Contrasto alla disinformazione, *Digital Services Act* e attività di private *enforcement*: fondamento, contenuti e limiti degli obblighi di *compliance* e dei poteri di autonormazione degli operatori*

Emanuele Birritteri

Abstract

Il contributo esamina l'impatto del Digital Services Act sull'attività di private enforcement per la moderazione dei contenuti immessi in rete dagli utenti – con la correlata due diligence – svolta dagli operatori digitali. Vengono analizzati fondamento, contenuti e limiti degli obblighi di compliance e dei poteri di autonormazione attribuiti al riguardo ai vari attori del sistema, mettendone in evidenza punti di forza e criticità con particolare riferimento alle strategie di contrasto alla disinformazione in rete. La parte finale dello scritto delinea alcune indicazioni di policy rivolte ai soggetti che saranno chiamati a conformarsi alle previsioni del nuovo Regolamento europeo.

This article aims at analysing the impact of the Digital Services Act on private enforcement activities for the moderation of user content – with the related due diligence – carried out by digital operators. In particular, the contribution examines the basis, content and limits of compliance obligations and self-regulatory powers attributed to the various actors involved, highlighting strengths and weaknesses, with a focus on strategies for combating disinformation online. The final part of the paper outlines some policy recommendations for subjects that will be required to comply with the provisions of this new European regulation.

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

Sommario

Keywords

Digital Services Act – *Compliance* – Autonormazione – *Due diligence* – *Private enforcement*

1. L'impatto del DSA sulle attività di *private enforcement* per il contrasto alla disinformazione: inquadramento generale

Nel corso dei primi due cicli della sezione giuridica di questa ricerca abbiamo rilevato come l'implementazione di strategie di contrasto alla disinformazione in rete non possa che fare affidamento sul coinvolgimento proattivo delle piattaforme online e degli operatori del mercato digitale, nella consapevolezza, come abbiamo cercato di dimostrare, dell'impossibilità di utilizzare il diritto criminale per punire di per sé la diffusione di notizie false, fuori dai casi in cui ciò arrechi pregiudizio ad interessi diversi dalla mera veridicità dell'informazione e per cui si ritenga possibile e necessaria la tutela penale[1].

Abbiamo altresì messo in luce come i decisori pubblici e gli studiosi del diritto punitivo debbano oggi necessariamente occuparsi delle pratiche di *private enforcement* tipiche di tale settore, dato che le attività di moderazione dei contenuti immessi in rete dagli utenti, realizzate soprattutto dalle grandi *corporation* digitali, possono incidere in misura significativa sui diritti fondamentali degli utenti (su tutti, la libertà di espressione), nel contesto di grandi arene digitali che, pur gestite da organizzazioni private, rappre-

[1] Sia consentito, anche per una più ampia *literature review*, il rinvio a E. Birritteri, *Punire la disinformazione: il ruolo del diritto penale e delle misure di moderazione dei contenuti delle piattaforme tra pubblico e privato*, in *Diritto penale contemporaneo – Rivista Trimestrale*, 4, 2021, 304 ss.

sentano oggi uno spazio di dibattito pubblico di rilevante importanza[2]. Ciò, inevitabilmente, finisce per "consegnare" nelle mani di tali *Big Tech* un grande potere, avendo tali soggetti collettivi la possibilità di farsi arbitri di tali dinamiche di interazione sociale e di esercitare una potestà "sanzionatoria" – in termini di rimozione di contenuti, disabilitazione di *account* anche di rilevanti personaggi politici, etc. – che può innescare un pericoloso *chilling effect* avuto riguardo al libero confronto democratico[3].

Di qui la necessità di costruire una cornice di regolazione pubblica volta a fissare le regole del gioco in materia, nell'ambito della quale gli operatori possano svolgere tali attività di autonormazione e "sanzionatorie" secondo regole fissate dal legislatore e sotto il controllo delle autorità pubbliche[4].

Il nuovo regolamento (UE) 2022/2065 relativo al mercato unico dei servizi digitali (*Digital Services Act*, d'ora in poi DSA) del 19 ottobre 2022[5] cerca di rispondere esattamente a tale esigenza, da un lato, prendendosi atto che gli «Stati membri stanno sempre più introducendo o stanno valutando di introdurre legislazioni nazionali sulle materia disciplinate dal presente Regolamento, imponendo in particolare obblighi di diligenza per i prestatori di servizi intermediari per quanto riguarda il modo in cui dovrebbero contrastare i contenuti illegali, la *disinformazione online* e altri rischi per la società»[6] e che alla luce «del carattere intrinsecamente transfrontaliero di internet […] tali legislazioni nazionali divergenti incidono negativamente sul mercato interno, che […] comporta uno spazio senza frontiere interne»[7]; dall'altro lato, riconoscendosi che, appunto, «un comportamento responsabile e diligente da parte dei prestatori di servizi intermediari è essenziale per un ambiente online sicuro, prevedibile e affidabile e per consentire ai cittadini dell'Unione e ad altre persone di esercitare i loro diritti fondamentali garantiti dalla Carta dei diritti fondamentali dell'Unione europea («Carta»), in particolare la libertà di espressione e di informazione, la libertà di impresa, il diritto alla non discriminazione e il conseguimento di un elevato livello di protezione dei consumatori»[8].

Obiettivo di questa sezione della presente ricerca è quello di esaminare l'impatto del DSA sull'attività di *private enforcement* per la moderazione dei contenuti immessi in rete dagli utenti – con la correlata *due diligence* – svolta dagli operatori digitali. Si tratta invero di pratiche che fino all'emanazione del regolamento europeo in questione venivano

[2] A. Gullo - G. Piccirilli, *Disinformazione e politiche pubbliche: una introduzione*, in *Diritto penale contemporaneo – Rivista Trimestrale*, 4, 2021, 248 ss.

[3] A. Gullo - G. Piccirilli, *ivi*, 249. In argomento v. anche A. Buratti, *Framing the Facebook Oversight Board: Rough Justice in the Wild Web?*, in questa *Rivista*, 2, 2022, 31 ss.

[4] Necessità che abbiamo ribadito anche all'esito del secondo ciclo della ricerca: v. il report del 2022, reperibile online in *esteri.it*.

[5] Per un primo inquadramento generale v. anche B. Tassone, *Riflessioni introduttive*, in *Diritto di internet*, 1, 2023, 3 ss. Nella letteratura internazionale v., ampiamente, anche per ulteriori riferimenti circa le varie implicazioni del nuovo regolamento, A. Turillazzi - M. Taddeo - L. Floridi - F. Casolari, *The digital services act: an analysis of its ethical, legal and social implications*, in *Law, Innovation and Technology*, 15(1), 2023, 83 ss.

[6] Cfr. il considerando 2 del regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), GU 2022 L 277/1 (corsivo nostro).

[7] V. sempre il considerando 2 del regolamento (UE) 2022/2065.

[8] Così il considerando 3 del regolamento (UE) 2022/2065.

svolte di fatto in assenza di una disciplina legislativa di riferimento, nonostante si trattasse e si tratti della prima (e soprattutto sovente anche unica) barriera "sanzionatoria" di contrasto alla diffusione della disinformazione in rete[9].

In linea generale, il primo effetto tangibile di questo regolamento su tali pratiche è determinato dall'art. 3, lett. t), che fornisce direttamente una definizione di «moderazione dei contenuti» –inquadrando così chiaramente, sul versante legislativo, il fenomeno che costituisce il *focus* di questa sezione del report – come «le attività, automatizzate o meno, svolte dai prestatori di servizi intermediari con il fine, in particolare, di individuare, identificare e contrastare contenuti illegali e informazioni incompatibili con le 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 informazioni, quali la loro retrocessione, demonetizzazione o rimozione o la disabilitazione dell'accesso agli stessi, o che incidono sulla capacità dei destinatari del servizio di fornire tali informazioni, quali la cessazione o la sospensione dell'account di un destinatario del servizio»[10].

Il Capo III del regolamento, poi, disciplina in dettaglio tutta una serie di *due diligence obligations* relative, tra l'altro, proprio a tali attività di *private enforcement*, con un sistema di obblighi strutturato secondo vari "livelli" di intensità crescente in base al particolare destinatario degli stessi, dalla dimensione "base" delle previsioni applicabili a tutti i prestatori di servizi intermediari fino all'ultimo "gradino" concernente le più gravose regole applicabili alle piattaforme online e ai motori di ricerca di "dimensioni molto grandi". In particolare, il passaggio a ogni livello successivo comporta la sottoposizione dell'operatore all'obbligo di conformarsi ad alcune disposizioni ulteriori che si aggiungono (e *non* si sostituiscono) a quelle degli stadi precedenti[11].

Nei paragrafi successivi descriveremo, quindi, i principali contenuti di tali obblighi di diligenza, cercando di metterne in evidenza punti di forza e limiti anche alla luce degli esiti dell'indagine svolta durante i primi due cicli della presente ricerca, per poi delineare, in conclusione, alcune indicazioni di *policy*.

1.1. Obblighi in punto di definizione di termini e condizioni del servizio

Come noto, la sezione 1 del Capo III del DSA riguarda le disposizioni applicabili a

[9] Per una più ampia analisi, sia consentito rinviare ancora a E. Birritteri, *Punire la disinformazione*, cit., 304 ss.

[10] Lo stesso art. 3, poi, per quanto qui interessa fornisce sia, alla lett. h), la definizione di contenuto illegale come «qualsiasi informazione che, di per sé o in relazione a un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme al diritto dell'Unione o di qualunque Stato membro conforme con il diritto dell'Unione, indipendentemente dalla natura o dall'oggetto specifico di tale diritto», sia, alla lett. u), quella di 'condizioni generali' come «tutte le clausole, comunque denominate e indipendentemente dalla loro forma, che disciplinano il rapporto contrattuale tra il prestatore dei servizi intermediari e il destinatario del servizio».

[11] Giustamente in dottrina si è subito parlato di approccio '*pyramid base*': v. M.L. Bixio, *Gli obblighi applicabili a tutti i prestatori di servizi intermediari, ai prestatori di servizi di* hosting *e ai fornitori di piattaforme* online *(Artt. 11-32 – Capo III, Sezioni, 1, 2, 3 e 4)*, in *Diritto di internet*, 1, 2023, 21.

tutti i prestatori di servizi intermediari.

La prima previsione che viene in considerazione in relazione all'oggetto di tale sezione della ricerca è senz'altro l'art. 14, che impone ai detti operatori di includere, con un linguaggio chiaro, semplice, comprensibile e adatto se del caso anche ai minori, nelle loro condizioni generali di erogazione del servizio, ogni informazione relativa a: a) tutte le politiche, le procedure e gli strumenti utilizzati nel moderare i contenuti immessi in rete dagli utenti, con informazioni specifiche sul «processo decisionale algoritmico e la verifica umana»[12]; c) le regole procedurali del loro sistema interno di gestione dei reclami[13].

È significativo notare come il legislatore europeo imponga a tali soggetti regolati, in definitiva, un obbligo di trasparenza rispetto alla necessità di informare i loro utenti sulle politiche connesse alla moderazione dei contenuti immessi in rete e sul funzionamento dei relativi mezzi di reclamo. Nulla si dice, quindi, sulle specifiche caratteristiche di dettaglio che tali procedure di *private enforcement* debbano avere, sui "connotati" dei processi di moderazione e su quelli, conseguenti, di reclamo da parte dell'utente rispetto alla decisione della piattaforma di imporre una restrizione sull'informazione immessa in rete. In tal senso, in questa previsione il DSA non impone modelli particolari.

Gli operatori, di conseguenza, rimangono sostanzialmente liberi di regolare nel modo da loro ritenuto più opportuno tanto i meccanismi di moderazione dei contenuti degli utenti, quanto i correlati strumenti di reclamo, dovendo però, nel farlo, come si legge al paragrafo 4 dell'art. 14 con una indicazione tanto generale quanto importante, agire «in modo diligente, obiettivo e proporzionato» e «tenendo debitamente conto dei diritti e degli interessi legittimi di tutte le parti coinvolte, compresi i diritti fondamentali dei destinatari del servizio, quali la libertà di espressione, la libertà e il pluralismo dei media, e altri diritti e libertà fondamentali sanciti dalla Carta»[14].

La scelta di *policy* qui fatta propria dal decisore eurounitario ci pare presenti aspetti positivi e alcune criticità.

Da un lato, invero, introdurre specifiche procedure di dettaglio sul piano della mo-

[12] Con una disposizione che evoca chiaramente i contenuti di cui all'art. 22 del GDPR, e l'esigenza quindi di una specifica forma di trasparenza in relazione ai principi ivi sanciti, che stabiliscono il diritto dell'interessato a non essere sottoposto a decisioni basate su trattamenti integralmente automatizzati che producano effetti che incidano sulla sua sfera giuridica, imponendo che tale automazione sia in tal senso parte di una procedura valutativa più ampia che, tra l'altro, preveda necessariamente l'intervento umano.

[13] I parr. 5 e 6 dell'art. 14 dettano poi alcune specificazioni di dettaglio ulteriori per le piattaforme e i motori di ricerca molto grandi «I fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi forniscono ai destinatari dei servizi una sintesi concisa delle condizioni generali, di facile accesso e leggibile meccanicamente, compresi le misure correttive e i mezzi di ricorso disponibili, in un linguaggio chiaro e privo di ambiguità. Le piattaforme online di dimensioni molto grandi e i motori di ricerca online di dimensioni molto grandi ai sensi dell'articolo 33 pubblicano le loro condizioni generali nelle lingue ufficiali di tutti gli Stati membri in cui offrono i loro servizi». In linea generale, poi, la disposizione obbliga i prestatori a informare i destinatari di ogni significativa variazione in merito alle condizioni generali del servizio.

[14] È significativo evidenziare come ai sensi del considerando 47 del DSA, nel «progettare, applicare e far rispettare [le] restrizioni […] i prestatori di servizi intermediari dovrebbero inoltre tenere debitamente conto delle pertinenti norme internazionali in materia di tutela dei diritti umani, quali i principi guida delle Nazioni Unite su imprese e diritti umani».

derazione dei contenuti e dei reclami, valide per qualsiasi prestatore di servizi intermediari a prescindere dallo specifico mercato di riferimento, dal tipo di attività, dalla dimensione, secondo un modello *one size fits all*, sarebbe stato molto rischioso e, forse, controproducente, con il rischio di imporre oneri eccessivamente gravosi e non necessari[15]; anche il richiamo esplicito alla libertà di espressione e al pluralismo dei media, poi, appare molto importante specie sul piano del contrasto alla disinformazione, sensibilizzando gli operatori sulla necessità di adottare un approccio molto prudente e attento al rispetto dei diritti fondamentali nel disciplinare e applicare tali *policy* che, come ricordavamo, possono avere un impatto molto significativo su simili *fundamental rights* e generare un pericoloso e non auspicale *chilling effect*.

Dall'altro lato, però, pur senza legittimare inutili irrigidimenti burocratici, sarebbe stato a nostro avviso utile aggiungere qualche specificazione in più in merito ai "diritti di garanzia" minimali dell'utente sul piano delle misure che la piattaforma può disciplinare e adottare incidendo sui suoi diritti fondamentali (su tutti, dalla nostra prospettiva, la libertà di espressione). Nelle indicazioni di *policy* che avevamo formulato al termine dei precedenti due cicli della presente ricerca, ad esempio, avevamo menzionato sul punto, tra l'altro, come minimo «il principio di legalità delle violazioni e delle misure sanzionatorie/interdittive, con i relativi corollari della irretroattività, della tassatività/precisione delle previsioni punitive, e del divieto di analogia, nonché con una chiara definizione dei soggetti titolari della potestà di dettare tali regole; il principio di proporzionalità del trattamento sanzionatorio rispetto alla concreta gravità della violazione; il divieto di responsabilità oggettiva e l'affermazione del principio di colpevolezza, con la necessità di specificare l'elemento soggettivo (dolo o colpa) necessario per integrare la violazione»[16]. Come avremo modo di evidenziare a breve, su taluni di tali profili alcune disposizioni aggiuntive previste dal DSA e applicabili a certi operatori sembrano offrire soluzioni più soddisfacenti, ma tale prima previsione restituisce l'impressione di una non del tutto compiuta valorizzazione di profili di non secondaria importanza per una efficace protezione degli utenti. Del resto, sul versante specifico del contrasto alla disinformazione, è proprio su tali preliminari aspetti – *i.e.*, sulla determinazione dei principi di comportamento degli utenti e delle modalità d'uso del servizio, piuttosto che esclusivamente sul successivo *private enforcement* di tali regole – che i decisori pubblici sono chiamati a misurarsi con le più delicate ripercussioni dell'esercizio da parte delle *corporation* tecnologiche di tale potestà di autoregolare il dibattito pubblico e il confronto politico che si svolge sulle loro reti, con tutti i rischi di censura e di impatto negativo sui diritti fondamentali che ciò comporta[17].

