte le parti interessate all'elaborazione di codici e valuterà, assieme al Comitato europeo per i servizi digitali, la loro efficacia.

4.3. *Segue*: cenni al controllo pubblico

La proposta DSA reca, infine, una disciplina dei poteri di controllo e di intervento delle autorità nazionali e della Commissione, cui si può solo accennare in questa sede[259].

[256] Così il considerando 57.
[257] *Supra*, nota 240 ss. e testo corrispondente. Per ulteriori rilievi critici v. A. PEUKERT, *Five*, *cit.*
[258] L'idoneità di queste norme a contrastare in maniera effettiva la diffusione dei contenuti illegali o incompatibili rimane però tutta da vedere: così H. RUSCHEMEIER, *Re-Subjecting State-Like Actors to the State*, in *Verfassungsblog*, 6.09.2021.
[259] Cfr. M. EIFERT – A. METZGER – H. SCHWEITZER – G. WAGNER, *Taming*, *cit.*, p. 1019 ss., e B. WAGNER – H. JANSSEN, *A first impression of regulatory powers in the Digital Services Act*, in *Verfassungsblog*, 4.01.2021.

I poteri dei coordinatori nazionali dei servizi digitali sono regolati dall'art. 41. Ai nostri fini, rilevano i poteri di ordinare la cessazione delle violazioni e imporre misure correttive (par. 2, lett. b)[260], oltre a quello di adottare misure provvisorie per evitare un rischio di danno grave (lett. e). Qualora queste misure non diano risultati, la violazione causi un danno grave e integri un reato grave che comporta minaccia per la vita o la sicurezza delle persone, i coordinatori avranno il potere di chiedere alle autorità giudiziarie di ordinare la restrizione temporanea dell'accesso degli utenti interessati dalla violazione oppure, se non praticabile, la restrizione dell'accesso all'interfaccia *online* dell'ISP sui cui servizi ha luogo la violazione (par. 3, lett. b). Tali restrizioni, che dovranno rispettare le misure di salvaguardia del par. 3 e le garanzie del par. 6, potranno essere disposte per un periodo di 4 settimane, ulteriormente prorogabili.

Va poi ricordato che poteri analoghi – peraltro, simili a quelli in materia *antitrust* – sono esercitabili anche dalla Commissione, sebbene solo nei confronti delle piattaforme *online* molto grandi (artt. 50-66).

Infine, a presidio delle regole suesposte, gli artt. 42 e 59 permettono rispettivamente ai coordinatori nazionali e alla Commissione di irrogare sanzioni effettive, proporzionate e dissuasive che possono arrivare fino al 6% del fatturato annuo degli ISP interessati.

5. Conclusioni

In questo lavoro si è tentato di fornire un quadro della disciplina UE, in vigore e in divenire, sulla moderazione e la rimozione o disabilitazione dei contenuti illegali *online*. Si tratta, com'è noto, di un problema sempre più rilevante: i cambiamenti che stanno interessando la regolamentazione della Rete, il ruolo sempre più incisivo delle piattaforme *online*, la banale circostanza per cui ognuno di noi passa un periodo di tempo significativo su Internet, tutto ciò sta determinando un cambiamento di approccio nei confronti della presenza di tali contenuti e, quindi, della responsabilità degli ISP.

Si sta passando, come già detto, da una fase in cui la diffusione dei contenuti illegali è stata in qualche modo tollerata al fine di intralciare il meno possibile lo sviluppo dei servizi *online*, a una di maggiore maturità (e rigore) determinata da specifiche esigenze (repressione del fenomeno terroristico, lotta contro gli abusi sessuali dei minori, limitazione alla diffusione degli *hate speech*) e dalla generale consapevolezza di dover porre un freno alla tradizionale "irresponsabilità" dei prestatori intermediari.

