# Come individuare e contrastare operazioni coordinate di disinformazione in Italia.

## Casi di studio e indicazioni di *policy* per istituzioni pubbliche e private

terzo ciclo di ricerca

**Come individuare e contrastare operazioni coordinate di disinformazione in Italia.**
Casi di studio e indicazioni di *policy* per istituzioni pubbliche e private

**Direzione della Ricerca:**

**Antonio Gullo**, Direttore della Ricerca per la parte legale e cybersecurity, Luiss Guido Carli
**Irene Pasquetto**, Direttore della Ricerca per la parte di research design, media e disinformazione, Harvard Kennedy School/University of Michigan
**Gianni Riotta**, Direttore della Ricerca per la parte di media e disinformazione, Luiss Guido Carli
**Costanza Sciubba Caniglia**, Direttore del Progetto e della Ricerca per la parte teorica e di relazioni internazionali, Harvard Kennedy School

**Con il supporto di:**

Stefania Ardito
Emanuele Birritteri
Luca D'Agostino
Michelangelo Gennaro
Alberto Olivieri
Rossella Sabia
Federica Urzo

**Data di pubblicazione**
30 Giugno 2023
"Questa ricerca è stata realizzata con un contributo dell'Unità di Analisi, Programmazione e Documentazione Storica del Ministero degli Affari Esteri e della Cooperazione Internazionale ai sensi dell'Art. 23 bis del Decreto del Presidente della Repubblica n. 18 del 5 gennaio 1967". "Le opinioni contenute in questa ricerca riflettono l'opinione degli autori e non sono necessariamente rappresentative dell'opinione del Ministero degli Affari Esteri e della Cooperazione Internazionale, dell'Università Luiss Guido Carli, della HKS Misinformation Review, dell'Università del Michigan, e dell'Istituto di Geopolitica Digitale."

Ministero degli Affari Esteri
della Cooperazione Internazionale

Luiss
Dipartimento
di Giurisprudenza

HARVARD KENNEDY SCHOOL
Misinformation Review

SCHOOL OF INFORMATION
UNIVERSITY OF MICHIGAN

LUISS
Data Lab

Luiss
Master di Giornalismo

zeta

IGD

# Sommario

# Introduzione

**Introduzione alla ricerca, di C. Sciubba Caniglia, Direttrice del progetto e della ricerca**

Si conclude con questo report il terzo ciclo di questa ricerca, iniziato nel marzo 2020, all'inizio della crisi pandemica. Da allora, moltissimo è cambiato, e con questa ricerca abbiamo avuto l'opportunità di seguire gli sviluppi e i cambiamenti di alcune narrative di disinformazione in Italia. I nostri ricercatori hanno studiato a fondo queste comunità, e ne hanno compreso dinamiche e reti di *network* molto complesse e anche diverse tra loro. Questo lavoro è stato importante, perché ci ha permesso di osservare filoni di disinformazione in evoluzione, e di avere una comprensione tanto dell'evoluzione di tattiche e strategie di disinformazione, quanto delle comunità che ne hanno facilitato la diffusione.



Se già da alcuni anni, tanto la ricerca accademica, quanto la pubblica arena si sono occupate di osservare ed analizzare gli effetti della disinformazione e di operazioni di informazione volte a manipolare l'opinione pubblica, mai come in questi ultimi anni la minaccia che esse rappresentano per la democrazia è apparsa tanto evidente.

Dal marzo 2020 ad oggi, la comprensione del fenomeno disinformativo in Italia è cresciuta enormemente. Gli ultimi due anni e mezzo, fra la pandemia e l'inizio della guerra in Ucraina, non hanno fatto che amplificare l'evidenza e la portata di questo strumento di conflitto, particolarmente nel nostro Paese. Spero che questa ricerca abbia avuto un ruolo per illuminare alcune di queste tattiche e strategie, così come i gruppi che le utilizzano, e che i risultati di queste osservazioni possano essere utili per elaborare strategie di risposta istituzionale.

La nostra ricerca nasce infatti dall'idea di offrire alle istituzioni sia pubbliche che private strumenti per analizzare, monitorare e rispondere alla disinformazione in generale, inclusi attacchi volti a manipolare l'informazione per scopi politici, economici, o ideologici. Per questo abbiamo lavorato per riportare in Italia una linea di ricerca sviluppata negli Stati Uniti e particolarmente ad Harvard.

Tramite una collaborazione *ad hoc* fra la Harvard Kennedy School Misinformation Review, il Luiss Data Lab, il Dipartimento di Giurisprudenza dell'Università Luiss Guido Carli, il Master in Giornalismo e Comunicazione multimediale dell'Università Luiss Guido Carli, l'University of Michigan e l'Istituto di Geopolitica Digitale, abbiamo voluto analizzare concretamente gli effetti delle campagne manipolatorie nel nostro Paese e valutare le contromisure di *policy* e legislative che possono essere sviluppate in risposta al problema.