[15] Su questi temi si veda diffusamente anche P. Leerssen, *An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation*, in *Computer Law & Security Review*, 48, 2023, 6.

[16] Vedi testualmente l'indicazione di *policy* n. 20, nella versione del report della ricerca del 2022, reperibile online in *esteri.it*.

[17] A.P. Heldt, *EU Digital Services Act: The White Hope of Intermediary Regulation*, in T. Flew - F.R. Martin (a cura di), *Digital Platform Regulation. Global Perspectives on Internet Governance*, Cham, 2022, 79.

1.2. Relazioni di trasparenza

La sezione 1 del Capo III del DSA prevede all'art. 15 un ulteriore obbligo di *due diligence* per tutti i prestatori di servizi intermediari[18], afferente al nostro ambito di interesse: si tratta del dovere di pubblicare, almeno una volta all'anno, «relazioni chiare e facilmente comprensibili sulle attività di moderazioni dei contenuti svolte durante il periodo di riferimento».

Tali relazioni devono comprendere una serie di informazioni su, tra l'altro: *a)* le attività di moderazione di contenuti avviate di propria iniziativa anche mediante l'uso di strumenti automatizzati; per qualsiasi utilizzo di questi ultimi nelle attività di moderazione, peraltro, si devono fornire dettagli concernenti «la descrizione qualitativa, la descrizione delle finalità precise, gli indicatori di accuratezza e il possibile tasso di errore degli strumenti automatizzati utilizzati nel perseguimento di tali scopi e le eventuali garanzie applicate»; *b)* le misure implementate per fornire una specifica formazione e assistenza alle persone dell'organizzazione incaricate di svolgere tale attività di *private enforcement*; *c)* il numero e il tipo di "sanzioni" irrogate agli utenti avuto riguardo a ogni restrizione all'uso del servizio, con la necessità, tra l'altro, di classificare e differenziare tali informazioni in base alle diverse tipologie di contenuto illegale o alle specifiche regole interne della piattaforma violate, nonché con riferimento al metodo di rilevamento dell'inosservanza; *d)* il numero di reclami ricevuti[19]. Per le piattaforme online e i motori di ricerca "di dimensioni molto grandi", in linea con gli obblighi aggiuntivi per loro previsti[20], si prevedono altresì misure ancor più stringenti in merito ai contenuti e alle tempistiche di tale relazione[21].

---

[18] Il par. 2 dell'art. 15 peraltro stabilisce che «Il paragrafo 1 del presente articolo non si applica ai prestatori di servizi intermediari che si qualificano come microimprese o piccole imprese come definite nella raccomandazione 2003/361/CE e che non sono piattaforme online di dimensioni molto grandi a norma dell'articolo 33 del presente regolamento».

[19] In base alle lett. a) e b) del par. 1 dell'art. 15, inoltre, occorre indicare «a) per i prestatori di servizi intermediari, il numero di ordini ricevuti dalle autorità degli Stati membri, compresi gli ordini emessi a norma degli articoli 9 e 10, classificati in base al tipo di contenuti illegali in questione, lo Stato membro che ha emesso l'ordine e il tempo medio necessario per informare l'autorità che ha emesso l'ordine o qualsiasi altra autorità specificata nell'ordine in merito al suo ricevimento e per dare seguito allo stesso; b) per i prestatori di servizi di memorizzazione di informazioni, il numero di segnalazioni presentate a norma dell'articolo 16, classificate in base al tipo di contenuto illegale presunto di cui trattasi, il numero di segnalazioni presentate da segnalatori attendibili, nonché eventuali azioni intraprese in applicazione delle segnalazioni, specificando se l'azione sia stata avviata in virtù di disposizioni normative oppure delle condizioni generali del prestatore, il numero di segnalazioni trattate utilizzando strumenti automatizzati e il tempo mediano necessario per intraprendere l'azione». Rispetto ai reclami, poi, la lett. d) stabilisce che è necessario anche menzionare «per i fornitori di piattaforme online, conformemente all'articolo 20, la base di tali reclami, le decisioni adottate in relazione a tali reclami, il tempo mediano necessario per adottare tali decisioni e il numero di casi in cui tali decisioni sono state revocate». Ai sensi dell'art. 24 del DSA, tra l'altro, i fornitori di piattaforme online devono includere alcune informazioni aggiuntive in tale relazione, tra cui il numero di controversie sottoposte all'esame degli organismi di risoluzione extragiudiziale e il numero di sospensioni imposte *ex* art. 23 DSA.

[20] Sui quali ci soffermeremo nel dettaglio *infra* (par. 4 e ss. del presente capitolo).

[21] L'art. 42 del DSA stabilisce, infatti, che questi operatori debbano pubblicare, in almeno una delle lingue ufficiali degli Stati membri, «le relazioni di cui all'articolo 15 al più tardi entro due mesi dalla data di applicazione di cui all'articolo 33, paragrafo 6, secondo comma, e successivamente almeno ogni sei mesi», specificando «oltre alle informazioni di cui all'articolo 15 e all'articolo 24, paragrafo 1: a) le risorse

La commissione, inoltre, potrà adottare «atti di esecuzione per stabilire modelli relativi alla forma, al contenuto e ad altri dettagli delle relazioni a norma del paragrafo 1 del presente articolo, compresi periodi di comunicazione armonizzati», diffondendo quindi *best practice* operative e modelli standard di riferimento che potranno essere di concreto ausilio agli operatori per adeguarsi a tali obblighi di conformità.
Si tratta senz'altro di una previsione condivisibile ove l'obbligo di trasparenza imposto alle piattaforme muove dalla prospettiva *in the books* dell'art. 14 a quella, per così dire, *in action*, imponendosi una *disclosure* anche sul modo in cui le regole autonormate dalle piattaforme sull'attività di moderazione dei contenuti sono effettivamente applicate in concreto, nella quotidiana realtà operativa dell'organizzazione.
Ciò sembra poter consentire agli organi di *enforcement* di accedere a informazioni che hanno indubbiamente un peso specifico significativo per valutare se gli obblighi definiti dall'art. 14 del DSA siano effettivamente rispettati, pur rimanendo naturalmente ferme le perplessità sul margine di libero apprezzamento lasciato alle piattaforme nel definire, a monte, tali regole del gioco. Si tratta invero di un potere che non pare poter essere ridotto dal dovere, a valle, di pubblicare relazioni in merito alla concreta applicazione di misure costruite secondo una discrezionalità che rimane, come abbiamo rilevato, certamente ampia per larghi tratti.

2. Disposizioni aggiuntive applicabili ai prestatori di servizi di memorizzazione di informazioni, comprese le piattaforme online

Come osservato in apertura il DSA prevede una serie di doveri di diligenza a intensità crescente per gli operatori, che variano a seconda del tipo di soggetto regolato[22]; il pas-

umane dedicate dal fornitore di piattaforme online di dimensioni molto grandi alla moderazione dei contenuti in relazione al servizio offerto nell'Unione, suddivise per ciascuna lingua ufficiale applicabile degli Stati membri anche per il rispetto degli obblighi di cui agli articoli 16 e 22, nonché per il rispetto degli obblighi di cui all'articolo 20; b) le qualifiche e le competenze linguistiche delle persone che svolgono le attività di cui alla lettera a), nonché la formazione e il sostegno forniti a tale personale; c) gli indicatori di accuratezza e le relative informazioni di cui all'articolo 15, paragrafo 1, lettera e), suddivisi per ciascuna lingua ufficiale degli Stati membri», nonché ulteriori informazioni concernenti il numero medio mensile dei destinatari del servizio, anche per ciascun Stato membro. Specifici obblighi di pubblicazione e comunicazione aggiuntivi si riferiscono poi, ai sensi dei parr. 4 e 5 dell'art. 42 del DSA, agli *independent audit* cui tali soggetti, come vedremo (cfr. infra par. 4.4.), devono sottoporsi, prevedendosi tra l'altro che qualora «un fornitore di piattaforme online di dimensioni molto grandi o di motori di ricerca online di dimensioni molto grandi ritenga che la pubblicazione di informazioni a norma del paragrafo 4 possa comportare la divulgazione di informazioni riservate di tale fornitore o dei destinatari del servizio, comportare notevoli vulnerabilità per la sicurezza del suo servizio, compromettere la sicurezza pubblica o danneggiare i destinatari, può rimuovere tali informazioni dalle relazioni disponibili al pubblico. In tal caso il fornitore trasmette le relazioni complete al coordinatore dei servizi digitali del luogo di stabilimento e alla Commissione, corredate di una spiegazione dei motivi alla base della rimozione delle informazioni dalle relazioni disponibili al pubblico».

[22] G. Buttarelli, *La regolazione delle piattaforme digitali: il ruolo delle istituzioni pubbliche*, in *Giornale di diritto amministrativo,* 1, 2023, 116 ss. Autorevole dottrina rileva inoltre come, tra obblighi di diligenza privati e responsabilità pubbliche di *enforcement*, il DSA preveda un sistema "a rete" di poteri di vigilanza e controllo: L. Torchia, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in *Rivista trimestrale di diritto pubblico*, 4, 2022, 1108.

saggio a ogni nuovo livello comporta l'applicazione di obblighi aggiuntivi, che vanno a sommarsi a quelli dei "piani" precedenti. Il primo di tali "strati" di *obligation* aggiuntive è costituito dalle disposizioni della sezione II del capo III del DSA, concernente le regole applicabili ai prestatori di servizi di "memorizzazione di informazioni", comprese le piattaforme online. Per quanto qui interessa assumono in particolare rilievo gli artt. 16 e 17 del DSA, sui quali quindi soffermeremo subito la nostra attenzione.

2.1. Meccanismo di *notice and action*

La prima rilevante previsione è quella dell'art. 16 del DSA, che impone a tutti i prestatori di servizi di memorizzazione di predisporre meccanismi di «facile accesso e uso» per «consentire a qualsiasi persona o ente» di notificare la presenza «nel loro servizio di informazioni specifiche che tale persona o ente ritiene costituiscano contenuti illegali», con la possibilità di presentare «segnalazioni esclusivamente per via elettronica». Tali operatori, poi, dovranno predisporre misure idonee a facilitare le segnalazioni che appaiano «sufficientemente precise e adeguatamente motivate», qualificandosi in sostanza come tali quelle che presentino una serie di contenuti di dettaglio descritti analiticamente dal par. 2 dell'art. 16[23].

In tale disposizione, poi, il DSA, si occupa di fornire alcune indicazioni ulteriori, sia di carattere più generale che di dettaglio, circa gli obblighi procedurali a carico del prestatore e i diritti previsti per gli utenti interessati.

Dal primo punto di vista, infatti, in parte ricalcando quanto l'art. 14 precisa rispetto alla definizione di termini e condizioni, si prevede l'obbligo per i detti prestatori di prendere in carico simili segnalazioni e di adottare le decisioni in merito alle informazioni cui queste si riferiscono «in modo tempestivo, diligente, non arbitrario e obiettivo», fornendo altresì informazioni specifiche sull'eventuale uso di strumenti automatizzati nel trattare e assumere provvedimenti rispetto alle stesse.

Dal secondo punto di vista, poi, delineando un livello basilare e minimo di "diritti procedurali", si prevede che l'operatore digitale debba informare, sempre «senza indebito ritardo», il segnalatore (che può essere sia una persona fisica che un ente, che abbia fornito il proprio contatto «elettronico») sia del ricevimento della segnalazione, sia della decisione presa in merito, fornendo contestualmente ogni informazione circa i ricorsi disponibili per contestare il provvedimento del prestatore.

È significativo notare, inoltre, come le segnalazioni in questione siano in grado di dispiegare effetti anche rispetto al regime di responsabilità del *provider,* nella misura in cui

[23] E cioè «a) una spiegazione sufficientemente motivata dei motivi per cui la persona o l'ente presume che le informazioni in questione costituiscano contenuti illegali; b) una chiara indicazione dell'ubicazione elettronica esatta di tali informazioni, quali l'indirizzo o gli indirizzi URL esatti e, se necessario, informazioni supplementari che consentano di individuare il contenuto illegale adeguato al tipo di contenuto e al tipo specifico di servizio di memorizzazione di informazioni; c) il nome e l'indirizzo di posta elettronica della persona o dell'ente che presenta la segnalazione, tranne nel caso di informazioni che si ritiene riguardino uno dei reati di cui agli articoli da 3 a 7 della Direttiva 2011/93/UE (n.d.r. gli illeciti penali relativi agli abusi, allo sfruttamento sessuale dei minori e alla pornografia minorile); d) una dichiarazione con cui la persona o l'ente che presenta la segnalazione conferma la propria convinzione in buona fede circa l'esattezza e la completezza delle informazioni e delle dichiarazioni ivi contenute».

il paragrafo 3 dell'art. 16 sancisce che, ove tali *notices* consentano all'organizzazione di prendere contezza dell'illegalità del contenuto «senza un esame giuridico dettagliato», «si considera» che queste permettono all'operatore di acquisire una conoscenza effettiva dell'illegalità dell'attività o dell'informazione veicolata tramite i suoi servizi, con tutto ciò che ne consegue a norma dell'art. 6 circa la *hosting provider liability*[24].

La previsione dell'art. 16 è particolarmente opportuna nella misura in cui consente di "istituzionalizzare" un meccanismo di cruciale importanza come quello delle segnalazioni, con cui enti e persone fisiche possono "stimolare" gli operatori digitali a porre in essere in modo più efficace la loro attività di *private enforcement*, anche in un certo senso affiancandoli e supportandoli in procedure senz'altro molto onerose già sul piano gestionale e organizzativo. Del resto, *ad impossibilia nemo tenetur*, sicché non potremmo certo aspettarci/pretendere che i soggetti regolati in questione siano in grado, da soli, di identificare ogni contenuto illegale condiviso tramite i loro sevizi.

È molto importante evidenziare, però, come tale meccanismo di *notice and action* debba essere obbligatoriamente predisposto solo per ciò che concerne la segnalazione di attività e contenuti *illegali*[25] e non già, stando alla "lettera" dell'art. 16, per quelli meramente lesivi delle condizioni generali d'uso del servizio o c.d. standard della *community*. Fermo restando che le piattaforme, naturalmente, potranno pur sempre spontaneamente estendere il raggio applicativo di tali procedure, consentendo di attivarle anche per segnalare la presenza di contenuti non illegali, ma semplicemente lesivi delle condizioni d'uso del servizio quanto ad attività che non possono essere svolte sui loro servizi, bisognerebbe forse interrogarsi sulla condivisibilità o meno di tale scelta di regolazione e della decisione del legislatore europeo di non estendere l'adozione obbligatoria di simili procedure anche alle informazioni in parola.

Specie per ciò che concerne il contrasto alla disinformazione, infatti, molto spesso alcune modalità d'utilizzo del servizio (si pensi alla interazione tra più *account* al fine di aumentare artificiosamente la visibilità di certe notizie, o all'uso coordinato di *fake account* o *bot* automatici, etc.) non possono dirsi di per sé – o comunque non possono sempre agevolmente qualificarsi – come illegali; lo stesso vale per molte affermazioni false veicolate in campagne anche coordinate di disinformazione che, secondo quanto abbiamo avuto modo di osservare ampiamente nei precedenti cicli della ricerca, non hanno sovente alcuna rilevanza penale o, in generale, carattere di illiceità per l'ordinamento giuridico[26].

A volte, però, si tratta di informazioni rispetto alle quali la piattaforma può legittimamente decidere di applicare delle restrizioni (da quelle più *soft* concernenti l'utilizzo di

[24] In argomento rinviamo integralmente alla disamina svolta in dettaglio nel primo saggio della presente sezione (di L. D'Agostino, *Disinformazione e obblighi di* compliance *degli operatori del mercato digitale alla luce del nuovo* Digital Services Act). Sul tema v. anche, di recente, S. Braschi, *Il nuovo Regolamento sui servizi digitali: quale futuro per la responsabilità degli* Internet Service Provider*?*, in *Diritto penale e processo*, 3, 2023, 367 ss.

[25] Osserva M.L. Bixio, *Gli obblighi applicabili a tutti i prestatori di servizi*, cit., 23, che «la struttura *pyramid base*, tra i diversi tipi di servizi intermediari, ammette solo per l'*hosting* la segnalazione da parte di un soggetto privato e, per conseguenza, l'art. 9 tratta solo degli ordini (e non delle segnalazioni) rivolte ai prestatori di servizi intermediari».

[26] Per ogni riferimento v. E. Birritteri, *Punire la disinformazione*, cit., 316 ss.

banner con rinvio ad *alert* di *fact-checkers* indipendenti, fino a misure più incisive come la riduzione di visibilità o la rimozione del contenuto lesivo degli standard della *community*), per cui simili meccanismi di *notice and action* potrebbero rivestire particolare utilità, ferma restando naturalmente la 'generale 'esigenza, sopra evidenziata, che le piattaforme disciplinino l'utilizzo di tale potere "sanzionatorio" nel rispetto dei minimali principi di garanzia propri di qualsiasi paradigma disciplinare/punitivo, anche in ambito privato.