Non stupisce, pertanto, che l'UE abbia affrontato e stia affrontando il problema da diversi punti di vista, cercando di individuare un punto di equilibrio accettabile tra le confliggenti tutele della libertà d'impresa dei prestatori intermediati, della libertà di espressione e dei diritti fondamentali degli individui coinvolti.

La complessità della questione è testimoniata anche dalla diversità dei tipi di contenuti illegali da

[260] Per alcune problematiche concernenti il controllo delle piattaforme molto grandi da parte delle (sole) autorità nazionali dello Stato membro di stabilimento, v. D. HOLZNAGEL, *Ireland cannot do it alone. All Member States should contribute to the supervision of very large online platforms under the Digital Services Act*, *ivi*, 27.04.2021.

rimuovere e, quindi, dalla necessità di utilizzare strumenti adeguati alle differenti situazioni. Ecco perché, pur non mettendo in discussione (almeno formalmente) il regime della direttiva *eCommerce*, la normativa si è in qualche modo "stratificata", divenendo più complessa e diramandosi in numerosi rivoli. La proposta di *Digital Services Act* tenta quanto più possibile di "mettere ordine", sebbene non sia certo che le nuove regole, così come disegnate dalla Commissione, siano davvero in grado di affrontare in maniera efficace tutte le problematiche messe in luce, da ultimo, dai *Facebook Files*[261].

Quel che è certo è che la complessità della materia e le scelte della Commissione si stanno riflettendo non solo nell'attività di *lobbying* delle imprese del settore[262] ma anche nella varietà di posizioni all'interno e tra le Istituzioni legislative. Al momento in cui si scrive, la procedura per l'approvazione della proposta DSA è in fase di prima lettura.

Per il Parlamento europeo, la relatrice Schaldemose della commissione IMCO ha presentato il 28 maggio 2021 un progetto di relazione in cui si chiede l'introduzione di regole più stringenti per proteggere meglio i consumatori, ulteriori misure di trasparenza e requisiti per garantire la protezione degli utenti e rafforzare le disposizioni di attuazione e applicazione[263]. Tra le novità, si segnalano l'aggiunta di un par. 1-*bis* all'art. 5 sugli *hosting providers*, secondo cui questi ultimi sarebbero tenuti a rimuovere o disabilitare l'accesso a contenuti illegali entro 24 ore se possono danneggiare gravemente l'ordine pubblico, la sicurezza pubblica o la salute pubblica o danneggiare gravemente la salute o la sicurezza dei consumatori, oppure entro 7 giorni negli altri casi; di un co. 1-*bis* all'art. 6 su alcune garanzie aggiuntive per l'applicazione del principio del buon samaritano; nonché di un par. 6-*ter* all'art. 14 sull'obbligo di adottare misure di *stay-down* in relazione ai prodotti già dichiarati illegali e posti nuovamente in vendita sui *marketplaces*[264].

In Consiglio, invece, si sono svolte numerose riunioni. Già dal *progress report* del 12 maggio si ricavava il favore degli Stati per l'impianto complessivo della proposta, pur con l'esigenza di approfondire alcuni punti[265]. Il 4 e il 16 giugno, la presidenza portoghese ha fatto circolare due bozze di compromesso in cui si confermava la generale accettazione del nuovo atto (seppur condizionata allo scioglimento di alcuni nodi)[266]. Infine, il 25 novembre 2021 il Consiglio ha approvato l'orientamento generale proposto dalla

[261] Così M. SCOTT, *The Facebook Papers reveal the limits of regulation. It's time to think bigger*, in Politico, 26.10.2021.

[262] Sul punto v. M. BANK – F. DUFFY – V. LEYENDECKER – M. SILVA, *The Lobby Network: Big Tech'S Web of Influence in the EU*, agosto 2021.

[263] V. il progetto di relazione del 28 maggio 2021, PE693.594v01-00.