Lo scoppio della pandemia prima, e della guerra in Ucraina dopo, ci hanno mostrato chiaramente il pericolo che un'opinione pubblica influenzata e manipolata può rappresentare per la democrazia e per la sicurezza nazionale.

Questo tipo di analisi consente una risposta più immediata in casi emergenziali, come dimostrato dal nostro lavoro durante la crisi in Ucraina. In questi ultimi due anni, abbiamo osservato un improvviso spostarsi del *focus* di tutte le comunità su argomenti relativi al conflitto, a partire da febbraio 2022, che è continuato anche quest'anno. Grazie al nostro lavoro di "censimento" e monitoraggio dei *network* della disinformazione, siamo però stati in grado di tracciare immediatamente queste nuove narrative, e di condividere anche con i nostri *partners* queste informazioni, in modo da supportarne il monitoraggio in tempo reale.

Io credo che questo sia un buon esempio di una collaborazione virtuosa fra Università e Istituzioni, e spero di vedere in futuro maggiori scambi in questo senso.

In generale, abbiamo potuto osservare alcuni elementi positivi nello sviluppo della normativa e della risposta istituzionale. Negli ultimi anni, infatti, le istituzioni sia italiane che Europee e di altri Paesi hanno maggiormente compreso l'importanza di questa sfida e stanno intensificando la cooperazione sia interna che con altri *partners* esterni, mettendo in campo soluzioni concrete per rispondere a questo problema. Ne sono esempio le innovazioni in ambito di comunicazione diplomatica e coordinazione istituzionale del Ministero degli Esteri, così come le nuove *policy* Europee, come il DSA e il rafforzamento del *Code of Practice on Disinformation*. Il Segretariato generale delle Nazioni Unite sta inoltre lavorando a un *Code of Conduct on Trustworthy Information*, da rendere pubblico nel 2024.



Nei prossimi anni, queste iniziative dovranno intensificarsi e il nostro ruolo sarà quello di capire come la disinformazione si diffonde in Italia per dare anche strumenti alle Istituzioni per reagire.

Seppure la disinformazione non rappresenti un'assoluta novità strategica, le innovazioni tecnologiche e le modifiche all'ecosistema dell'informazione degli ultimi anni hanno aggiunto ulteriori livelli di complessità, portando allo sviluppo di nuove e più sofisticate tattiche e strategie, che rendono queste campagne più rapide ed efficaci e permettono a diversi gruppi di attori, tanto pubblici quanto privati, tanto domestici quanto stranieri, di intervenire in maniera ingannevole nel dibattito democratico.

Ed è per questo che abbiamo sviluppato questo lavoro, che speriamo sarà utile a facilitare una maggiore comprensione del problema e a porre spunti di riflessione per risposte di *policy*, sia pubbliche che private.

Crediamo infatti che solo grazie alla collaborazione fra diversi ambiti di ricerca accademica, istituzioni pubbliche e private e piattaforme digitali sarà possibile elaborare risposte efficaci a lungo termine.

# Caso di studio

## Introduzione al caso di studio (2022/2023)

**di I. Pasquetto, Direttore della ricerca**

SOMMARIO





## 1 Metodologia per raccolta dati, analisi ed interpretazione

I dati relativi al caso di studio presentato in questo report sono stati raccolti e analizzati seguendo una metodologia di ricerca chiamata "etnografia digitale investigativa," originariamente sviluppata dal gruppo di ricerca *Technology and Social Change Research Project* (TaSC) della Harvard Kennedy School, nella quale la Direttrice della ricerca Irene Pasquetto occupa il ruolo di *Senior Research Fellow*. L'etnografia digitale investigativa abbina le tecniche giornalistiche e forensi all'osservazione etnografica tradizionale di stampo antropologico. È un metodo particolarmente utile per comprendere il fenomeno della disinformazione online, e, nello specifico, per l'analisi e il tracciamento delle campagne di disinformazione. L'etnografia digitale si differenzia da altre metodologie di ricerca comunemente adottate per studiare la disinformazione su Internet sotto vari aspetti. Gli approcci quantitativi misurano la disinformazione su larga scala, utilizzando, per esempio, i sondaggi per valutare gli atteggiamenti delle persone e l'esposizione alla disinformazione, o la scienza dei dati per accertare dove e in che misura le informazioni false si diffondono online. Gli approcci qualitativi (come l'etnografia digitale) sezionano il contenuto stesso, identificando e analizzando temi comuni, artefatti mediatici, strategie retoriche, e le comunità che li creano e amplificano.