2.2. Obbligo di motivazione sulle misure di moderazione dei contenuti

La seconda previsione della sezione in analisi del DSA (art. 17) riguarda l'obbligo per i prestatori di *hosting services* di fornire ai destinatari del servizio, salvo che si tratti di contenuti commerciali ingannevoli ad ampia diffusione[27] o dell'esecuzione di ordini di autorità pubbliche *ex* art. 9 DSA, «una motivazione chiara e specifica»[28] su una serie di "sanzioni" applicate in sede di moderazione dei contenuti e nominalmente indicate dal par. 1 della disposizione (dalla semplice riduzione di visibilità dell'informazione, alla sospensione o cessazione della prestazione del servizio, fino alla chiusura dell'*account*)[29].
Il par. 3, inoltre, offre ulteriori e importanti dettagli sul contenuto specifico dell'obbligo di motivazione che grava su simili operatori.
Anzitutto, infatti, occorre chiarire la tipologia di sanzione che è stata irrogata, specificandone la portata territoriale e la durata.
Bisogna, poi, indicare «i fatti e le circostanze su cui si basa la decisione» di applicare la restrizione del servizio, specificando, ma solo «ove opportuno», se la sanzione sia stata applicata all'esito di una segnalazione pervenuta tramite il meccanismo di *notice and action* dell'art. 16 o in virtù di indagini volontarie intraprese di propria iniziativa dall'organizzazione, nonché – ma solo, anche qui, «ove strettamente necessario» – l'identità stessa del notificante. Queste ultime clausole di riserva attribuiscono un notevole margine di apprezzamento alle piattaforme e non potrà che essere l'*enforcement* concreto dal

[27] Qualche chiarimento sul punto è offerto dal considerando 55 del DSA, ove si legge che «L'obbligo di fornire una motivazione non dovrebbe tuttavia applicarsi ai contenuti commerciali ingannevoli ad ampia diffusione diffusi attraverso la manipolazione intenzionale del servizio, in particolare l'utilizzo non autentico del servizio, come l'utilizzo di bot o account falsi o altri usi ingannevoli del servizio».

[28] Il par. 4 della previsione aggiunge che le «Le informazioni fornite dai prestatori di servizi di memorizzazione di informazioni a norma del presente articolo devono essere chiare e facilmente comprensibili e il più possibile precise e specifiche tenuto conto delle circostanze del caso. In particolare le informazioni devono essere tali da consentire ragionevolmente al destinatario del servizio interessato di sfruttare in modo effettivo le possibilità di ricorso di cui al paragrafo 3, lettera f)».

[29] Nello specifico, il par. 1 dell'art. 17 DSA prevede l'obbligo di fornire tale motivazione rispetto alle seguenti misure: «a) eventuali restrizioni alla visibilità di informazioni specifiche fornite dal destinatario del servizio, comprese la rimozione di contenuti, la disabilitazione dell'accesso ai contenuti o la retrocessione dei contenuti; b) la sospensione, la cessazione o altra limitazione dei pagamenti in denaro; c) la sospensione o la cessazione totale o parziale della prestazione del servizio; d) la sospensione o la chiusura dell'account del destinatario del servizio». Si specifica al par. 2, tra l'altro, che tale previsione «si applica solo se le pertinenti coordinate elettroniche sono note al prestatore» e «al più tardi dalla data a partire dalla quale la restrizione è imposta, indipendentemente dal motivo o dal modo in cui è imposta».

DSA a chiarirne effettivamente la portata. Ci sembra, comunque, si possa leggere tra le righe la volontà del legislatore eurounitario di tutelare i segnalanti, lasciando però agli operatori digitali il delicato compito di operare un complesso bilanciamento tra tali esigenze di protezione e i "diritti di difesa" dell'utente che ha subito la restrizione imposta dalla piattaforma.

Occorre, inoltre, chiarire se la decisione sia stata presa in virtù dell'illegalità del contenuto o della sua incompatibilità con le condizioni generali d'uso del servizio (quindi, con le regole autonormate dalla piattaforma circa i c.d. standard della *community*), in entrambi i casi indicando la specifica base giuridica o la clausola contrattuale "interna" che si assume violata e i motivi per cui l'informazione o il contenuto vengono considerati in contrasto con tali previsioni.

Infine, con ulteriori due indicazioni, come visto, ricorrenti in tutto il DSA, si prevede l'obbligo per il prestatore di chiarire se la decisione sia stata presa utilizzando strumenti automatizzati anche, se del caso, per individuare il contenuto oggetto del provvedimento "sanzionatorio", nonché di fornire «informazioni chiare e di facile comprensione sui mezzi di ricorso a disposizione del destinatario del servizio in relazione alla decisione, in particolare […] attraverso i meccanismi interni di gestione dei reclami, la risoluzione extragiudiziale delle controversie e il ricorso per via giudiziaria».

L'art. 17 del DSA riveste, come ben può intuirsi, una primaria importanza rispetto al funzionamento concreto delle dinamiche di *private enforcement* degli operatori digitali.

Infatti, nella fase di autonormazione a monte, come abbiamo rilevato, i soggetti regolati mantengono un significativo margine di apprezzamento nell'individuare le informazioni o i contenuti (anche sul piano della lotta alla disinformazione) che possono essere veicolati o meno tramite le loro piattaforme, al netto della "sintetica" menzione della necessità di esercitare tale potestà di autoregolazione «in modo diligente, obiettivo e proporzionato» e «tenendo debitamente conto dei […] diritti e [delle] libertà fondamentali sanciti dalla Carta». Nella fase di *enforcement* a valle di tali regole autonormate, invece, l'articolo in commento appare più "sensibile" alle esigenze sia di dettagliare maggiormente, e non solo con clausole di carattere generale, gli obblighi degli operatori, sia di rafforzare e specificare con più analiticità i diritti e le garanzie procedurali minime per gli utenti che subiscono simili misure para-punitive[30].

L'ampiezza dell'obbligo motivazionale imposto ai soggetti regolati, infatti, pur ponendo in capo ad essi significativi oneri gestionali e organizzativi, appare una soluzione necessaria in considerazione dei diritti fondamentali su cui simili attività possono significativamente incidere, oltre a fornire una base di informazioni di partenza indispensabile per l'utente che voglia avvalersi degli strumenti di reclamo "interni" o "esterni" effettivamente disponibili a tutela della sua posizione.

In parte qua, allora, e anche tenuto conto del più limitato novero di operatori cui, come

[30] P. Leerssen, *An end to shadow banning?*, cit., 8, che osserva anche in chiave critica come «*the DSA's approach is inflexible in that it bundles all relevant due process rights – notice, explanation and appeals – into the singular concept of a 'moderation action'. In practice there may be a large set of edge-cases where integral explanation and/or appeal could be onerous in terms of costs, or too sensitive in terms of security, but where a bare notice right could still be of substantial value as a bulwark against shadow banning and as a minimal precondition for legal and social accountability. In this light, the DSA's attempt at balancing is somewhat rudimentary, and in future may benefit from further refinement, such as by incorporating more factors into the shadow banning calculus and unbundling notice safeguards from other aspects of due process*».

visto, si applica tale disposizione, il DSA opera un bilanciamento tutto sommato ragionevole tra tali interessi contrapposti, pure in considerazione del significativo squilibrio tra i "poteri" contrattuali delle parti[31].

3. Disposizioni aggiuntive applicabili alle piattaforme online

Nella struttura a intensità crescente delle *due diligence obligation* del DSA, la sezione III del Capo III del regolamento rafforza ulteriormente gli oneri di *compliance* gravanti sui più importanti *player* del mercato digitale, introducendo una serie di disposizioni aggiuntive applicabili alle piattaforme online, che, come noto, specie nel contrasto alla disinformazione, costituiscono i naturali interlocutori di qualsiasi strategia di regolazione del fenomeno.

Per quanto qui interessa, in particolare, vengono in rilievo le previsioni di cui agli artt. 20, 21 e 22 del DSA, applicabili a tutte le piattaforme online ad eccezione di quelle qualificabili come microimprese o piccole imprese ai sensi della Raccomandazione (CE) 2003/361, per quanto tale deroga non operi rispetto a quelli che, anche tra questi ultimi operatori, vengano designati come «piattaforme online di dimensioni molto grandi a norma dell'articolo 33, indipendentemente dal fatto che si qualifichino come microimprese o piccole imprese»[32].

3.1. Il sistema interno di gestione dei reclami

La prima *due diligence obligation* aggiuntiva per le piattaforme online consiste nell'obbligo di fornire ai propri utenti, comprese persone o enti che presentano una segnalazione, per almeno sei mesi[33] dalla decisione sulla segnalazione o dall'applicazione della "sanzione" nell'ambito dell'attività di moderazione di contenuti illegali o contrari alle

[31] Sul problema, in tali contesti, dell'"asimmetria delle posizioni' degli attori in campo v. B. Carotti, *La politica europea sul digitale: ancora molto rumore*, in *Rivista trimestrale di diritto pubblico*, 4, 2022, 998. Diffusamente cfr. anche G. Alpa, *Sul potere contrattuale delle piattaforme digitali*, in *Contratto delle imprese*, 2022, 721 ss.

[32] In particolare, l'art. 19 del DSA stabilisce in dettaglio che «1. La presente sezione, ad eccezione dell'articolo 24, paragrafo 3, non si applica ai fornitori di piattaforme online che si qualificano come microimprese o piccole imprese quali definite nella raccomandazione 2003/361/CE. La presente sezione, ad eccezione dell'articolo 24, paragrafo 3, non si applica ai fornitori di piattaforme online che si sono precedentemente qualificati come microimprese o piccole imprese quali definite nella raccomandazione 2003/361/CE nel corso dei 12 mesi successivi alla perdita di tale qualifica a norma dell'articolo 4, paragrafo 2, della medesima raccomandazione, tranne quando sono piattaforme online di dimensioni molto grandi ai sensi dell'articolo 33. 2. In deroga al paragrafo 1 del presente articolo, la presente sezione si applica ai fornitori di piattaforme online che sono stati designati come piattaforme online di dimensioni molto grandi a norma dell'articolo 33, indipendentemente dal fatto che si qualifichino come microimprese o piccole imprese».

[33] Il par. 2 dell'art. 20 precisa che il «periodo di almeno sei mesi di cui al paragrafo 1 del presente articolo decorre dal giorno in cui il destinatario del servizio è stato informato della decisione a norma dell'articolo 16, paragrafo 5, o dell'articolo 17».

condizioni generali del servizio[34], «l'accesso a un sistema interno di gestione dei reclami efficace, che consenta loro di presentare per via elettronica e gratuitamente reclami contro la decisione presa dal fornitore della piattaforma», che sia di «facile accesso e uso» e tale da consentire e agevolare «la presentazione di reclami sufficientemente precisi e adeguatamente motivati».

Anche in questo caso, sulla scorta di quanto già rilevato con riferimento all'art. 14 del DSA in punto di definizione di termini e condizioni del servizio, e in qualche modo a differenza dell'art. 17, il DSA non fornisce un *set* preciso di regole di dettaglio circa il funzionamento specifico di tali procedure interne di reclamo e sui correlati diritti procedurali specie del destinatario della "sanzione" irrogata dalla piattaforma.

Il par. 4 dell'art. 20, invero, si "limita" a sancire l'obbligo delle piattaforme online di gestire i reclami presentati tramite il loro sistema interno in modo «in modo tempestivo, non discriminatorio, diligente e non arbitrario», di ritirare la propria decisione ove il reclamo contenga «sufficienti motivi per indurre il fornitore a ritenere» che la decisione presa sia infondata, di comunicare senza indebito ritardo ai reclamanti la loro «decisione motivata» in merito al reclamo presentato nonché i mezzi ulteriori di ricorso a loro disposizione, nonché – in misura qui forse più significativa – la necessità che il ricorsi interni in questione vengano decisi «con la supervisione di personale adeguatamente qualificato e non avvalendosi esclusivamente di strumenti automatizzati» (essendo, del resto, costante l'attenzione rivolta dal DSA al rispetto dell'art. 22 del GDPR[35]).

Anche qui, dunque, alle piattaforme, fermi restando questi principi di fondo, viene lasciata ampia potestà di disciplinare nel modo ritenuto più opportuno il funzionamento concreto di tali procedure e sistemi interni di reclamo.

Pure in tal caso, però, senza legittimare formalismi eccessivi e non necessari, sarebbe stato auspicabile fornire indicazioni di maggiore dettaglio circa le garanzie procedurali minime a tutela di utenti che si trovino di fronte a decisioni capaci di incidere in modo significativo sui loro diritti fondamentali, avuto naturalmente particolare riguardo, nel settore del contrasto alla disinformazione, alla libertà di espressione.

Nei cicli precedenti della ricerca, del resto, avevamo osservato come proprio le procedure e le regole di funzionamento dei sistemi interni di reclamo fossero un ambito in cui le piattaforme online fanno spesso registrare un ridotto livello di trasparenza, e come fosse necessario costruire una cornice pubblica di regole del gioco tali da obbligare le piattaforme a garantire un livello minimo di "diritti di difesa" a tutela degli utenti, tra cui, ad esempio, il diritto al contraddittorio preventivo, la garanzia di sufficiente autonomia e indipendenza (anche rispetto alla distribuzione interna dei

[34] In particolare, il par. 1 dell'art. 20 del DSA menziona: «a) le decisioni che indicano se rimuovere le informazioni o disabilitare l'accesso alle stesse o se limitarne la visibilità; b) le decisioni che indicano se sospendere o cessare in tutto o in parte la prestazione del servizio ai destinatari; c) le decisioni che indicano se sospendere o cessare l'account dei destinatari; d) le decisioni che indicano se sospendere, cessare o limitare in altro modo la capacità di monetizzare le informazioni fornite dai destinatari».

[35] Sul tema, in generale, dei trattamenti automatizzati anche con riferimento a quest'ultima disposizione, v., nella dottrina penalistica, anche per più ampi riferimenti, tra gli altri: L. D'Agostino, *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al d.lgs. 10 agosto 2018, n. 101,* in *Archivio penale,* 1, 17 ss.; G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Diritto penale contemporaneo – Rivista Trimestrale*, 4, 2020, 75 ss.

poteri dell'organizzazione) dei soggetti deputati a irrogare la sanzione e a decidere sui connessi reclami, il diritto di richiedere, già a livello interno, un ulteriore riesame della decisione[36].

Pur non potendosi certamente imporre generali modelli standard secondo un analitico livello di dettaglio, insomma, l'impressione anche su questo versante è quella di un percorso che, pur avendo condivisibilmente istituzionalizzato tali meccanismi e correttamente sancito in linea generale l'obbligo delle piattaforme di agire in modo non discriminatorio e arbitrario e secondo diligenza anche nella gestione dei reclami interni, poteva essere ancora perfezionato nella direzione della più efficace tutela dei diritti degli utenti[37].

3.2. La risoluzione extragiudiziale delle controversie

L'art. 21 del DSA stabilisce che gli utenti e coloro che hanno presentato segnalazioni hanno il diritto di scegliere, rispetto a qualsiasi controversia inerente alle stesse decisioni delle piattaforme menzionate dal par. 1 dell'art. 20 del DSA, compresi i «reclami che non è stato possibile risolvere mediante il sistema interno di gestione dei reclami di cui a tale articolo», «qualunque organismo di risoluzione extragiudiziale delle controversie» certificato ai sensi del par. 3 dell'art. 21, che subordina l'ottenimento di tale certificazione, attribuita dal coordinatore dei servizi digitali dello Stato membro, al soddisfacimento di requisiti dettagliatamente descritti e volti principalmente ad assicurare la competenza, l'imparzialità e l'indipendenza di simili organismi e l'adozione da parte loro di «regole procedurali chiare ed eque»[38].

---

[36] E. Birritteri, *Punire la disinformazione*, cit., 322 ss.

[37] In dottrina, invero, nei primi commenti al DSA è subito emerso un primo dibattito anche su questi aspetti: cfr. F. G'sell, *The Digital Services Act: A General Assessment*, in A. von Ungern-Sternberg (a cura di), *Content Regulation in the European Union. The Digital Services Act*, Trier, 2023, 95.