[264] In attesa del rapporto della commissione IMCO, si sono già espresse le commissioni associate LIBE (3.9.2021, PE692.898), ITRE (29.9.2021, PE693.552), TRAN (30.9.2021, PE691.254), JURI (30.9.2021, PE694.960), CULT (5.10.2021, PE693.943), FEMM (13.10.2021, PE693.717) ed ECON (29.10.2021, PE693.929).

[265] Doc. 8570/21.

[266] Si vedano i documenti del 4 giugno 2021, 9288/21, e del 16 giugno 2021, 9288/1/21, non reperibili *online*, che abbiamo ottenuto previa richiesta di accesso agli atti al Segretariato generale del Consiglio.

presidenza slovena[267], che costituisce la posizione dell'Istituzione in vista del negoziato col Parlamento europeo.

L'orientamento generale presenta numerose novità, in parte già presenti nelle bozze precedenti, che non è possibile qui esaminare: ci limiteremo a quelle principali di nostro interesse. Anzitutto, si propone di estendere formalmente l'àmbito di applicazione del DSA anche ai motori di ricerca e ai *marketplaces online*[268] nonché di istituire la categoria dei "motori di ricerca *online* molto grandi"[269]. Particolare attenzione viene data ai minori, a vantaggio dei quali gli ISP devono compiere uno sforzo informativo supplementare nelle condizioni di servizio e le piattaforme molto grandi prevedere misure di attenuazione dei rischi sistemici che li riguardino. Il testo di compromesso chiede agli ISP anche di informare i fornitori dei contenuti della ricezione delle ingiunzioni nazionali e del sèguito dato (art. 8)[270] e di non far discendere la presunzione di conoscenza effettiva nel quadro delle *notice-and-action* dell'art. 14 da tutte le notifiche "complete", bensì solo da quelle in base alle quali un *provider* diligente possa rilevare l'illegalità dei contenuti[271]. Infine, quanto alle piattaforme molto grandi – il cui regime diventa più rigoroso di quello proposto dalla Commissione – è di grande interesse l'indicazione, tra le misure di attenuazione dei rischi sistemici, della rapida rimozione o disabilitazione degli *hate speech* (art. 27)[272].

Va sottolineato che il testo di compromesso del Consiglio non si discosta di molto dalla bozza della commissione parlamentare IMCO, il cui voto è atteso entro la fine del 2021, in vista dell'avvio di un probabile "trilogo" che, nelle intenzioni delle Istituzioni, dovrebbe portare all'approvazione del DSA. Al momento, peraltro, non è dato sapere qual è la reazione della Commissione agli emendamenti proposti dal Consiglio e dal Parlamento europeo.

Di certo, però, riteniamo che le suesposte esigenze di modernizzazione del quadro normativo e di migliore bilanciamento dei diritti nell'ambiente *online* difficilmente si risolveranno in un arretramento sulla strada aperta dalla proposta DSA. Rimane tuttavia il dubbio di fondo, espresso in più occasioni nei paragrafi precedenti, se le norme del futuro DSA si riveleranno davvero efficaci nel limitare la diffusione dei contenuti illegali soprattutto sui *social networks* e sui *marketplaces online*.

[267] Il testo è del 18 novembre 2021, doc. 13203/21.
[268] Mentre ai primi si applica lo stesso regime di responsabilità dei *caching providers*, i secondi sono oggetto della nuova sezione 3-bis che contiene specifici obblighi di diligenza, tra cui quelli riguardanti prodotti e servizi rimossi.
[269] Ai quali applicare la disciplina delle piattaforme *online* molto grandi.
[270] In sostanza, viene applicata anche in questo caso la regola dell'art. 15 in caso di rimozione disposta autonomamente da quei prestatori.
[271] In tal modo si circoscrive l'àmbito della presunzione e, per l'effetto, si ampliano le possibilità per i prestatori di usufruire dell'esenzione dalla responsabilità indiretta.
[272] In questa maniera, almeno per le grandi piattaforme, ne dovrebbe risultare a monte la maggiore efficacia delle attività di moderazione dei contenuti d'odio.