Le metodologie puramente quantitative solitamente studiano la disinformazione da un punto di vista passivo, per esempio mirano ad analizzare come certi modelli di reti sociali (i.e., *echo chambers*), algoritmi (i.e., *recommendation algorithms*) o certe predisposizioni psico-sociali (i.e., *motivated reasoning, identity dynamics, reasoning skills*) rendano alcuni utenti più o meno propensi a credere o a condividere notizie false o tendenziose sulle piatteforme *social*. L'approccio etnografico si concentra invece sull'identificazione e analisi delle pratiche di comunicazione digitali messe in atto da quei soggetti che attivamente e consapevolmente sfruttano i *network*, gli algoritmi, e le predisposizioni psico-sociali degli utenti a loro vantaggio, e nello specifico per la diffusione e amplificazione delle campagne di disinformazione online. Il metodo etnografico tradizionale studia i soggetti all'interno di spazi contrassegnati da rituali, credenze e produzioni culturali. Mentre l'etnografo interagisce con i soggetti studiati a vari livelli, nel caso dell'etnografia digitale, l'etnografo digitale studia le "tracce digitali" che gli utenti lasciano su Internet. Per essere effettuato correttamente, uno studio etnografico richiede tempo e pazienza, le osservazioni durano mesi e sono effettuate molteplici volte durante il corso della giornata.

Le fasi dell'etnografia investigativa:

1. Identificazione dell'argomento
2. Mappatura dell'ecosistema dei media e degli *influencer* chiave
3. Creazione dell'ambiente di monitoraggio
4. Sviluppo della strategia di monitoraggio
5. Audit e valutazione delle ipotesi di ricerca
6. Archiviazione e analisi dei risultati



## 2 Punti chiave emersi dall'analisi dati

Dalla ricerca empirica svolta, questo gruppo di ricerca ha riscontrato che:

- Come già osservato nello studio condotto nel 2020/2021 e 2021/2022, i gruppi che organizzano e diffondono campagne di disinformazione in Italia sono ben organizzati da un punto di vista tecnico e infrastrutturale. Questi mettono insieme vere e proprie **infrastrutture della disinformazione** digitale che si poggiano principalmente su pagine e account social, per poi andare a comprendere tutta una serie di siti internet, aggregatori di news, banche dati, canali di disinformazione alternativa, blog, forum, etc.;

- Nel ciclo di ricerca 2022/2023, abbiamo ulteriormente riscontrato che all'interno delle infrastrutture della disinformazione i **blog** sembrano coprire una posizione sempre più di rilievo, forse come risposta agli interventi anti-disinformazione messi in atto delle piattaforme e richiesti dal nuovo panorama legislativo internazionale. I blog rimangono infatti uno dei pochi spazi online a non essere moderato o censurato.

- Tali infrastrutture sono gestite da **agenti della disinformazione** (o *disinfluencers*), come *influencers* e personalità pubbliche, i quali vengono aiutati da un esercito di *follower* fedeli e interessati alla causa. La collaborazione e partecipazione attiva dei *follower* è indispensabile alla diffusione e mantenimento delle infrastrutture di disinformazione nel tempo;

- È ulteriormente emerso come, però, non tutte queste infrastrutture della disinformazione funzionino allo stesso modo. Nello specifico, i **canali "multitematici"** – i quali diffondono varie narrazioni di disinformazione su più tematiche – si distinguono dai **canali "specializzati"** che si focalizzano invece

su un argomento. I canali multitematici sostengono e diffondono narrazioni di disinformazione in relazione al ciclo delle news. Nella nostra analisi abbiamo riscontrato che tali canali si sono focalizzati sul conflitto bellico tra Russia e Ucraina a partire da febbraio 2022, mentre quelli specializzati hanno continuato a trattare narrazioni relative a specifici argomenti (e.g., vaccini);Il quadro che emerge dalla ricerca è quello di un pubblico non solo direttamente coinvolto nella produzione di disinformazione, ma anche in un certo senso abituato a dialogare e a produrre significato sulla base di una retorica disonesta e sensazionalista.

- I canali multitematici risultano particolarmente efficaci nel diffondere disinformazione in modo continuativa alle loro audience in quanto sviluppano **narrazioni di *crossover***, vale a dire narrazioni che riportano notizie false o tendenziose che si rifanno a più temi, legandoli concettualmente e facendo forza retorica sulla **continuità narrativa** (*storytelling*). Nel ciclo 2021/2022, ne era stato esempio la narrazione che si era diffusa sulla presenza di "biolabs" in Ucraina, la quale legava narrazioni di disinformazione sul Covid-19 a quelle sul conflitto in Ucraina;

- Come notato nell'analisi dei cicli precedenti, si conferma l'osservazione che molti dei *disinfluencers* responsabili per l'attivazione e diffusione di tali infrastrutture appartengono a ***categorie di professionisti*** quali avvocati, medici, liberi professionisti, giornalisti e politici. Le campagne di disinformazione sono costruite da "professionisti della disinformazione" e il fenomeno della disinformazione assume quindi le caratteristiche di una pratica professionale più che di un gioco di ruolo, culto religioso o passatempo (come è stata caratterizzata in passato). Va inoltre notato come 11 spesso questi *disinfluencers* derivano dei guadagni monetari dalle loro attività on e offline, per esempio vendendo prodotti, tessere associative o richiedendo offerte e donazioni;