[38] In particolare, il par. 3 dell'art. 21 del DSA prevede che «Il coordinatore dei servizi digitali dello Stato membro in cui è stabilito l'organismo di risoluzione extragiudiziale delle controversie certifica tale organismo, su sua richiesta, per un periodo massimo di cinque anni rinnovabile, se il medesimo ha dimostrato di soddisfare tutte le condizioni seguenti: a) è imparziale e indipendente, anche sul piano finanziario, dai fornitori di piattaforme online e dai destinatari del servizio prestato dai fornitori di piattaforme online, ivi compresi le persone o gli enti che hanno presentato segnalazioni; b) dispone delle competenze necessarie, in relazione alle questioni che sorgono in uno o più ambiti specifici relativi ai contenuti illegali o in relazione all'applicazione e all'esecuzione delle condizioni generali di uno o più tipi di piattaforme online, per consentire a tale organismo di contribuire efficacemente alla risoluzione di una controversia; c) i suoi membri sono retribuiti secondo modalità non legate all'esito della procedura; d) la risoluzione extragiudiziale delle controversie che offre è facilmente accessibile attraverso le tecnologie di comunicazione elettronica e prevede la possibilità di avviare la risoluzione delle controversie e di presentare i necessari documenti giustificativi online; e) è in grado di risolvere le controversie in modo rapido, efficiente ed efficace sotto il profilo dei costi e in almeno una delle lingue ufficiali delle istituzioni dell'Unione; f) la risoluzione extragiudiziale delle controversie che offre avviene secondo regole procedurali chiare ed eque che sono facilmente e pubblicamente accessibili e conformi al diritto applicabile, compreso il presente articolo. Ove opportuno il coordinatore dei servizi digitali specifica nel certificato: a) le questioni concrete cui si riferisce la competenza dell'organismo, a norma del primo comma, lettera b); e b) la lingua o le lingue ufficiali delle istituzioni dell'Unione in cui l'organismo è in grado di risolvere le controversie, a norma del primo comma, lettera e)». Il par. 4 della medesima previsione aggiunge che «I coordinatori dei servizi digitali elaborano ogni due anni

I fornitori di piattaforme online hanno l'obbligo di rendere edotti chiaramente i propri utenti sulle possibilità di avere accesso a tali strumenti di risoluzione extragiudiziale delle controversie, facendo sì che tali informazioni siano «agevolmente accessibili sulla loro interfaccia online», pur restando impregiudicato, ai sensi del par. 1 dell'art. 21, «il diritto del destinatario del servizio in questione di avviare, in qualsiasi fase, procedimenti per contestare tali decisioni da parte dei fornitori di piattaforme online dinanzi a un organo giurisdizionale conformemente al diritto applicabile».

Del resto, la disposizione è ben chiara nel prevedere che tali organismi di risoluzione extragiudiziale non abbiano il potere di imporre una decisione «vincolante per le parti» e che le stesse piattaforme online possano legittimamente rifiutarsi di adirli «qualora una controversia riguardante le stesse informazioni e gli stessi motivi di presunta illegalità o incompatibilità dei contenuti sia già stata risolta».

Sul piano procedurale, si prevede che le parti «adiscono in buona fede» l'organismo in questione, che deve mettere a loro disposizione[39] il proprio provvedimento, come visto, non vincolante, entro 90 giorni dal ricevimento del reclamo, con la possibilità di prorogare il termine per definire il procedimento di oltre 90 giorni al massimo in caso di controversie molto complesse.

Per ciò che concerne i risarcimenti e i costi della lite, tra l'altro, è evidente il *favor* legislativo nei confronti del reclamante, alla luce del noto squilibrio contrattuale e di poteri tra le parti in causa in questi contesti, specie nella misura in cui si prevede che gli utenti debbano poter accedere «gratuitamente, o per un importo simbolico» a tali meccanismi[40], nonché che, a differenza delle piattaforme, non debbano farsi carico dei e «diritti e [del]le altre spese che il fornitore della piattaforma online ha sostenuto o deve sostenere in relazione alla risoluzione della controversia, a meno che l'organismo di risoluzione extragiudiziale delle controversie non ritenga che detto destinatario abbia agito manifestamente in mala fede».

Tale previsione, al netto della natura non vincolante delle decisioni degli organismi in parola, ci pare rivesta in definitiva una indubbia importanza nella misura in cui offre agli utenti dei servizi digitali una ulteriore alternativa per tutelare la propria posizione,

una relazione sul funzionamento degli organismi di risoluzione extragiudiziale delle controversie da essi certificati. In particolare, tale relazione: a) elenca il numero di controversie che ciascun organismo di risoluzione extragiudiziale delle controversie certificato ha ricevuto ogni anno; b) indica l'esito delle procedure avviate dinanzi a tali organi e il tempo medio necessario per risolvere le controversie; c) individua e spiega eventuali carenze sistemiche o settoriali o difficoltà incontrate in relazione al funzionamento di tali organismi; d) individua le migliori prassi relative a tale funzionamento; e) formula raccomandazioni su come migliorare tale funzionamento, ove opportuno». Si vedano altresì i parr. 6, 7, 8 e 9 dell'art. 21 che prevedono rispettivamente: a) la possibilità per gli Stati membri di istituire organismi di risoluzione extragiudiziale delle controversie o di sostenere l'attività di quelli che hanno certificato; b) la possibilità di revocare la certificazione ove vengano meno le condizioni di cui al par. 3, assicurando un contradditorio preventivo prima di dar corso alla decisione; c) l'obbligo per il coordinatore dei servizi digitali di comunicare alla Commissione gli organismi certificati; d) il fatto che l'art. 21 lasci «impregiudicati la direttiva 2013/11/UE e le procedure e gli organismi di risoluzione alternativa delle controversie per i consumatori istituiti a norma di tale direttiva».

[39] Il par. 5 dell'art. 21 prevede altresì che prima «di avviare la risoluzione delle controversie, gli organismi di risoluzione extragiudiziale delle controversie certificati comunicano al destinatario del servizio, ivi compresi le persone o gli enti che hanno presentato una segnalazione, e al fornitore della piattaforma online interessata i diritti o i meccanismi utilizzati per determinarli».

[40] Che si rifanno alla logica delle *alternative dispute resolution* (ADR).

specie lì dove il sistema di reclamo interno alla piattaforma online non abbia dato gli esiti sperati o comunque presenti criticità, senza dover necessariamente adire l'autorità giudiziaria o in generale gli attori pubblici di *enforcement* e senza che l'innesco di tale binario alternativo di risoluzione delle controversia pregiudichi il diritto di poter percorrere comunque, in qualsiasi fase, le "strade" della giurisdizione statale.
Ciò potrà comportare benefici anche per gli stessi operatori digitali e, soprattutto, per la gestione statale dei servizi giudiziari, nella misura in cui tali ADR, se correttamente implementate, possono aiutare gli Stati a raggiungere l'obiettivo di gestire in modo più efficiente la macchina della giustizia, non aumentando la mole (in molti Paesi già considerevole) dei contenziosi[41].

3.3. Le previsioni in tema di segnalatori attendibili

L'art. 22 del DSA prevede l'obbligo per le piattaforme online di adottare «le misure tecniche e organizzative necessarie» per trattare con priorità e decidere «senza indebito ritardo» le segnalazioni circa la presenza di contenuti illegali presentate, tramite il meccanismo di *notice and action* di cui all'art. 16, da «segnalatori attendibili» entro «il loro ambito di competenza designato».
In particolare, la qualifica di segnalatore attendibile viene riconosciuta, a richiesta di qualunque ente, dal coordinatore dei servizi digitali «dello Stato membro in cui è stabilito il richiedente», a condizione che quest'ultimo dimostri di soddisfare una serie di condizioni specificamente indicate dal par. 2 dell'art. 22 e tese a garantire, tra l'altro, l'indipendenza, la particolare *expertise* e la diligenza di tali *trusted flaggers*[42], i quali, tra l'altro, devono pubblicare relazioni almeno annuali sulle loro attività[43] e possono ve-

[41] Per un commento a queste previsioni del DSA in tema di risoluzione alternativa delle controversie, nonché per una disamina del loro impatto sulla nostra legislazione nazionale in tema di ADR, v. G. Gioia - A. Bigi, *La risoluzione stragiudiziale delle controversie nel mercato dei servizi digitali (artt. 17, 20, 21, 24, 35 – Capo III, Sezioni 2, 3 e 5)*, in *Diritto di internet*, 1, 2023, 39 ss. V. altresì A.M. Felicetti, *La risoluzione extragiudiziale delle dispute nei mercati digitali: alcune novità dall'Europa*, in *Rivista trimestrale di diritto e procedura civile*, 1, 2023, 197 ss.

[42] In particolare, il par. 2 dell'art. 22 del DSA stabilisce che «La qualifica di «segnalatore attendibile» a norma del presente regolamento viene riconosciuta, su richiesta di qualunque ente, dal coordinatore dei servizi digitali dello Stato membro in cui è stabilito il richiedente al richiedente che abbia dimostrato di soddisfare tutte le condizioni seguenti: a) dispone di capacità e competenze particolari ai fini dell'individuazione, dell'identificazione e della notifica di contenuti illegali; b) è indipendente da qualsiasi fornitore di piattaforme online; c) svolge le proprie attività al fine di presentare le segnalazioni in modo diligente, accurato e obiettivo».

[43] Il par. 3 dell'art. 22 del DSA prevede specificamente che «I segnalatori attendibili pubblicano, almeno una volta all'anno, relazioni facilmente comprensibili e dettagliate sulle segnalazioni presentate conformemente all'articolo 16 durante il periodo di riferimento. La relazione elenca almeno il numero di segnalazioni classificate in base: a) all'identità del prestatore di servizi di memorizzazione di informazioni; b) al tipo di presunto contenuto illegale notificato; c) alle azioni adottate dal prestatore. Tali relazioni includono una spiegazione delle procedure in atto per assicurare che il segnalatore attendibile mantenga la propria indipendenza. I segnalatori attendibili inviano tali relazioni al coordinatore dei servizi digitali che ha conferito la qualifica e le mettono a disposizione del pubblico. Le informazioni in tali relazioni non contengono dati personali». Inoltre, ai sensi dei parr. 4, 5 e 8 dell'art. 22 in commento i coordinatori dei servizi digitali devono comunicare alla Commissione – la quale predisporrà una banca dati accessibile al pubblico con l'elenco di tutti i segnalatori attendibili e potrà emanare, se necessario, «orientamenti

dersi revocata la qualifica di segnalatori attendibili, anche su istanza delle piattaforme online, ove abbiano presentato un numero significativo di segnalazioni infondate o, comunque, in generale, ove siano venute meno le condizioni stabilite dal paragrafo 2[44].
Il considerando 61 del DSA fornisce interessanti chiarimenti circa le particolari figure cui il decisore pubblico europeo ha evidentemente pensato nel costruire tale disposizione, specificando che può trattarsi sia di enti di natura pubblica (ad es. Europol o le unità addette alle segnalazioni di contenuti terroristici su internet) sia di organismi privati (ad es. gli enti facenti parte della «rete di linee di emergenza per la segnalazione di materiale pedopornografico INHOPE e le organizzazioni impegnate nella notifica dei contenuti razzisti e xenofobi illegali online»), indicando tra l'altro l'importanza, per «evitare di attenuare il valore aggiunto di tale meccanismo», di «limitare il numero complessivo di qualifiche» conferite in conformità al DSA.
La decisione del legislatore eurounitario, in definitiva, è quella di obbligare le piattaforme online a predisporre una sorta di canale di segnalazione privilegiato per tali enti, nella convinzione che questi possano supportare in modo particolarmente efficace questi operatori digitali nelle loro attività di "*digital patrolling*", secondo un approccio improntato alla cooperazione tra i vari *stakeholder* che, come noto, ha rivestito e riveste grande importanza nella lotta alle campagne (coordinate e non) di disinformazione[45].

per assistere i fornitori di piattaforme online e i coordinatori dei servizi digitali nell'applicazione dei paragrafi 2, 6 e 7» – ogni provvedimento relativo al riconoscimento o alla sospensione/revoca della qualifica di segnatore attendibile.

[44] I parr. 6 e 7 dell'art. 22 del DSA, invero, sanciscono che «6. Se un fornitore di piattaforme online dispone di informazioni indicanti che un segnalatore attendibile ha presentato un numero significativo di segnalazioni non sufficientemente precise, inesatte o non adeguatamente motivate avvalendosi dei meccanismi di cui all'articolo 16, comprese le informazioni raccolte in relazione al trattamento dei reclami tramite i sistemi interni di gestione dei reclami di cui all'articolo 20, paragrafo 4, comunica dette informazioni al coordinatore dei servizi digitali che ha riconosciuto la qualifica di segnalatore attendibile all'ente interessato, fornendo le spiegazioni e i documenti giustificativi necessari. Una volta ricevute le informazioni dal fornitore delle piattaforme online e ove il coordinatore dei servizi digitali ritenga che vi siano motivi legittimi per avviare un'indagine, la qualifica di segnalatore attendibile è sospesa durante il periodo dell'indagine. Tale indagine è condotta senza indebiti ritardi. 7. Il coordinatore dei servizi digitali che ha riconosciuto la qualifica di segnalatore attendibile a un ente revoca tale qualifica se accerta, a seguito di un'indagine avviata di propria iniziativa o in base a informazioni ricevute da terzi, comprese le informazioni fornite da un fornitore di piattaforme online a norma del paragrafo 6, che l'ente non soddisfa più le condizioni di cui al paragrafo 2. Prima di revocare tale qualifica, il coordinatore dei servizi digitali dà all'ente in questione la possibilità di rispondere alle constatazioni della sua indagine e di reagire alla sua intenzione di revocarne la qualifica di segnalatore attendibile».

[45] Per una panoramica dei vari approcci in materia di contrasto alla disinformazione v. O. Pollicino, *The European approach to disinformation: comparing supranational and national measures*, in *Annuario di diritto comparato e di studi legislativi*, 1, 2020, 175 ss. In generale, sulle dinamiche di co-regolazione pubblico-privato che riguardano le piattaforme v. ampiamente A. Simoncini, *La co-regolazione delle piattaforme digitali*, in *Rivista trimestrale di diritto pubblico*, 4, 2022, 1031 ss.

4. Gli obblighi supplementari a carico delle *Very Large Online Platforms (VLOPs)* e dei *Very Large Online Search Engines (VLOSEs)*: la scommessa del legislatore europeo sulla compliance

La sezione V del Capo III del DSA corrisponde al "gradino" più elevato del sistema di *due diligence obligation* a livelli di intensità crescente costruito dal nuovo regolamento europeo, rivolgendosi ai motori di ricerca e alle piattaforme online di "dimensioni molto grandi", qualificandosi in questo modo gli operatori che vengono espressamente designati come tali da una decisione della Commissione europea[46], a norma dell'art. 33 DSA, con riferimento a coloro «che hanno un numero medio mensile di destinatari attivi[47] del servizio nell'Unione pari o superiore a 45 milioni».

Si tratta, per così dire, dei *target* più importanti della strategia di regolazione del legislatore eurounitario, rispetto ai quali il DSA riserva incisivi poteri di *enforcement* (esercitati direttamente, tra l'altro, avuto riguardo a tale sezione del regolamento, dalla Commissione europea, così da "contrapporre" un interlocutore sovranazionale "di peso" a società, esse stesse, multinazionali e detentrici di rilevanti poteri[48]), nonché i più significativi obblighi di conformità che si aggiungono, come sappiamo, a quelli delle sezioni del regolamento precedentemente analizzate.

Tra tali operatori, del resto, si collocano i più importanti *social network* (tra gli altri, Facebook e Twitter, in base alla prima *designation decision* resa pubblica dalla Commissione)[49]

---

[46] L'art. 24 del DSA impone invero alle piattaforme online e ai motori di ricerca di pubblicare nella loro interfaccia online e comunicare al coordinatore dei servizi digitali del luogo di stabilimento e alla Commissione, su loro richiesta, le informazioni sul numero medio mensile di destinatari attivi del servizio, calcolato in conformità alle metodologie stabilite con atti delegati dalla Commissione stessa, fermo restando che, ai sensi dell'art. 33, la Commissione può comunque adottare la decisione circa la designazione di tali operatori come piattaforme o motori di ricerca 'di dimensioni molto grandi' sulla base di «qualsiasi altra informazione a sua disposizione», dovendo tuttavia in quest'ultimo caso garantire al *provider* una sorta di contradditorio preventivo, dandogli la possibilità di presentare il proprio parere in merito a tale decisione entro dieci giorni lavorativi. Si prevede, inoltre, che la Commissione adotti tali decisioni «previa consultazione dello Stato membro di stabilimento o tenuto conto delle informazioni fornite dal coordinatore dei servizi digitali del luogo di stabilimento a norma dell'articolo 24, paragrafo 4». La Commissione, infine, deve pubblicare sulla Gazzetta Ufficiale dell'Unione europea, e costantemente aggiornare, l'elenco degli operatori qualificati 'di dimensioni molto grandi', potendo porre fine alla designazione del *provider* come tale ove successivamente quest'ultimo non soddisfi più tale requisito quantitativo.

[47] L'art. 3 del DSA fornisce, alle lett. p) e q), le seguenti definizioni: «p) «destinatario attivo di una piattaforma online»: il destinatario del servizio che si è avvalso di una piattaforma online richiedendo alla piattaforma online di ospitare informazioni o esponendosi alle informazioni ospitate dalla piattaforma online e diffuse attraverso la sua interfaccia online; q) «destinatario attivo di un motore di ricerca online»: il destinatario del servizio che ha formulato una richiesta a un motore di ricerca online e si è esposto a informazioni indicizzate e presentate sulla sua interfaccia online».

[48] Cfr. nel dettaglio, anche per ogni ulteriore riferimento, il tezo saggio della presente sezione (di R. Sabia, *L'*enforcement *pubblico del* Digital Services Act *tra Stati membri e Commissione europea: implementazione, monitoraggio e sanzioni*). Che si tratti degli interlocutori più importanti in qualche misura è "dimostrato" anche dal fatto che ai sensi dell'art. 43 DSA la Commissione europea «addebita ai fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi un contributo annuale per le attività di vigilanza al momento della loro designazione a norma dell'articolo 33».

[49] In conformità al DSA, il 25 aprile 2023 la Commissione ha già provveduto a designare come di "dimensioni molto grandi" 2 motori di ricerca (Bing e Google Search) e 17 piattaforme (Alibaba

che, nel contrasto alla disinformazione, esercitano un ruolo assolutamente decisivo e che devono essere necessariamente chiamati dal decisore pubblico a svolgere un ruolo proattivo, come abbiamo cercato di argomentare già nei precedenti cicli della ricerca[50]. Ed è proprio quest'ultimo obiettivo quello che il DSA tenta qui di raggiungere, tramite una scelta di *policy* ben precisa: quella di puntare sugli stilemi, sui paradigmi, sugli strumentari ormai classici dell'era della *corporate compliance*, già sperimentati in qualche misura in altri regolamenti europei (spicca su tutti ovviamente, per importanza e contiguità con il DSA, il *General Data Protection Regulation*)[51].

Come subito vedremo, peraltro, il legislatore eurounitario sembra scommettere su tale scelta di politica del diritto in modo ancor più deciso, disciplinando con un particolare livello di dettaglio, per quanto qui interessa, i criteri di valutazione e gestione dei rischi, l'architettura dei sistemi e delle metodologie di controllo interno, i meccanismi di cooperazione pubblico-privato specie nella risposta alle crisi.

Si entra qui, insomma, nel "cuore pulsante" del regolamento, che ha a che fare con la gestione e la mitigazione dei "*systemic risks*" degli ambienti digitali moderni – per ciò che concerne, tra l'altro, i diritti fondamentali, la libertà di espressione, il pluralismo dei media, i diritti dei minori, l'integrità dei processi elettorali, la salute e la sicurezza pubblica – la cui valutazione e mitigazione viene affidata agli stessi operatori che generano simili rischi e alle dinamiche di cooperazione istituzionalizzata tra pubblico-privato, secondo modelli di regolazione, appunto, ormai consolidati in vari ordinamenti e in diversi settori di disciplina (si pensi all'ambiente, alla sicurezza sul lavoro, alla *privacy*)[52].

4.1. Obblighi di *risk assessment*

La prima *due diligence obligation* aggiuntiva per i detti operatori di "dimensioni molto grandi" riguarda l'obbligo di effettuare almeno una volta all'anno, nonché «in ogni caso prima dell'introduzione di funzionalità che possono avere un impatto critico», un *assessment* concernente l'individuazione, l'analisi e la valutazione «con diligenza» degli eventuali «rischi sistemici» derivanti dalla progettazione, dal funzionamento o dall'uso dei loro servizi e dei relativi sistemi (anche algoritmici).

L'art. 34 del DSA esige un'analisi specifica «e proporzionata ai rischi sistemici, tenendo in considerazione la loro gravità e la loro probabilità», che comprenda i seguenti "*systemic risks*": *a)* la diffusione di contenuti illegali tramite il proprio servizio; *b)* «eventuali effetti negativi, attuali o prevedibili» collegati alla propria attività e relativi all'esercizio di diritti fondamentali tra cui, tra l'altro, la tutela dei dati personali, la libertà di espres-

AliExpress; Amazon Store; Apple AppStore; Booking.com; Facebook; Google Play; Google Maps; Google Shopping; Instagram; LinkedIn; Pinterest; Snapchat; TikTok; Twitter; Wikipedia; YouTube; Zalando): cfr. *europa.eu/commission*.

[50] V. *supra* par. 1 per tutti i necessari rinvii. In argomento v. anche, da ultimo, le considerazioni di V. Zeno-Zencovich, *The EU regulation of speech. A critical view*, in questa *Rivista*, 1, 2023, 14.

[51] Da ultimo, per un confronto tra DSA e GDPR, v., anche per ogni ulteriore approfondimento, M. Iaselli, Digital Services Act *e* Privacy, in *Diritto di internet*, 1, 2023, 67 ss.

[52] V., per tutti, A. Gullo, voce *Compliance*, in G. Mannozzi - C. Perini - F. Consulich - C. Piergallini - M. Scoletta - C. Sotis (a cura di), *Studi in onore di Carlo Enrico Paliero*, Milano, 2022, 1289 ss.

sione e di informazione, inclusi il pluralismo dei media, la non discriminazione, i diritti del minore, la tutela dei consumatori[53]; *c)* eventuali effetti negativi «sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica»; *d)* qualsiasi incidenza non positiva in relazione «alla violenza di genere, alla protezione della salute pubblica e dei minori e alle gravi conseguenze negative per il benessere fisico e mentale della persona».
Si tratta, a ben vedere, non solo dei principali ambiti rispetto ai quali diversi *social media* già disciplinano *policy* interne più o meno articolate[54], ma anche di alcuni degli interessi sui quali la *misinformation* e le azioni (coordinate e non) di disinformazione possono più significativamente incidere, con la conseguenza che inevitabilmente piattaforme online e motori di ricerca "*very large*" saranno chiamati, secondo la predetta cadenza periodica, ad autovalutare attentamente il rischio che simili comportamenti possano essere compiuti nell'ambito dei propri servizi e, come vedremo tra poco[55], a farsi carico del delicato compito di introdurre misure per mitigare questi potenziali effetti negativi. Lo stesso considerando 84 del DSA, del resto, chiarisce come tali fornitori dovrebbero «prestare particolare attenzione al modo in cui i loro servizi sono utilizzati per diffondere o amplificare contenuti fuorvianti o ingannevoli, compresa la disinformazione».
Molto opportunamente, poi, il par. 2 dell'art. 34 del DSA detta ulteriori criteri per "guidare" e orientare correttamente tale *risk assessment*, nella misura in cui si esige che la valutazione in questione tenga conto «in particolare, dell'eventualità e del modo in cui i seguenti fattori influenzano uno dei rischi sistemici di cui al paragrafo 1: a) la progettazione dei loro sistemi di raccomandazione e di qualsiasi altro sistema algoritmico pertinente; b) i loro sistemi di moderazione dei contenuti; c) le condizioni generali applicabili e la loro applicazione; d) i sistemi di selezione e presentazione delle pubblicità; e) le pratiche del fornitore relative ai dati […]; [la] manipolazione intenzionale del loro servizio, anche mediante l'uso non autentico o lo sfruttamento automatizzato del servizio, nonché l'amplificazione e la diffusione potenzialmente rapida e ampia di contenuti illegali e di informazioni incompatibili con le condizioni generali»[56].
La centralità di questi aspetti, nel contrasto alla disinformazione, è di palmare evidenza. Anche nel corso dei precedenti cicli della ricerca[57], infatti, avevamo osservato come

[53] Nel dettaglio, l'art. 34, par. 1, lett. b) del DSA si riferisce a «eventuali effetti negativi, attuali o prevedibili, per l'esercizio dei diritti fondamentali, in particolare i diritti fondamentali alla dignità umana sancito nell'articolo 1 della Carta, al rispetto della vita privata e familiare sancito nell'articolo 7 della Carta, alla tutela dei dati personali sancito nell'articolo 8 della Carta, alla libertà di espressione e di informazione, inclusi la libertà e il pluralismo dei media, sanciti nell'articolo 11 della Carta, e alla non discriminazione sancito nell'articolo 21 della Carta, al rispetto dei diritti del minore sancito nell'articolo 24 della Carta, così come all'elevata tutela dei consumatori, sancito nell'articolo 38 della Carta».

[54] Abbiamo effettuato un'analisi di dettaglio di queste politiche in E. Birritteri, *Punire la disinformazione*, cit., 304 ss.

[55] Cfr. il paragrafo successivo.

[56] Si prevede altresì che «La valutazione tiene conto di specifici aspetti regionali o linguistici, anche laddove siano specifici di uno Stato membro. 3 I fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi conservano i documenti giustificativi delle valutazioni dei rischi per almeno tre anni dopo l'esecuzione delle valutazioni dei rischi e, su richiesta, li comunicano alla Commissione e al coordinatore dei servizi digitali del luogo di stabilimento».

[57] Cfr. *supra*, par. 1, per tutti i necessari rinvii rispetto ai temi qui di seguito menzionati. Ampiamente su tali profili v. recentemente A. Manganelli - A. Nicita, *Regulating Digital Markets. The European Approach*, Cham, 2022, 177 ss.

alcune caratteristiche specifiche del modello di business di tali *Big Tech* siano in grado di favorire la diffusione dei possibili effetti negativi che la condivisione di notizie false online può generare su interessi come l'integrità dei processi e delle consultazioni elettorali, la salute pubblica (si pensi alle molte informazioni false condivise in relazione al Covid-19), il pluralismo dei media. Ad esempio, come noto, i sistemi di raccomandazione tendono a riproporre all'utente contenuti sempre più in linea con la propria precedente attività in rete, con la conseguenza di innescare un continuo "bombardamento" nei suoi riguardi di contenuti falsi che lo hanno già in precedenza interessato – e che rischiano così di divenire rapidamente virali in rete con tutto ciò che di negativo può derivarne – o di *post* potenzialmente molto pericolosi per il suo benessere psicofisico (si pensi a utenti che tendono ad essere attratti, per uno stato depressivo, da informazioni relative ad atti di autolesionismo). Si può far riferimento, altresì, alle tecniche di manipolazione intenzionale del servizio (tra cui l'interazione artificiosa tra più *account* per aumentare in modo fraudolento la visibilità di certe notizie, o l'uso agli stessi fini di *bot* automatici e profili *fake*) spesso utilizzati in campagne coordinate di disinformazione. Ancora, palese è il richiamo, nel riferimento da parte dell'art. 34 del DSA alle modalità di moderazione dei contenuti e alla definizione delle condizioni generali d'uso del servizio, al rischio che una non equilibrata politica di articolazione di simili *policy* interne finisca per risolversi in una illegittima censura nell'ambito del libero confronto politico, e, in generale, in una forma di illecita interferenza sulla libertà di espressione di personaggi pubblici e cittadini.

Di qui l'impatto di tali realtà digitali sui menzionati diritti fondamentali e la necessità per le organizzazioni in questione di autovalutare con attenzione tali risvolti potenzialmente "perversi" dei loro sistemi e servizi.

Si tratta di una norma chiave che si pone l'obiettivo di sensibilizzare le piattaforme sull'esigenza di farsi carico degli interessi di tutti gli *stakeholder* che possono in qualche misura essere influenzati dalla loro attività, non potendo le esigenze di *business* e di profitto essere perseguite a discapito di tali diritti individuali e beni collettivi[58]. Ciò secondo un approccio sistematico e sfruttando la capacità organizzativa e di gestione di modelli di *compliance* e metodologie di analisi del rischio che simili grandi *corporation* certamente possiedono[59].

Sotto tale profilo, allora, ci pare che questa disposizione detti una condivisibile cornice pubblicistica di riferimento per una attività di *risk assessment* che appare oggi indispensabile e che, pur ponendo un significativo onere organizzativo e gestionale in capo a tali attori, sembra proporzionata alla loro "potenza di fuoco" sul mercato globale e un bilanciamento tutto sommato più che ragionevole tra i vari interessi contrapposti[60].

[58] Su tale esigenza con specifico riguardo alla lotta alla disinformazione v. ampiamente P. Severino, voce *Disinformazione*, in G. Mannozzi - C. Perini - F. Consulich - C. Piergallini - M. Scoletta - C. Sotis (a cura di), *Studi in onore di Carlo Enrico Paliero*, Milano, 2022, 1373 ss.

[59] In generale, sul tema dell'articolazione della *compliance* nelle realtà multinazionali, v. da ultimo in dettaglio S. Manacorda, *The "Dilemma" of Criminal Compliance for Multinational Enterprises in a Fragmented Legal Word*, in S. Manacorda - F. Centonze (a cura di), *Corporate Compliance on a Global Scale*, Cham, 2022, 67 ss. Sul punto v. anche V. Mongillo, *Presente e futuro della* compliance *penale*, in *sistema penale.it*, 11 gennaio 2022.

[60] In generale, sull'approccio del DSA in punto di bilanciamento tra i vari interessi contrapposti, v. G.

L'auspicio dei regolatori, tra l'altro, è che la possibilità per i soggetti regolati di essere esposti, in caso di non conformità con tali obblighi di *due diligence*, a sanzioni e meccanismi di *enforcement* potenzialmente molto efficaci[61], certamente stimolerà le c.d. VLOPs (*Very Large Online Platforms*) e i c.d. VLOSEs (*Very Large Online Search Engines*) ad effettuare tali valutazioni con serietà e significativo impegno, scongiurando la possibilità di legittimare forme di c.d. mera *cosmetic* o *paper compliance*[62].

4.2. Le previsioni in punto di mitigazione dei rischi

Il DSA disciplina naturalmente anche la fase conseguente al *risk assessment* effettuato ai sensi dell'art. 34, richiedendo alle piattaforme online e ai motori di ricerca di dimensioni molto grandi l'adozione di «misure di attenuazione ragionevoli, proporzionate ed efficaci, adattate ai rischi sistemici specifici individuati a norma dell'articolo 34, prestando particolare attenzione agli effetti di tali misure sui diritti fondamentali».
L'art. 35 contempla un elenco molto fitto di alcune possibili "*mitigation measures*", strettamente interconnesse agli ambiti di rischio identificati dall'art. 34, tra cui: l'adeguamento di progettazione, caratteristiche e funzionamento dei servizi, condizioni generali e correlato *enforcement*, sistemi algoritmici, di raccomandazione e pubblicità, interfacce online; misure di sensibilizzazione e l'adeguamento «delle procedure di moderazione dei contenuti, compresa la velocità e la qualità del trattamento delle segnalazioni concernenti tipi specifici di contenuti illegali e, se del caso, la rapida rimozione dei contenuti oggetto della notifica o la disabilitazione dell'accesso agli stessi, in particolare in relazione all'incitamento illegale all'odio e alla violenza online, nonché l'adeguamento di tutti i processi decisionali pertinenti e delle risorse dedicate alla moderazione dei contenuti»[63]; l'avvio o l'adeguamento della cooperazione con i *trusted flaggers* e l'attuazione delle decisioni degli organismi di risoluzione extragiudiziale delle controversie; la cooperazione con altre piattaforme o motori di ricerca sulla base di codici di condotta e protocolli di crisi *ex* art. 45 e 48 del DSA; misure a tutela dei minori come «strumenti di verifica dell'età e di controllo parentale, o strumenti volti ad aiutare i minori a segnalare abusi o ottenere sostegno»; misure specifiche afferenti, in sostanza, al fenomeno dei cc.dd. *deep fake*[64].

Caggiano, *La proposta di* Digital Services Act *per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, in *Annali AISDUE*, 1, 2021, 28.

[61] Cfr. ancora il terzo saggio della presente sezione monografica.

[62] Su tale nozione v., per tutti, V. Mongillo, *La responsabilità penale tra individuo ed ente collettivo*, Torino, 2018, 187 e 471.

[63] La lett. f) del par. 1 dell'art. 35 del DSA menziona anche, in generale, «il rafforzamento dei processi interni, delle risorse, della sperimentazione, della documentazione o della vigilanza sulle loro attività, in particolare per quanto riguarda il rilevamento dei rischi sistemici».