- Il nuovo studio conferma anche **il ruolo centrale dei media tradizionali** nel dare voce e amplificare le campagne di disinformazione nate nella rete. Per quanto riguarda i **giornali**, abbiamo assistito a un caso di un troll online, quindi un account il cui scopo è quello di provocare altri utenti diffondendo notizie false o tendenziose, che è approdato sulla carta stampata, caso gravissimo perché va ovviamente a dare ulteriore visibilità a questo *account* e allo stesso tempo legittima e normalizza le strategie di *trolling* e manipolazione *online* messe in atto da questo *account*. Per quanto riguarda le **televisioni**, abbiamo notato che i *talk show* – proprio per il loro carattere sensazionalista – forniscono agli *influencers* una fonte infinita di virgolettati da poter usare per giustificare le narrazioni di disinformazione, o per attaccare politici e altri personaggi in vista;

- Già nei cicli di ricerca precedenti era anche emerso che, però, spesso gli agenti della disinformazione **riprendono articoli o media dal contenuto accurato e li ricontestualizzano in maniera fuorviante e tendenziosa**. Il caso di studio presentato di seguito riporta diversi esempi in questo senso. Va notato che questa tattica di disinformazione – chiamata *recontextualized media tactic* – rimane essere la più diffusa, anche più della diffusione di contenuto falso.

- Quest'anno abbiamo anche riscontrato la presenza di una vera e propria ***meme war*** tra fazioni diverse. Notizia sotto certi aspetti positiva perché indica l'esistenza di una **resistenza organica digitale** contro la disinformazione. Sarebbe opportuno fare ulteriori studi su questo aspetto e in particolare andare a capire se questo fenomeno può essere in qualche modo sfruttato nelle campagne anti-disinformazione e operazioni di *debunking*.

- Per quanto riguarda le nuove narrazioni di disinformazione, abbiamo riscontrato meno attenzione sulle tesi complottiste dei biolab e una concentrazione delle narrazioni sulla **guerra in Donbass**, si parla meno di Covid-19 ma ancora molto di vaccini;

- Mentre invece per quanto riguarda i **progressi** degli interventi anti-disinformazione online, va notato che mentre le piattaforme hanno fatto progressi da un punto della rimozione dei contenuti falsi organici, resta il problema dei **contenuti sensibili** su Telegram e di quelli falsi **sponsorizzati** su FB. Pagando, è ancora ad oggi possibile pubblicare notizie false su Facebook.

# 3 Raccomandazioni per i media, le piattaforme e il pubblico

- Come osservato già nei cicli precedenti, le piattaforme dovrebbero tener conto dell'aspetto temporale quando organizzano interventi contro la disinformazione come il ***deplatforming***. Se il *deplatforming* non avviene in modo tempestivo, avrà un effetto limitato nello sradicare tali gruppi e limitare l'efficacia delle campagne. Va inoltre notato che il *deplatforming* non è mai una soluzione definitiva, ma deve invece essere effettuato in maniera iterativa in quanto i gruppi di disinformazione sviluppano tattiche e strategie precise che consentono loro di adattarsi volta per volta a nuove condizioni tecniche;

- Alla luce di quanto osservato in questa ricerca, i canali "multitematici" risulteranno particolarmente difficili da individuare, in quanto condividono narrazioni di disinformazione su molti argomenti. Anche la tattica di *decontextualized media* rappresenta una sfida per la moderazione del contenuto, in quanto non consiste nella condivisione di contenuto falso ma di **contesto falso**;

- Anche i media tradizionali possono svolgere un ruolo centrale nella prevenzione e diminuzione della disinformazione. Da un lato, tramite l'adozione di ***strategic silence*** da parte dei media, una tattica di coordinazione giornalistica che prevede la consapevole presa di coscienza del ruolo dei media nell'amplificare le campagne di disinformazione, e la conseguente decisione di non dare visibilità a tali campagne messe in atto dai gruppi della disinformazione. In secondo luogo, si consiglia lo sviluppo di un **curriculum giornalistico** svolto ad educare nuove generazioni di giornalisti sul funzionamento della disinformazione online;

- Per una migliore comprensione del fenomeno a lungo termine e per sviluppare adeguate contromisure tecniche e regolamentari, questo gruppo di ricerca consiglia inoltre di promuovere lo scambio e la collaborazione fra l'Università, le Istituzioni pubbliche, e le imprese private tramite **lo stanziamento di fondi strutturali** per creare e mantenere gruppi di ricerca e discussione a livello nazionale ed internazionale, di natura sia formale che informale.