[64] In particolare, ai sensi dell'art. 35, par. 1, lett. k) del DSA, si tratta del «il ricorso a un contrassegno ben visibile per fare in modo che un elemento di un'informazione, sia esso un'immagine, un contenuto audio o video, generati o manipolati, che assomigli notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che a una persona appaia falsamente autentico o veritiero, sia distinguibile quando è presentato sulle loro interfacce online e, inoltre, la fornitura di una funzionalità di facile utilizzo che consenta ai destinatari del servizio di indicare tale informazione». Per un recente approfondimento del

Al di là di alcune indicazioni di maggiore dettaglio (ad es. in tema di azioni a tutela dei minori e di contrasto, come visto da ultimo, ai *deep fake*), quindi, il DSA menziona soltanto, per così dire, le macro-tipologie di misure che le piattaforme possono autonormare e adottare al fine di gestire e mitigare i rischi connessi all'impatto dei loro servizi sui detti diritti fondamentali e interessi individuali e collettivi. Ci si riferisce, insomma, all'adeguamento di certe *policy* o determinati processi, ma non si forniscono indicazioni più precise e puntuali su *come farlo*, sulle specifiche misure adottabili per conseguire l'obiettivo di risolvere le criticità delle procedure individuate in sede di valutazione del rischio. Il regolatore europeo, in linea con quanto si è visto accade anche rispetto ad altre disposizioni del regolamento, è sempre ben attento a non imporre agli operatori digitali particolari e dettagliate politiche sull'organizzazione e la gestione operativa dei loro servizi, lasciando loro, anche in tale sede, un ampio margine di apprezzamento.
La convinzione pare essere quella dell'impossibilità o comunque dell'inopportunità di fornire procedure e modelli di gestione "preconfezionati", positivizzando analiticamente le cautele imposte, e della necessità, piuttosto, di lasciare liberi i soggetti regolati di costruire autonomamente le proprie "regole interne" secondo una logica *taylor made*, fornendo indicazioni di scopo di carattere generale e qui, in qualche misura, anche una metodologia di analisi e un elenco di possibili contromisure e ambiti di rischio specifici da considerare, menzionando soltanto il *genus* di riferimento delle varie possibili "*effective mitigation measures*"[65].
La scelta finale e "di merito" circa le *policy* da adottare in concreto, quindi, spetterà sempre agli operatori, il che ci pare sia un tema molto significativo anche sul versante sanzionatorio, nella misura in cui il DSA, in tale ambito, potrà a rigore dirsi violato allorquando i soggetti regolati abbiamo in tutto o in parte omesso o non effettuato correttamente[66], secondo i predetti generali criteri metodologici di analisi e gestione, lo svolgimento delle attività di *risk assessment* e *management*, e non già, di per sé, per la (motivata) scelta di non adottare (o di adottare in un certo modo) le specifiche, singole misure di gestione del rischio, rispetto alla quale le *corporation* mantengono un autonomo potere decisorio; nell'introdurre l'elenco delle tipologie di politiche di mitigazione

tema cfr. M. Cazzaniga, *Una nuova tecnica (anche) per veicolare disinformazione: le risposte europee ai* deepfakes, in questa *Rivista*, 1, 2023, 170 ss.

[65] La dottrina ha quindi evidenziato come il DSA, in tal senso, adotti un approccio in qualche misura riportabile al concetto di *meta-regulation* o *enforced-self regulation*: v. N. Zingales, *The DSA as a Paradigm Shift for Online Intermediaries' Due Diligence*, in J. van Hoboke - J.P. Quintais - N. Appelman - R. Fahy - I. Buri - M. Straub (a cura di), *Putting the DSA into Practice. Enforcement, Access to Justice and Global Implications*, Berlino, 2023, 213-214, il quale, da un lato, evidenzia che «*This approach, which on the one hand leaves businesses with a significant amount of discretion in the implementation of regulatory principles, and on the other involves a process of continuous evaluation and monitoring of the results, has been called "metaregulation" or "enforced self-regulation": "meta" because one (macro) regulator oversees another (micro) regulator in their management of risk; "enforced" because, in case of inadequacy of the self-regulatory practices, the (macro) regulator has the power to take enforcement measures», e, dall'altro lato, che «while the shift to a metaregulatory model should be welcomed for enabling reflexive and adaptive regulation, we must also be weary of its risk of collapsing in the absence of well-resourced and independent institutions*». Per un inquadramento approfondito del fenomeno dell'autonormazione (e delle varie classificazioni operabili) in relazione al sistema penale v. la recente indagine monografica di D. Bianchi, *Autonormazione e diritto penale. Intersezioni, potenzialità, criticità*, Torino, 2022.

[66] Ad esempio, effettuando soltanto un'analisi molto vaga, sommaria e superficiale dei rischi legati, in generale, a un certo *business* digitale, senza tarare tale *assessment* sulle proprie specificità, sulle proprie concrete dinamiche operative, sui propri servizi, nella logica di una valutazione realmente *tailor made*.

dei rischi suggerite alle piattaforme, invero, il testo originale in inglese del DSA utilizza la chiara dicitura per cui «such measures *may*[67] include» (cioè possono, non devono).
Ai sensi dei parr. 2 e 3 dell'art. 35, ad ogni modo, le istituzioni europee potranno adottare periodicamente relazioni e orientamenti volti ad agevolare, secondo dinamiche flessibili e tali da assicurare anche consultazioni pubbliche con un coinvolgimento preventivo dei vari *stakeholder*, la diffusione delle *best practice* implementate nel settore e informazioni di rilievo circa i rischi sistemici più rilevanti, così da aiutare concretamente le piattaforme online e i motori di ricerca ad adeguarsi a tali obblighi di *compliance*, fornendo loro indicazioni ancor più puntuali sulle migliori strategie da attuare per conseguire gli obiettivi di prevenzione fissati dal regolamento[68].
L'auspicio, dunque, è che tale interazione tra disciplina normativa e orientamenti integrativi fornite dalle autorità di *enforcement*, che sembra in qualche misura ispirarsi a pratiche ampiamente sperimentate in molti ordinamenti specie con riferimento alla *corporate criminal liability*[69], possa delineare chiaramente le regole del gioco, alla luce del non facile compito qui assegnato dal DSA alle organizzazioni più importanti del mondo digitale. Specie nel settore del contrasto alla disinformazione, del resto, la costruzione e l'im-

[67] Corsivo nostro.

[68] In particolare, si prevede che «2. Il comitato, in cooperazione con la Commissione, pubblica relazioni annuali esaustive. Le relazioni comprendono gli elementi seguenti: a) individuazione e valutazione dei rischi sistemici più rilevanti e ricorrenti segnalati dai fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi o identificati mediante altre fonti di informazione, in particolare le informazioni fornite in conformità degli articoli 39, 40 e 42; b) le migliori pratiche che consentano ai fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi di attenuare i rischi sistemici individuati. Tali relazioni presentano i rischi sistemici suddivisi per Stato membro in cui si sono verificati e in tutta l'Unione, se del caso. 3. La Commissione, in cooperazione con i coordinatori dei servizi digitali, può emanare orientamenti sull'applicazione del paragrafo 1 in relazione a rischi concreti, con l'obiettivo specifico di presentare le migliori pratiche e raccomandare eventuali misure, tenendo debitamente conto delle possibili conseguenze di tali misure sui diritti fondamentali di tutte le parti interessate sanciti dalla Carta. Nell'elaborazione di tali orientamenti la Commissione organizza consultazioni pubbliche». Inoltre, ai sensi dell'art. 44 del DSA «1. La Commissione consulta il comitato e sostiene e promuove lo sviluppo e l'attuazione di norme volontarie fissate dai competenti organismi di normazione europei e internazionali almeno per quanto riguarda: a) la presentazione elettronica delle segnalazioni di cui all'articolo 16; b) modelli, progettazione e norme di processo per comunicare con i destinatari del servizio in modo facilmente fruibile sulle restrizioni derivanti dalle condizioni generali e sulle relative modifiche; c) la presentazione elettronica di segnalazioni da parte dei segnalatori attendibili a norma dell'articolo 22, anche per mezzo di interfacce di programmazione delle applicazioni; d) interfacce specifiche, comprese le interfacce di programmazione delle applicazioni, per agevolare il rispetto degli obblighi di cui agli articoli 39 e 40; e) le revisioni delle piattaforme online di dimensioni molto grandi e dei motori di ricerca online di dimensioni molto grandi a norma dell'articolo 37; f) l'interoperabilità dei registri della pubblicità di cui all'articolo 39, paragrafo 2; g) la trasmissione di dati tra intermediari pubblicitari a sostegno degli obblighi di trasparenza a norma dell'articolo 26, paragrafo 1, lettere b), c) e d); h) misure tecniche che consentano il rispetto degli obblighi in materia di pubblicità di cui al presente regolamento, compresi gli obblighi riguardanti i contrassegni ben visibili per la pubblicità e le comunicazioni commerciali di cui all'articolo 26; i) interfacce di scelta e presentazione delle informazioni sui principali parametri dei diversi tipi di sistemi di raccomandazione, conformemente agli articoli 27 e 38; j) norme per misure mirate a tutela dei minori online. 2. La Commissione sostiene l'aggiornamento delle norme alla luce degli sviluppi tecnologici e del comportamento dei destinatari dei servizi in questione. Le informazioni pertinenti relative all'aggiornamento delle norme devono essere disponibili al pubblico e facilmente accessibili».

[69] V. da ultimo l'approfondita indagine monografica di R. Sabia, *Responsabilità da reato degli enti e paradigmi di validazione dei modelli organizzativi. Esperienze comparate e scenari di riforma*, Torino, 2022.

plementazione di *policy* da parte delle piattaforme presuppone una complessa opera di bilanciamento tra diritti fondamentali individuali e collettivi tra loro contrapposti, per cui occorre che quella alle *Big Tech* private non sia una delega totalmente "in bianco", ma, al contrario, sia frutto di una strategia di gestione condivisa di tali rischi[70], sotto la guida dei decisori pubblici, anche e soprattutto alla luce dei rilevanti poteri sanzionatori che possono essere azionati in caso di omesso o non corretto adeguamento a tali obblighi di *due diligence* da parte di questi soggetti economici.

4.3. Il *crisis response mechanism*

L'art. 36 del DSA disciplina una procedura particolare destinata ad applicarsi, con riferimento a piattaforme online e motori di ricerca di dimensioni molto grandi, in condizioni di crisi definite espressamente come «circostanze eccezionali [che] comportano una grave minaccia per la sicurezza pubblica o la salute pubblica nell'Unione o in parti significative di essa». Il considerando 91 del regolamento fornisce, peraltro, alcuni esempi significativi, specificando che tali «crisi potrebbero derivare da conflitti armati o atti di terrorismo, compresi conflitti o atti di terrorismo emergenti, catastrofi naturali quali terremoti e uragani, nonché pandemie e altre gravi minacce per la salute pubblica a carattere transfrontaliero».

Si tratta, a ben vedere, di ambiti particolarmente sensibili proprio rispetto al contrasto alle campagne (coordinate e non) di disinformazione; in numerosissimi casi, infatti, le notizie false maggiormente virali circolate in rete, e tali da poter influire negativamente sui diritti collettivi e individuali in gioco (salute e sicurezza pubblica), hanno avuto ad oggetto proprio le crisi internazionali in questione[71]. Appare quindi chiaro, e di interesse per questa ricerca, il retroterra "socio-criminologico" di riferimento di tale previsione.

Ora, in queste situazioni, la disposizione in questione del DSA prevede che la Commissione europea, su raccomandazione del comitato europeo per i servizi digitali[72], possa

[70] V. l'introduzione alla presente ricerca di A. Gullo, *Contenuti, scopi e traiettoria della ricerca: le nuove frontiere della* compliance *nel mercato digitale*. Su tali profili, in relazione al DSA e con interessanti riferimenti alle indicazioni della giurisprudenza del Corte suprema federale tedesca, v. A. von Ungern-Sternberg, *Freedom of Speech goes Europe – EU Laws for Online Communication*, in A. von Ungern-Sternberg (a cura di), *Content Regulation in the European Union*, cit., 45; nello stesso volume cfr. anche il contributo di R. Janal, *Impacts of the Digital Services Act on the Facebook "Hate Speech" Decision by the German Federal Court of Justice*, 119 ss.

[71] Si veda da ultimo il caso studio – in corso di pubblicazione sul sito istituzionale del MAECI – del terzo ciclo della presente ricerca (*Narrazioni e strategie di propaganda nelle* community *filorusse*), dedicato proprio alla disamina dei fenomeni di disinformazione legati al recente conflitto armato in Ucraina, cui si rinvia per ogni riferimento. In argomento v. anche L. Ciliberti, Free flow of information – *Il contrasto alla disinformazione in tempi di guerra*, in questa *Rivista*, 2, 2022, 349 ss., e S. Lattanzi, *La lotta alla disinformazione nei rapporti tra Unione e Stati terzi alla luce del conflitto russo-ucraino*, ivi, 3, 2022, 158 ss.

[72] L'art. 61 del DSA stabilisce invero che «1. È istituito un gruppo consultivo indipendente di coordinatori dei servizi digitali per la vigilanza sui prestatori di servizi intermediari denominato «comitato europeo per i servizi digitali» («comitato»). 2. Il comitato fornisce consulenza ai coordinatori dei servizi digitali e alla Commissione conformemente al presente regolamento per conseguire gli obiettivi seguenti: a) contribuire all'applicazione coerente del presente regolamento e alla cooperazione efficace dei coordinatori dei servizi digitali e della Commissione nelle materie disciplinate dal presente regolamento;

adottare una decisione «che impone» a tali operatori di intraprendere una o più tra le seguenti azioni: *a)* una valutazione sull'eventualità e, in caso affermativo, sulla portata e sul modo in cui il funzionamento o l'uso dei propri servizi può, si legge letteralmente, «contribuire» a una delle suindicate minacce gravi per la sicurezza o la salute pubblica; *b)* l'individuazione e l'applicazione di una delle misure di attenuazione dei rischi sistemici pocanzi menzionate e definite dall'art. 35, o dall'art. 48, par. 2, del DSA – si tratta, in quest'ultimo caso, dei protocolli di crisi volontari che possono essere elaborati, sperimentati e applicati, sempre per far fronte a analoghe situazioni emergenziali, tra tali organizzazioni e la Commissione europea[73] –, così da «prevenire, eliminare o limitare tale contributo alla grave minaccia individuata»; *c)* una relazione alla Commissione in merito alle misure adottate e alle valutazioni effettuate nel corso dell'implementazione di tale meccanismo di risposta alla crisi[74].

b) coordinare e contribuire agli orientamenti e all'analisi della Commissione, dei coordinatori dei servizi digitali e di altre autorità competenti sulle questioni emergenti nel mercato interno in relazione alle materie disciplinate dal presente regolamento; c) assistere i coordinatori dei servizi digitali e la Commissione nella vigilanza sulle piattaforme online di dimensioni molto grandi».

[73] L'art. 48 nel dettaglio dispone che «1. Il comitato può raccomandare alla Commissione di avviare l'elaborazione, conformemente ai paragrafi 2, 3 e 4, di protocolli di crisi volontari per affrontare situazioni di crisi. Dette situazioni sono strettamente limitate a circostanze straordinarie che incidono sulla sicurezza pubblica o sulla salute pubblica. 2. La Commissione incoraggia e facilita i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi e, ove opportuno, i fornitori di altre piattaforme online o di altri motori di ricerca online a partecipare all'elaborazione, alla sperimentazione e all'applicazione di tali protocolli di crisi. La Commissione provvede affinché tali protocolli di crisi comprendano una o più delle misure seguenti: a) la ben evidenziata visualizzazione di informazioni sulla situazione di crisi fornite dalle autorità degli Stati membri o a livello di Unione o, a seconda del contesto della crisi, da altri organismi competenti affidabili; b) la garanzia che il fornitore di servizi intermediari designi uno specifico punto di contatto per la gestione delle crisi; ove opportuno, può trattarsi del punto di contatto elettronico di cui all'articolo 11 oppure, nel caso dei fornitori di piattaforme online di dimensioni molto grandi o di motori di ricerca online di dimensioni molto grandi, del responsabile della conformità di cui all'articolo 41; c) ove opportuno, l'adeguamento delle risorse destinate a garantire il rispetto degli obblighi di cui agli articoli 16, 20, 22, 23 e 35 alle esigenze che sorgono dalla situazione di crisi. 3. La Commissione coinvolge, se opportuno, le autorità degli Stati membri e può coinvolgere anche le istituzioni, gli organi e gli organismi dell'Unione nell'elaborazione, nella sperimentazione e nella supervisione dell'applicazione dei protocolli di crisi. Ove necessario e opportuno, la Commissione può coinvolgere anche le organizzazioni della società civile o altre organizzazioni competenti nell'elaborazione dei protocolli di crisi. 4. La Commissione mira a garantire che i protocolli di crisi definiscano chiaramente tutti gli elementi seguenti: a) i parametri specifici per determinare che cosa costituisca la specifica circostanza eccezionale che il protocollo di crisi intende affrontare e gli obiettivi che persegue; b) il ruolo dei singoli partecipanti e le misure che devono mettere in atto durante la fase preparatoria e in seguito all'attivazione del protocollo di crisi; c) una procedura chiara per stabilire quando debba essere attivato il protocollo di crisi; d) una procedura chiara per determinare il periodo durante il quale devono essere messe in atto le misure da adottare dopo l'attivazione del protocollo di crisi, periodo strettamente limitato a quanto necessario per far fronte alle specifiche circostanze eccezionali in questione; e) le garanzie necessarie per far fronte ad eventuali effetti negativi sull'esercizio dei diritti fondamentali sanciti dalla Carta, in particolare la libertà di espressione e di informazione e il diritto alla non discriminazione; f) una procedura per riferire pubblicamente in merito a tutte le misure adottate, alla loro durata e ai loro esiti, al termine della situazione di crisi. 5. Se ritiene che un protocollo di crisi non affronti efficacemente la situazione di crisi o non garantisca l'esercizio dei diritti fondamentali di cui al paragrafo 4, lettera e), la Commissione chiede ai partecipanti di rivedere tale protocollo, anche adottando misure supplementari». In argomento si veda anche la disamina effettuata nel capitolo 1 del presente report.