# Caso di studio:

## Narrazioni e strategie di propaganda nelle *community* filorusse

**di A. Olivieri e M. Gennaro***

SOMMARIO





## 1 Introduzione e nota metodologica

Per studiare le operazioni di disinformazione e propaganda filorussa in Italia, in particolare riguardo la guerra in Ucraina, siamo partiti dalle piattaforme Telegram, Twitter e Facebook. Seguendo il modello di *Investigative Digital Ethnography* delineato da Brian Friedberg (2020), la ricerca si è svolta in continuità con il precedente ciclo di studi del 2022, durante il quale erano stati individuati i principali *influencer* e organizzazioni attivi nelle campagne mediatiche favorevoli alla Russia. Dal *database* di partenza, abbiamo selezionato alcuni degli attori risultati ancora attivi e influenti nelle *community* filorusse italiane, con un numero di *follower* compreso tra i 1.000 e i 120.000.

* Il lavoro è frutto del lavoro congiunto degli Autori. In particolare, sono da attribuire a M. Gennaro l'analisi qualitativa e la stesura del testo e ad A. Olivieri l'analisi quantitativa e le visualizzazioni.

Per Twitter e Telegram, sono state sviluppate due applicazioni in Python per scaricare *tweet*, messaggi, condivisioni e commenti, presi dagli *account* diffusori di disinformazione sulla guerra in Ucraina. Una volta raccolto questo dato grezzo, le applicazioni lo puliscono e formattano in modo da poter salvare i dati così trattati in un *database* SQL, facilitando la successiva fase di analisi. Il download dei dati è avvenuto tramite accesso API, elevato nel caso di Twitter, comune nel caso di Telegram. Questo ha permesso di monitorare l'attività di 34 canali Telegram e 5 *account* Twitter. Il campione ristretto di Twitter si spiega per le tempistiche più lunghe dovute al *rate limit* - il numero massimo di richieste in una data unità temporale - imposto alle chiamate dell'API da Twitter stesso. La raccolta automatizzata, affiancata dalle osservazioni a mano sull'andamento dei *trend* sui *social media*, è iniziata l'1 dicembre 2022 e si è conclusa il 28 febbraio 2023. Le applicazioni, avendo incorporati programmi per automatizzare la realizzazione di visualizzazioni e analisi di base sui dati, sono state utilizzate per creare le tabelle e le immagini di questo report. Questo ci ha permesso una comprensione più approfondita della situazione, e ci ha altresì permesso di individuare i post che hanno ricevuto maggiore *engagement*, interazioni e condivisioni, e gli *hashtag* più utilizzati.

A partire dal campione di 5 *account* Twitter, abbiamo ricostruito uno *User Network* che rappresenta le interazioni tra utenti della *community* (menzioni, *retweet* e *tweet* di citazione) con determinati *target* come punto centrale dell'indagine. Per Telegram invece, abbiamo analizzato le dieci *reaction* più usate dagli utenti sotto i messaggi dei nostri *target*. Per completare questa parziale *sentiment analysis*, abbiamo individuato per ognuna delle *reaction* i dieci post che ne hanno ricevute di più.

## Hashtag



#NATO

#Fuoridalcoro

#Zelensky

#ZelenskyWarCriminal

#Sanremo2023

#agorarai

#Ucraina

#Russia

#USA

#Parsi

#Tocci

#Meloni

| |
|---|
| #UE |
| #BastaCensuraPerMarioImprota |
| #Biden |
| #VonDerLeyen |
| #NotInMyName |
| #Putin |
| #StopWar |
| #Kiev |

***Tabella 1:*** *La lista degli hashtag propagandistici usati dai 5 account Twitter e dagli utenti che hanno risposto ai loro post sulla guerra in Ucraina.*

Poiché Facebook non consente il *download* di dati, sulla piattaforma di Meta l'indagine è stata condotta manualmente. A partire da una ricerca euristica per parole chiave ("Putin", "Ucraina", "Lavrov", "Zakharova"), abbiamo individuato alcune pagine e gruppi pubblici impegnati nella diffusione di propaganda filorussa. Successivamente, l'algoritmo della piattaforma ci ha condotto alla scoperta di nuovi contenuti e attori di disinformazione. Le osservazioni sono avvenute due volte a settimana per un totale di 22 ore, mentre le principali organizzazioni, *influencer*, testate, siti *web*, *hashtag* e articoli filorussi sono stati catalogati in un'apposita *spreadsheet*. Tramite Zotero, abbiamo poi creato una biblioteca digitale con i nostri studi, gli articoli, libri e documenti citati nelle narrazioni propagandistiche sulla guerra in Ucraina.