[74] In dettaglio, la lett. c) del par. 1 dell'art. 36 del DSA si riferisce alla predisposizione di «una relazione alla Commissione, entro una certa data o a intervalli regolari specificati nella decisione, in merito alle

Ai sensi del par. 3, occorre che le azioni richieste dalla Commissione siano «strettamente necessarie, giustificate e proporzionate» tenuto conto della gravità della minaccia in corso e delle implicazioni, specie per i diritti fondamentali di tutte le parti interessate, delle misure richieste; la Commissione dovrà inoltre indicare «un termine ragionevole entro il quale devono essere adottate le misure specifiche» in questione, anche considerandone l'urgenza e il tempo necessario per la loro preparazione e attuazione; è stabilito in ogni caso che le azioni richieste debbano essere «limitate a un periodo non superiore a tre mesi», eventualmente prorogabili dalla Commissione per un periodo non superiore a ulteriori tre mesi[75]. L'organo di *enforcement* europeo, poi, dovrà monitorare l'applicazione da parte dell'operatore delle misure in parola, avviando se del caso un "dialogo" con quest'ultimo per valutare l'efficacia di tali azioni e richiedendo eventualmente al soggetto regolato di riesaminarle, previa consultazione del Comitato, ferma restando la possibilità, in ogni caso, di revocare la decisione di applicare il meccanismo di risposta alla crisi tenendo conto dell'evoluzione (e specie della cessazione) della situazione emergenziale.

Emerge con chiarezza, tra le righe della disposizione, lo sforzo del legislatore eurounitario di bilanciare le esigenze contrapposte in gioco.

È evidente, invero, come vi sia la consapevolezza dell'attribuzione alla Commissione europea di poteri particolarmente significativi, che gli danno la possibilità di incidere significativamente, con un provvedimento "individuale" e di carattere certamente non poco invasivo, sull'esercizio delle attività di piattaforme online e motori di ricerca di dimensione molto grandi, imponendogli, in tempi molto stretti e con particolare urgenza, l'adozione di diverse misure che presuppongono ponderazioni difficili e scelte molto delicate e complesse alla luce del loro impatto sui diritti fondamentali, specie in simili situazioni d'emergenza. Non è del resto un caso che – tenuto conto delle possibili ripercussioni di tali procedure sia sui diritti delle *corporation* cui vengono richieste le azioni di risposta alla crisi, sia su quelli dei loro utenti che, "di rimbalzo", si troveranno a subire gli effetti dei provvedimenti emergenziali implementati dalle piattaforme e che possono risolversi in significative ingerenze sulla loro sfera giuridica – parte della dottrina abbia subito criticato la genericità e l'ampiezza dei presupposti in grado di inne-

valutazioni di cui alla lettera a), sul contenuto preciso, l'attuazione e l'impatto qualitativo e quantitativo delle misure specifiche adottate a norma della lettera b) e su qualsiasi altra questione connessa a tali valutazioni o misure, come specificato nella decisione».

[75] Il par. 4 dell'art. 36 prevede altresì che «4. A seguito dell'adozione della decisione di cui al paragrafo 1, la Commissione adotta, senza indebito ritardo, tutte le seguenti misure: a) notifica la decisione al fornitore o ai fornitori destinatari della decisione; b) rende la decisione disponibile al pubblico; e c) informa il comitato della decisione, lo invita a presentare il proprio parere e lo tiene informato di eventuali sviluppi successivi relativi alla decisione». In base ai parr. 7, 10 e 11 della medesima previsione, poi, «7. La Commissione monitora l'applicazione delle misure specifiche adottate a norma della decisione di cui al paragrafo 1 del presente articolo sulla base delle relazioni di cui alla lettera c) di tale paragrafo e di ogni altra informazione pertinente, comprese le informazioni che può richiedere a norma dell'articolo 40 o 67, tenendo conto dell'evoluzione della crisi. La Commissione riferisce periodicamente al Comitato in merito a tale monitoraggio, almeno una volta al mese. […] 10. La Commissione tiene nella massima considerazione le raccomandazioni del comitato a norma del presente articolo. 11. La Commissione riferisce al Parlamento europeo e al Consiglio una volta all'anno a seguito dell'adozione di decisioni di cui al presente articolo e, in ogni caso, tre mesi dopo la fine della crisi, in merito all'applicazione delle misure specifiche adottate a norma di tali decisioni».

scare il potere della Commissione di applicare la disposizione in questione[76]. Si pensi, ad esempio, rispetto ai temi della presente ricerca e per meglio chiarire i termini problematici della questione, alla possibilità di applicare tale istituto per "reagire" a campagne di disinformazione su larga scala in occasione di conflitti armati internazionali o pandemie e altre crisi sanitarie gravi, con la richiesta alle piattaforme di modificare le loro condizioni generali d'uso del servizio, con l'effetto di impedire agli utenti di condividere determinate notizie circa lo scontro armato o la minaccia per la salute pubblica in corso; il rischio di forme di indebita censura e di compressione di fondamentali libertà democratiche è in queste ipotesi, evidentemente, tutt'altro che secondario.

Di qui, come forme di *counterbalance*, sia la decisione di perimetrare in un arco temporale molto circoscritto la possibilità di dar corso a tali meccanismi, sia l'importante indicazione di cui al par. 5 dell'art. 36, a tenore del quale la «scelta delle misure specifiche da adottare a norma del paragrafo 1, lettera b), e del paragrafo 7, secondo comma, spetta al fornitore o ai fornitori destinatari della decisione della Commissione»[77]. In linea con un approccio, come visto, che costituisce la cifra dell'intero regolamento, ci pare che tale locuzione debba essere interpretata nel senso che la Commissione possa imporre, nella propria decisione, soltanto l'adozione di un certo e ampio *genus* di misure (ad es., l'adeguamento dei sistemi di raccomandazione delle notizie, oppure delle condizioni generali o delle procedure di moderazione dei contenuti), dovendo essere lasciate al libero apprezzamento del soggetto regolato, in ultima istanza, la costruzione e l'attuazione specifica della *policy*, della misura di dettaglio da adottare, la scelta su "come mettere a terra" concretamente le modifiche delle proprie regole autonormate, senza che i poteri di ingerenza dell'organo pubblico europeo possano spingersi fino a obbligare gli attori privati ad adottare misure "predeterminate", escludendo qualsiasi margine di scelta su come implementare e integrare il tipo di provvedimenti richiesti all'interno del proprio contesto operativo interno.

[76] V. in particolare V. Colarocco - M. Cogode, *Gli obblighi applicabili a piattaforme* online *di dimensioni molto grandi (Artt. 33-43 – Capo III, Sezione 5)*, in *Diritto di internet*, 1, 2023, 32, ove si è osservato che «Le decisioni che riguardano la libertà di espressione e l'accesso alle informazioni, in particolare in tempi di crisi, non possono essere legittimamente prese dal solo potere esecutivo ma occorre un controllo parlamentare sull'esistenza e sulla durata della situazione emergenziale al fine di evitare abusi. La definizione di crisi deve, infatti, soddisfare i principi di chiarezza e specificità e non deve autorizzare la Commissione a mantenere misure di crisi per un periodo prolungato o indefinito. La definizione dovrebbe quindi, nella concreta interpretazione che ne verrà fornita, essere limitata alle minacce che sono in grado di destabilizzare seriamente le strutture costituzionali, politiche, economiche o sociali fondamentali dell'Unione o parti significative di esse. E il meccanismo proposto dovrebbe, a sua volta e per logica conseguenza, prevedere un ruolo più centrale degli organi rappresentativi dei cittadini, sottraendo all'esecutivo il potere unilaterale di limitare in modo quasi permanente l'accesso del pubblico alle informazioni e alla loro diffusione».

[77] Il par. 1 della stessa disposizione prevede altresì che «Nell'individuare e applicare le misure di cui alla lettera b) del presente paragrafo, il prestatore o i prestatori di servizi tengono debitamente conto della criticità della grave minaccia di cui al paragrafo 2, dell'urgenza delle misure e delle implicazioni effettive o potenziali per i diritti e gli interessi legittimi di tutte le parti interessate, compresa l'eventuale inosservanza dei diritti fondamentali sanciti dalla Carta».

4.4. L'*independent audit*

L'art. 37 del DSA, facendo propria una tipica metodologia della *corporate compliance*, sancisce l'obbligo per le piattaforme online e i motori di ricerca di dimensioni molto grandi di sottoporsi, a proprie spese «e almeno una volta all'anno», a *independent audit*[78] – effettuati da organizzazioni che soddisfino requisiti di indipendenza, comprovata esperienza, obiettività e deontologia professionale dettagliatamente normati dal par. 3 della disposizione[79] – volti a valutare la conformità dell'organizzazione: «a) agli obblighi stabiliti al capo III; b) agli impegni assunti a norma dei codici di condotta di cui agli articoli 45 e 46 e dei protocolli di crisi di cui all'articolo 48».

Al termine dell'attività di revisione, tali organismi redigeranno una relazione finale, che conterrà un giudizio circa il rispetto, da parte del soggetto regolato, dei detti obblighi stabiliti dal regolamento.

L'esito finale di tale revisione, in particolare, potrà essere «positivo», «positivo con osservazioni», o «negativo», in questi ultimi due casi dovendosi naturalmente fornire «raccomandazioni operative su misure specifiche per conseguire la conformità e sui tempi raccomandati per conseguirla»[80], con l'obbligo per le organizzazioni in questione

[78] La previsione fornisce naturalmente ulteriori dettagli sia rispetto agli obblighi di cooperazione delle piattaforme nello svolgimento delle revisioni, sia con riferimento alla trasparenza e agli aspetti di riservatezza e segreto professionale correlati a tali attività, stabilendo in particolare al par. 2 che «I fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi consentono alle organizzazioni che effettuano le revisioni a norma del presente articolo la cooperazione e l'assistenza necessarie per consentire loro di svolgere tali revisioni in modo efficace, efficiente e tempestivo, anche provvedendo a dare loro accesso a tutti i dati e ai locali pertinenti, e rispondendo a domande orali o scritte. Essi si astengono dall'ostacolare, influenzare indebitamente o compromettere lo svolgimento della revisione. Dette revisioni garantiscono un adeguato livello di riservatezza e il segreto professionale per quanto riguarda le informazioni ottenute dai fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi e da terzi nel contesto delle revisioni, anche dopo la loro conclusione. Tuttavia, il rispetto di tale obbligo non deve pregiudicare l'esecuzione delle revisioni e delle altre disposizioni del presente regolamento, in particolare quelle in materia di trasparenza, vigilanza ed esecuzione. Se necessario ai fini della relazione sulla trasparenza a norma dell'articolo 42, paragrafo 4, la relazione di revisione e la relazione di esecuzione della revisione di cui ai paragrafi 4 e 6 del presente articolo sono accompagnate dalle versioni prive di informazioni che potrebbero essere ragionevolmente considerate riservate».

[79] Ove è stabilito che «Le revisioni effettuate a norma del paragrafo 1 sono eseguite da organizzazioni: a) indipendenti e in assenza di conflitti di interessi con il fornitore di piattaforme online di dimensioni molto grandi o di motori di ricerca online di dimensioni molto grandi in questione, e con qualsiasi persona giuridica connessa con tale fornitore; in particolare: i) non devono aver fornito servizi diversi dalla revisione relativi alle questioni sottoposte a revisione al fornitore della piattaforma online di dimensioni molto grandi interessata o del motore di ricerca online di dimensioni molto grandi in questione e a qualsiasi persona giuridica collegata a tale fornitore nei 12 mesi precedenti l'inizio della revisione, e devono essersi impegnati a non fornire tali servizi nei 12 mesi successivi al completamento della revisione; ii) non devono aver fornito servizi di revisione a norma del presente articolo al fornitore della piattaforma online di dimensioni molto grandi interessata o del motore di ricerca online di dimensioni molto grandi in questione e a qualsiasi persona giuridica collegata a tale fornitore per un periodo superiore a dieci anni consecutivi; iii) non possono effettuare la revisione a fronte di corrispettivi che dipendono dall'esito dello stesso; b) sono dotate di comprovata esperienza nel settore della gestione dei rischi, di competenze e di capacità tecniche; c) sono dotate di comprovata obiettività e deontologia professionale, basata in particolare sull'adesione a codici di condotta o standard appropriati».

[80] In dettaglio i parr. 4 e 5 dell'art. 37 del DSA prevedono che «4. I fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi provvedono affinché le organizzazioni che effettuano le revisioni redigano una relazione per ciascuna revisione. Tale relazione

di tener «debitamente conto» di queste ultime e di adottare, entro «un mese dal ricevimento di tali raccomandazioni» una «relazione di attuazione della revisione con cui stabiliscono tali misure» oppure forniscono adeguata giustificazione delle ragioni per cui ritengono di non darvi corso, descrivendo, tuttavia, le «misure alternative» adottate per risolvere tutte le "*instances of non-compliance*" che siano state identificate[81]. Quest'ultima specificazione, in particolare, costituisce l'ennesima conferma della scelta del legislatore eurounitario di non imporre mai l'adozione di specifiche *policy* di dettaglio, lasciando sempre alle piattaforme la decisione definitiva sulle modalità concrete di adempimento ai doveri di *due diligence* loro imposti.

Si tratta, in definitiva, di una disposizione "di chiusura" che, unitamente all'art. 41 del DSA relativo all'istituzione di una specifica *compliance function* aziendale, sul quale subito ci soffermeremo[82], completa il novero degli obblighi gravanti sui grandi *player* del mercato digitale, chiamati a confrontarsi con organismi indipendenti esterni in merito alla correttezza del proprio apparato rispetto a quanto richiesto dal nuovo regolamento europeo. È un ulteriore *step* di una strategia di regolazione volta a garantire il più possibile l'effettività e la correttezza del *private enforcement* di operatori il cui impegno proattivo sarà essenziale per consentire il raggiungimento degli obiettivi della riforma[83].

è motivata per iscritto e contiene almeno gli elementi seguenti: a) il nome, l'indirizzo e il punto di contatto del fornitore della piattaforma online di dimensioni molto grandi o del motore di ricerca online di dimensioni molto grandi oggetto della revisione e il periodo di riferimento della revisione; b) il nome e l'indirizzo dell'organizzazione o delle organizzazioni che eseguono la revisione; c) una dichiarazione di interessi; d) una descrizione degli elementi specifici sottoposti a revisione e della metodologia applicata; e) una descrizione e una sintesi delle principali constatazioni derivanti dalla revisione; f) un elenco delle parti terze consultate nel quadro della revisione; g) un giudizio di revisione sul rispetto, da parte del fornitore della piattaforma online di dimensioni molto grandi o del motore di ricerca online di dimensioni molto grandi oggetto della revisione, degli obblighi e degli impegni di cui al paragrafo 1, giudizio che può essere segnatamente «positivo», «positivo con osservazioni» o «negativo»; h) se il giudizio di revisione non è «positivo», raccomandazioni operative su misure specifiche per conseguire la conformità e sui tempi raccomandati per conseguirla. 5. Qualora l'organizzazione che ha effettuato la revisione non abbia potuto verificare determinati elementi specifici o esprimere un giudizio di revisione sulla base delle proprie indagini, la relazione di revisione include una spiegazione delle circostanze e dei motivi per cui tali elementi non hanno potuto essere sottoposti a revisione».

[81] Ai sensi del par. 7 dell'art. 37 del DSA, peraltro, e in linea con altre analoghe previsioni del regolamento, viene conferito alla Commissione europea «il potere di adottare atti delegati conformemente all'articolo 87 al fine di integrare il presente regolamento stabilendo le norme necessarie per lo svolgimento delle revisioni a norma del presente articolo, in particolare per quanto riguarda la regolamentazione necessaria per le fasi procedurali, le metodologie di revisione e i modelli di comunicazione delle revisioni effettuate a norma del presente articolo. Tali atti delegati tengono conto di eventuali standard di revisione volontari a norma dell'articolo 44, paragrafo 1, lettera e)».

[82] Cfr. il paragrafo successivo.

[83] In dottrina, ad ogni modo, non si è mancato di identificare alcuni possibili rischi, nella misura in cui «*VLOPs may leverage their market power against their new mandatory auditors and risk assessors, a threat theorised as 'audit capture'*»: cfr. J. Laux - S. Wachter - B. Mittelstadt, *Taming the few: Platform regulation, independent audits, and the risks of capture created by the DMA and DSA*, in *Computer Law & Security Review*, 1, 2021, 43.