## 2 Gruppi e *Influencer*

Gli *account* più rilevanti nelle *community* filorusse, per numero di *follower* ed *engagement*, sono gestiti da personaggi e organizzazioni differenti, spesso impegnati in campagne mediatiche su vari temi. Di centrale importanza sono i *blog* di (dis)informazione, anche chiamati siti di "*clickbait*", *website* che promuovono i loro articoli su Facebook, Twitter e Telegram accompagnati da brevi claim di forte impatto emotivo per invogliare gli utenti alla lettura (vd. def. "*Clickbait website*" da *Merriam Webster Dictionary*, https://www.merriam-webster.com/dictionary/clickbait). Di solito, questi siti *web* hanno un *design* simile ai giornali *online*, utile a rendere più credibile il loro lavoro pseudo- giornalistico. La loro produzione di contenuti non si limita agli articoli, ma comprende *podcast*, programmi radio, riviste, *newsletter* e, in alcuni casi, i *blog* sono associati a case editrici omonime, possono prescindere dai contenuti video e nella maggior parte dei casi hanno un canale Youtube, una sezione del sito o una *web tv* dove caricare live, interviste, servizi giornalistici, telegiornali, persino documentari e lungometraggi.

Per fare concorrenza ai media tradizionali - che prendono di mira con campagne denigratorie e accuse di asservimento al potere - questi *blog* sono multitematici e seguono il flusso delle notizie quotidiane, con particolare attenzione ai temi più cari al loro pubblico. Non si occupano esclusivamente di guerra

in Ucraina e hanno linee editoriali differenti. Alcuni *website* sono animati da un forte posizionamento politico di carattere sovranista, euroscettico, omofobo e xenofobo, altri sono specializzati in tesi antiscientifiche sulla pandemia da Covid-19, in particolare sui presunti «malori improvvisi» che, secondo gli attivisti novax, sarebbero causati dai vaccini. Uno dei *blog*, che propone anche articoli in inglese, si definisce *web media* di «Informazione Giornalistica Cristiana».

Ciò che accomuna i *blog* di (dis)informazione italiani è l'avversione alle istituzioni europee, alla NATO, all'amministrazione Biden, allo Stato ed esercito ucraino, al governo guidato da Giorgia Meloni, ai partiti italiani di area liberale e di centro-sinistra. Spesso questi *alternative media* funzionano come aggregatori di interviste e interventi di personaggi considerati autorevoli dalle *community* filorusse. Tra questi troviamo anche politici, alcuni eletti nel parlamento europeo nel 2020 e alle elezioni politiche italiane del 2022, altri esponenti della galassia dei partiti extraparlamentari che si definiscono anti-sistema. Il posizionamento anti-atlantista e le simpatie per la Federazione Russa accomunano i partiti anti-sistema sovranisti e di estrema sinistra. Tra i promotori delle battaglie contro il sostegno militare italiano all'Ucraina, sia sui *social media* che con manifestazioni pubbliche, anche un sindacato e un collettivo operaio, già attivi in campagne contro l'obbligo vaccinale e il *green pass*.

Tuttavia, la categoria di *influencer* filorussi più numerosa è quella dei sedicenti giornalisti indipendenti, che si arrogano il compito di svelare le «verità che nessuno racconta». Solo in rare eccezioni si tratta di professionisti iscritti all'Ordine Dei Giornalisti e nella maggior parte dei casi sono *influencer*, che si dicono dediti alla libera informazione. Alcuni sono promotori di tesi complottiste a sfondo antisemita, riguardo *elite* globaliste di miliardari che controllerebbero finanza, informazione, politica e istituzioni internazionali. In questi casi, la propaganda filorussa viene inserita in una visione del mondo più estesa, che contrappone un governo mondiale sommerso al progetto multipolare portato avanti da **Russia, Cina e dagli altri Paesi BRICS**.



É raro che i sedicenti giornalisti parlino solo di Ucraina e spesso hanno partecipato - e continuano tuttora - alle campagne mediatiche contro i vaccini e le istituzioni sanitarie, confermando lo stretto legame tra disinformazione antivaccinista e filorussa riscontrato nel ciclo di ricerca precedente (*Come individuare e contrastare operazioni coordinate di disinformazione in Italia*, 2022, pp. 10-20, https://www.esteri.it/wp-content/uploads/2022/09/LUISS-Come-individuare-e- contrastare-operazioni-coordinate-di-disinformazione-in-Italia.pdf). Fanno eccezione due reporter italiani che scrivono dalle Repubbliche di Donetsk e Lugansk, che coprono unicamente la guerra in Ucraina. Questi raccontano il conflitto dal punto di vista della popolazione civile delle città separatiste occupate dal Cremlino, documentando le conseguenze dei bombardamenti ucraini e intervistando esclusivamente i cittadini che considerano i soldati russi come liberatori. I reporter in Donbass sono anche autori di video in cui prigionieri di guerra ucraini, ad esempio i combattenti del Battaglione Azov catturati a Mariupol, mostrano simboli nazisti tatuati sul corpo, oppure raccontano come Kiev mandi a morire in prima linea persone senza addestramento, reclutate con la forza come «carne da cannone». Queste dichiarazioni, che sembrerebbero scritte dai loro carcerieri a scopo propagandistico, servono a demonizzare il governo di Volodymyr Zelensky ed esaltare la clemenza dei soldati russi, non solo disposti a risparmiare la vita dei propri nemici, ma anche a metterli in salvo dal fuoco amico dell'artiglieria ucraina.

Meritano una menzione i gruppi estremisti e complottisti su Facebook e Telegram. Da un lato, troviamo i canali di destra populista, abitati da utenti e *meme* novax, omofobi e contro l'immigrazione. Dall'altro i gruppi estremisti di sinistra, dove i nostalgici dell'Unione Sovietica celebrano le imprese dell'Armata Rossa: qui i separatisti del Donbass vengono raccontati come partigiani antifascisti e rivoluzionari, in lotta contro il governo nazista di Kiev. Ciò che accomuna i gruppi di estrema destra e sinistra è la visione della Federazione Russa come garante dei valori tradizionali, che a seconda del contesto possono riguardare

la famiglia e la fede cristiana, oppure la lotta anticapitalista, contro la globalizzazione e l'egemonia internazionale degli Stati Uniti. Le differenze ideologiche si appianano nei gruppi nazionalbolscevichi, che vantano decine di migliaia di iscritti sui *social media*, e nei numerosi gruppi Facebook dedicati al culto della personalità del presidente Vladimir Putin, ritratto durante eventi pubblici, manifestazioni sportive e in compagnia di animali domestici.

## 3 Piattaforme *social*

La ricerca si è svolta sulle piattaforme Twitter, Telegram e Facebook, in continuità con il caso di studio su novax e guerra in Ucraina svolto nel 2022. Ogni *social media* presenta caratteristiche peculiari e attori in comune, che gestiscono *account* su più piattaforme. Su Twitter, i cinque *account* presi in considerazione si sono dimostrati molto attivi nella pubblicazione di *tweet*, risposte e condivisioni (*occurrences*). L'*account target* più attivo, M.V. (5892 *follower*)[1], conta quasi 87 *occurrences* medie giornaliere nell'arco temporale di 90 giorni preso in esame, da dicembre 2022 a febbraio 2023. Questo numero elevato permette di ipotizzare che il profilo venga gestito da più persone, oppure si avvalga di *tool* per automatizzare le attività sulla piattaforma.

Dall'*account* meno attivo (I.P., 4776 *follower*), si sono registrate solo 1,47 occorrenze giornaliere. Quest'ultimo *target* è stato preso in considerazione come esponente di una categoria nota nella diffusione di propaganda filorussa su Twitter: i *troll*, *account* anonimi che pubblicano commenti provocatori e irritanti per inquinare il dibattito sulla piattaforma. Peraltro, I.P. fa parte del gruppo organizzato dei "mattonisti", che si identificano dall'*emoticon* del mattone presente nel loro nome utente. I "mattonisti" contano almeno un centinaio di *account* e avevano attirato la nostra attenzione nel ciclo di ricerca precedente, per la capacità di coordinarsi e mandare in tendenza le proprie parole d'ordine. La novità è che i gruppi coordinati filorussi si trovano oggi a competere con un gruppo coordinato atlantista, la "NAFO" (*North Atlantic Fellas Organization*), che ingaggia battaglie di *meme* e cerca di contrastare la disinformazione sulla guerra.

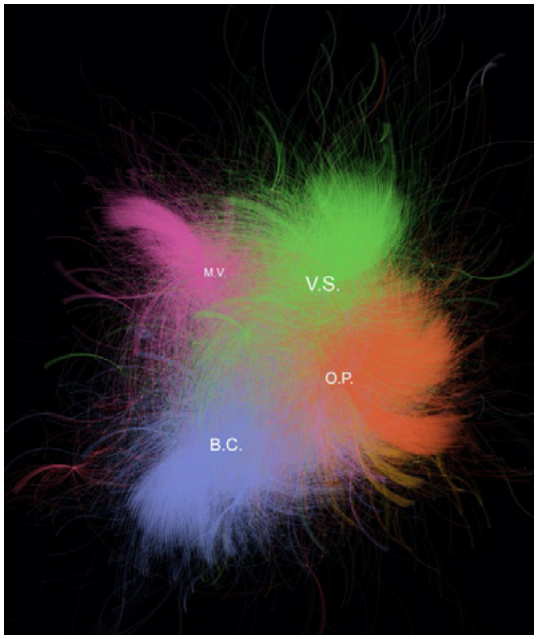



*Immagine 1: Lo User Network di Twitter rappresenta le interazioni tra utenti della community (menzioni, retweet e tweet di citazione) con determinati target come punto centrale dell'indagine. Poiché l'account target I.P. ricopre una posizione periferica e un basso numero di interazioni all'interno del Network, non è visibile nell'immagine.*

Come evidenziato dal caso dei mattonisti, Twitter permette agli utenti di identificarsi per le loro idee politiche inserendo *emoticon* nel nome utente. Nello specifico, molti *account* promotori di disinformazione sulla guerra in Ucraina presentano bandiere della Russia nel *nickname*. Similmente, su Facebook gli utenti filorussi inseriscono una bandiera russa, il simbolo Z o il nastro di San Giorgio nella loro immagine del profilo. In questo modo, i filorussi si riconoscono velocemente, entrano in contatto e creano *community* più estese. La piattaforma

[1] Le abbreviazioni non si riferiscono a nomi propri di persona, ma a pseudonimi usati dagli utenti online. I dati sui *follower* sono aggiornati al 16/05/2023.