4.5. L'istituzione di una specifica funzione aziendale di *compliance* per monitorare la conformità dell'organizzazione agli obblighi del DSA

L'art. 41 del DSA, come anticipato, "chiude" il cerchio degli obblighi aggiuntivi gravanti sulle piattaforme online e sui motori di ricerca di dimensioni molto grandi, stabilendo che questi ultimi debbano istituire una specifica *compliance function* al fine di monitorare la conformità dell'organizzazione agli obblighi sanciti dal nuovo regolamento; dovrà trattarsi di una articolazione societaria indipendente dalle funzioni operative, composta da uno o più "*compliance officer*s", compreso l'*head* di tale "ufficio" (quale figura che in qualche modo si 'ispira' a quella del DPO in ambito *privacy*).
La previsione in questione, in linea con le consolidate *best practice* in tema di *corporate governance*, delinea una funzione di controllo a diretto riporto dell'organo di gestione, composta, quanto all'*head*, da un «un alto dirigente indipendente con responsabilità distinta per la funzione di controllo della conformità», nonché, quanto ad ogni altro componente, da soggetti in possesso delle «qualifiche professionali, delle conoscenze, dell'esperienza e delle capacità necessarie».
L'organo di gestione manterrà la responsabilità ultima in ordine alla approvazione e al riesame periodico delle strategie di valutazione, gestione e monitoraggio dei rischi (in particolare quelli di cui all'art. 34 del DSA), nonché rispetto alla costruzione di sistemi di *governance* che garantiscano, anche tramite la separazione delle responsabilità e la prevenzione dei conflitti di interesse, l'indipendenza della funzione di DSA *compliance* e l'assegnazione ai relativi *officer* di risorse, *status* e poteri necessari per adempiere alle proprie funzioni[84].
I compiti di tale funzione di *compliance* consistono, appunto, nel vigilare sul rispetto da parte della *corporation* delle *obligation* sancite dal DSA. In particolare, tale organismo sarà chiamato a: collaborare con il coordinatore dei servizi digitali del luogo di stabilimento e con la Commissione; assicurare il corretto svolgimento delle attività di *risk assessment* e *management* di cui agli artt. 34 e 35 del DSA; organizzare e sovraintendere agli adempimenti connessi agli *independent audit* di cui all'art. 37; informare e consigliare i dirigenti e i dipendenti dell'organizzazione in merito agli obblighi del regolamento ed esercitare un ruolo di impulso nei confronti dell'organo di gestione rispetto a tutte le questioni connesse alla DSA *compliance*; monitorare la conformità agli obblighi connessi ai codici di condotta e ai protocolli di crisi *ex* artt. 45 e ss. del DSA.
A fronte dell'inesistenza di un *dovere generale* per le società di istituire una simile funzione societaria, come noto resa obbligatoria esclusivamente in specifici ambiti settoriali[85], è quindi molto significativo notare come il legislatore europeo abbia scelto qui di rendere cogente la sua costituzione, con una decisione che è del resto in linea, come detto, con le *policy* fatte proprie da fonti normative analoghe; la presenza di un punto

[84] Si prevede, inoltre, che l'*head* della funzione di *compliance* non possa essere rimosso senza previa approvazione dell'organo di gestione e l'obbligo per i soggetti di regolati di comunicare nominativo e riferimenti di tale soggetto al coordinatore dei servizi digitali del luogo di stabilimento e alla Commissione europea.

[85] Cfr. chiaramente, ad esempio, l'art. 7 del Codice di autodisciplina delle società quotate italiane, reperibile in *borsaitaliana.it*.

di riferimento unico all'interno dell'organizzazione, che sovraintenda alle varie attività di controllo della conformità, e svolga un ruolo di impulso e di coordinamento complessivo dei correlati adempimenti, facendo da "collettore" delle varie istanze, è invero giustamente considerata un passaggio essenziale di completamento della disciplina, a presidio della sua efficacia.

Sarà, per il resto, importante verificare come la prassi si orienterà rispetto all'organizzazione e al funzionamento concreto della funzione di DSA *compliance*.

Due ci sembrano gli aspetti più rilevanti.

Anzitutto, la lettera del regolamento consente espressamente di scegliere tra una composizione monocratica o collegiale. Se da un lato una maggiore flessibilità può sembrare apprezzabile, di contro è molto difficile ipotizzare che, nel contesto di *corporation* di "dimensioni molto grandi", un unico funzionario possa assicurare uno svolgimento realmente efficace dei compiti assegnati a tale articolazione in organizzazioni complesse con una considerevole mole di utenti e, quindi, di *workflow*. Ci sembra sia preferibile allora, quantomeno di regola, optare per la nomina di plurimi responsabili, in numero adeguato alle specificità di ogni operatore.

In secondo luogo, in base la lettera del regolamento non è chiaro se debba trattarsi di un organismo da istituire totalmente *ex novo*, o se le responsabilità definite dall'art. 41 DSA possano essere assegnate a o uno o più componenti delle funzioni di *compliance* eventualmente già esistenti nelle organizzazioni (come è molto probabile che sia in enti di questo tipo), sempre, naturalmente, a condizione che tali uffici e i loro singoli membri – che la piattaforma voglia designare come DSA *compliance officer* – soddisfino i predetti requisiti delineati dal nuovo regolamento europeo. Il testo originale, che utilizza la locuzione «*shall establish*» ("istituiscono" nella traduzione italiana), non pare offrire certezze in merito, pur sembrando maggiormente "evocare"[86], almeno a livello strettamente letterale, la creazione di una nuova struttura. Tuttavia, a noi pare sia ragionevole (e conforme alla *ratio* del regolamento[87]) considerare legittima la seconda soluzione, se del caso costruendo un *team* "*ad hoc*" all'interno dell'ufficio già presente, anche per assicurare una ragionevole allocazione delle risorse organizzative e finanziarie e lo sfruttamento di quelle già esistenti, nell'ottica di una *compliance* realmente integrata quale approccio ormai indispensabile in uno scenario regolatorio sempre più complesso e variegato per i soggetti metaindividuali.

5. Riflessioni conclusive e indicazioni di *policy*

Il DSA è riuscito a colmare una significativa lacuna che caratterizzava lo scenario normativo europeo e di diversi Stati membri, in un panorama regolamentare in cui si erano iniziate ad affacciare, a "macchia di leopardo" e in singoli ordinamenti, iniziati-

[86] A conclusioni diverse si sarebbe senza alcun dubbio giunti nel caso di utilizzo di termini più neutri come "designare" o "nominare" ("*appoint*" in lingua inglese).

[87] Del resto, ciò in qualche modo potrebbe contribuire anche a chiarire la ragione per cui il DSA consente di nominare anche un solo responsabile della conformità.

ve legislative parziali[88], che toccavano solo alcuni punti dei profili poi organicamente ricondotti ad unità dalla nuova normativa eurounitaria; ciò anche con riferimento alla responsabilizzazione degli operatori digitali nelle attività di autonormazione e auto-organizzazione che abbiamo descritto in questa parte della ricerca. Ed è peraltro molto importante che ci si sia fatti carico di risolvere tale *gap* mediante un regolamento europeo, trattandosi di uno strumento per definizione più adatto a disciplinare un fenomeno, afferente ai più importanti modelli di *business* digitali, per sua natura transnazionale e che necessita, inevitabilmente, di risposte di pari respiro e non già esclusivamente "locali".

Anche solo guardando alla situazione immediatamente precedente l'approvazione del DSA, quindi, si può essere soddisfatti dei risultati raggiunti. La sensazione è quella di essere di fronte a un prodotto normativo di buona fattura, pure al netto di alcune criticità che abbiamo cercato di porre in evidenza e che forse, in fin dei conti, sono del tutto comprensibili in un atto legislativo che è stato giustamente ed efficacemente definito come "pioneristico"[89]. Insomma, si tratta di un percorso in cui, nel complesso, le luci prevalgono sulle ombre.

Giunti alla fine di questo contributo, non resta allora che tentare di fornire alcune indicazioni di *policy* che confluiranno nel documento contenuto in calce allo studio in cui, come per gli scorsi cicli della ricerca, avremo cura di tesaurizzare i risultati delle indagini condotte nelle varie sezioni in cui è stata articolata la nostra disamina del DSA, costruendo un prospetto unitario di raccomandazioni rivolte ai vari attori del settore.

Procediamo con ordine, ripercorrendo nella stessa "direzione di marcia" fin qui seguita i vari temi di cui ci siamo occupati in questo lavoro e cercando di isolare le questioni maggiormente importanti dall'angolo visuale del contrasto alla disinformazione.

Quattro sono gli aspetti su cui, a nostro avviso, occorre concentrare l'attenzione.

Un primo tema attiene alla definizione di termini e condizioni del servizio (c.d. standard della *community*). Qui, come visto[90], le piattaforme dovrebbero rafforzare l'apparato di garanzie minime definito dall'art. 14, disciplinando l'esercizio dei propri poteri "sanzionatori" nel rispetto di diritti essenziali che devono necessariamente essere riconosciuti nell'implementazione di qualsiasi paradigma punitivo, anche in ambito privato: la legalità delle violazioni e delle misure sanzionatorie/interdittive, con i corollari della irretroattività, della tassatività/precisione delle previsioni punitive e del divieto di analogia; la dettagliata definizione dei soggetti titolari della potestà di dettare tali regole; il principio di proporzionalità del trattamento sanzionatorio; il divieto di responsabilità oggettiva e l'affermazione del principio di colpevolezza, etc.

Per ciò che concerne nello specifico la strutturazione di *policy* anti-disinformazione può essere rischioso e controproducente limitarsi a prevedere un generale divieto per

[88] Cfr. *supra* par. 1. Per un'analisi che ha messo in evidenza tale evoluzione del panorama normativo europeo, anche con richiami ad alcuni «*worrying trends toward criminalisation*», v. R. Ò Fathaigh - N. Helberger - N. Appelman, *The perils of legally defining disinformation*, in *Internet Policy Review*, 10(4), 2021, 2 ss.

[89] V. l'introduzione alla presente ricerca di A. Gullo, *Contenuti, scopi e traiettoria della ricerca*, cit. Non a caso in dottrina si è rilevato come «*the DSA is likely to shape the global approach to content regulation in this emerging area of law*»: cfr. P. Church - C.N. Pehlivan, *The Digital Services Act (DSA): A New Era for Online Harms and Intermediary Liability*, in *Global Privacy Law Review*, 4(1), 2023, 53 ss.

[90] Cfr. *supra* par. 1.1.

gli utenti, invero troppo ampio e indeterminato, di condivisione di notizie false. La difficoltà, come sappiamo[91], di segnare un preciso confine tra esternazioni di fatti e opinioni personali, oggettivo e soggettivo, vero e falso, finirebbe per rendere tale "regola interna" difficilmente attuabile dai soggetti chiamati, all'interno dell'organizzazione, a moderare i contenuti immessi in rete dagli utenti e, soprattutto, per risolversi in molti casi in una indebita compressione della libertà di espressione dei destinatari del servizio.

Nella strutturazione di *term and conditions*, da tale specifica prospettiva, occorre allora introdurre divieti ben circostanziati, circoscritti, tassativi, con un approccio *case by case* e procedendo per singoli settori sensibili, vietando, ad esempio, l'intenzionale condivisione di notizie obiettivamente qualificabili come non vere per cui si riportino inesistenti difficoltà di accesso ai seggi elettorali o nelle operazioni di voto, con l'obiettivo di disincentivare le persone a recarsi alle urne e ledendo quindi l'interesse all'integrità ai processi elettorali, o notizie di analogo tenore volte ad arrecare pregiudizio a campagne vaccinali a tutela della salute pubblica, e così via.

Ancora, non dovrebbero essere consentite, a prescindere dal contenuto della notizia condivisa (e dalla sua veridicità), specifiche modalità decettive di utilizzo del servizio come l'interazione artificiosa tra più *account* o l'uso di *bot* automatici al fine di aumentare fraudolentemente la visibilità di certe informazioni.

I settori sensibili nei quali disciplinare e applicare tali politiche interne di gestione del servizio, inoltre, andrebbero identificati tramite un'analisi dei rischi svolta secondo i criteri di cui all'art. 34 DSA, le cui indicazioni di metodo dovrebbero essere seguite anche da piattaforme e motori di ricerca non qualificati come organizzazioni di "dimensioni molto grandi", pur, naturalmente, tenendo conto delle proprie specificità operative e organizzative e adattando di conseguenza i detti principi di *assessment*. Bisognerà poi coordinare la costruzione di tali standard della *community* con le conseguenti misure di mitigazione del rischio anche sul versante tecnico[92], tra cui la riduzione della visibilità o la c.d. demonetizzazione dei contenuti, la revisione dei sistemi di raccomandazione e pubblicità per evitare che dette informazioni diventino virali, l'utilizzo di contrassegni ben visibili per consentire agli utenti di identificare chiaramente i c.d. *deep fake* (e per dare la possibilità agli autori di *post* che li immettano in rete di indicare chiaramente la loro natura "falsa"[93]), unitamente a ogni altro accorgimento, sul piano del funzionamento concreto del servizio, indispensabile per rendere tale *enforcement* realmente efficace.

Una seconda questione concerne i meccanismi di *notice and action*: abbiamo infatti rile-

[91] Per una più ampia disamina, e altri riferimenti bibliografici, sia consentito rinviare ancora a E. Birritteri, *Punire la disinformazione*, cit., 304 ss.

[92] Per un inquadramento di queste misure, con particolare riferimento ai filtri tecnici, v. M. Steinebach, *Potential and Limits of Filter Technology for the Regulation of Hate Speech and Fake News*, in A. von Ungern-Sternberg (a cura di), *Content Regulation in the European Union*, cit., 13 ss.

[93] L'art. 35, par. 1, lett. k), del DSA si riferisce, come abbiamo già evidenziato, al ricorso «a un contrassegno ben visibile per fare in modo che un elemento di un'informazione, sia esso un'immagine, un contenuto audio o video, generati o manipolati, che assomigli notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che a una persona appaia falsamente autentico o veritiero, sia distinguibile quando è presentato sulle loro interfacce online e, inoltre, la fornitura di una funzionalità di facile utilizzo che consenta ai destinatari del servizio di indicare tale informazione».

vato[94] che rispetto al contrasto alla disinformazione diversi contenuti o modalità d'utilizzo del servizio non possono spesso dirsi di per sé illegali; di conseguenza, le piattaforme online dovrebbero rendere disponibili i propri sistemi interni di segnalazione anche per l'invio di report che evidenzino semplicemente l'incompatibilità del contenuto con i c.d. standard della *community* (e in particolare con le *policy* dettate in materia di condivisione di notizie false).

Un terzo punto cruciale riguarda i sistemi interni di gestione dei reclami, trattandosi di un profilo particolarmente delicato dell'*enforcement* privato delle politiche anti-disinformazione, alla luce della tensione che inevitabilmente si genera tra esse e il rispetto della libertà di espressione. Per tali ragioni, anche in tal caso a nostro avviso è necessario che le piattaforme assicurino un livello maggiore di garanzie rispetto a quello minimo richiesto dagli artt. 17 e 20 del DSA, assicurando agli utenti, tra l'altro, un pieno contraddittorio preventivo, la garanzia di sufficiente autonomia e indipendenza (con riferimento alla distribuzione dei poteri dell'organizzazione) dei soggetti deputati a irrogare la sanzione e a decidere sui connessi reclami, il diritto di richiedere il riesame della decisione già a livello interno[95].

Un ultimo aspetto, infine, è quello legato al rafforzamento degli strumenti di monitoraggio continuo dell'efficacia dell'apparato di DSA *compliance* realizzato da queste organizzazioni[96], essendo auspicabile che anche piattaforme e motori di ricerca non designati come operatori "di dimensioni molto grandi" nominino *compliance officer* dedicati e si sottopongano, ove possibile, ad *audit* interni ed esterni indipendenti su base volontaria, pur con un approccio improntato a un'ampia flessibilità e alla possibilità di modellare gli adempimenti alla luce delle proprie specificità. Considerata la natura estremamente sensibile di tali pratiche di autonormazione, e per certi versi anche l'indubbia difficoltà di implementare una strategia di contrasto alla disinformazione, infatti, appare essenziale non soltanto avvalersi di figure incaricate di monitorare la conformità dell'organizzazione agli obblighi del DSA, e la loro efficace attuazione, ma anche favorire un proficuo confronto tra la *corporation* e i vari attori del sistema, dal momento che solo una ampia e costante cooperazione tra i diversi *stakeholder* potrà realmente assicurare il raggiungimento degli obiettivi che questa ambiziosa riforma ha cercato di conseguire all'esito di un difficile bilanciamento di tutti gli interessi in gioco.

[94] Cfr. *supra* par. 2.1.

[95] V. anche *supra* par. 3.1.

[96] Cfr. *supra* parr. 4.4 e 4.5.