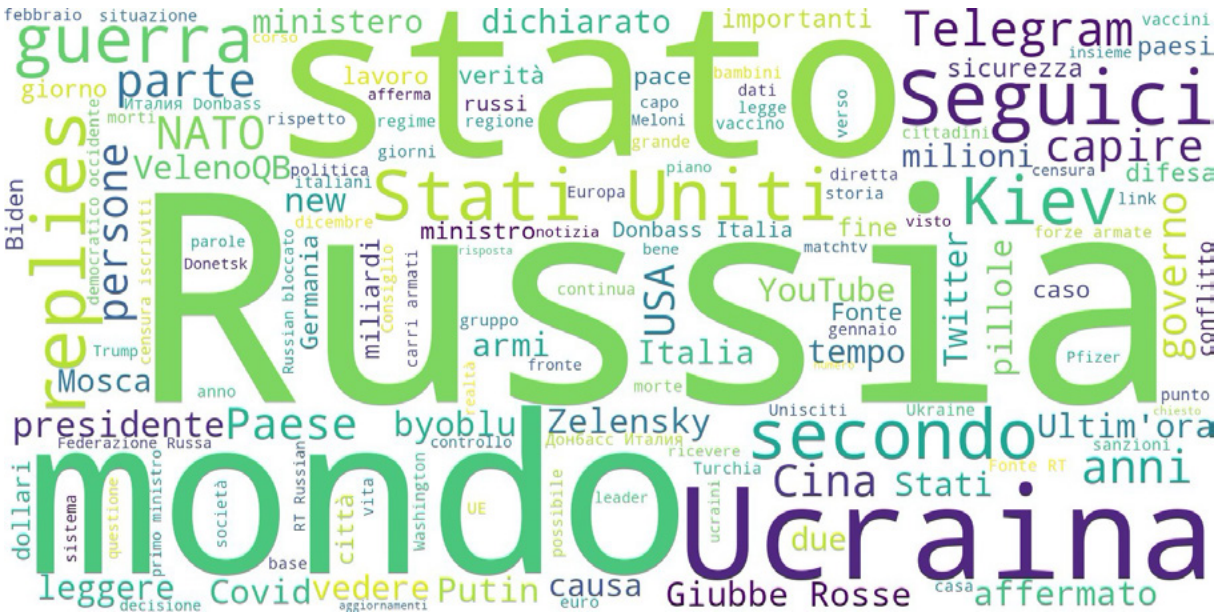
di Meta presenta anche una funzione di traduzione automatica immediata ed efficiente, che permette di estendere le *community* oltre le barriere linguistiche. Proprio la traduzione simultanea potrebbe in parte spiegare l'elevato numero di interazioni tra utenti italiani e russi osservate su Facebook.

*Il nastro di San Giorgio disposto a forma di Z, ripreso dall'immagine del profilo di un utente su Facebook. Il vessillo arancione e nero è diventato il simbolo della vittoria sulla Germania nazista dell'Unione Sovietica durante la Seconda Guerra Mondiale. Viene esibito sulle divise delle Forze Armate della Federazione durante la celebrazione pubblica della Festa della Vittoria.*

Per quanto riguarda Telegram, i canali *target* selezionati sono gestiti da uno o più *admin*. Nella maggior parte dei casi, lasciano attiva la sezione commenti dei loro post per permettere agli utenti di interagire. Alcuni *target* gestiscono anche una *chat*, ovvero un secondo canale dove tutti gli iscritti possono inviare messaggi liberamente. La particolarità di Telegram è la sua elevata tutela della *privacy*, che permette di pubblicare contenuti non ammessi sugli altri *social media*, senza incorrere in conseguenze legali o nel *ban* dalla piattaforma. Infatti, non è raro incontrare contenuti sensibili non censurati, come video che ritraggono i corpi accatastati di soldati ucraini o di civili gettati in fosse comuni. L'elevato numero di video provenienti dal fronte è dovuto ai *reportage* che decine di giornalisti russi, di fede nazionalista o comunque allineati al Cremlino, pubblicano regolarmente sui loro *account* Telegram.

La condivisione sui canali filorussi italiani del lavoro realizzato da questi reporter permette di mettere in contatto diretto il pubblico con gli autori dei contenuti propagandistici, per invogliare gli utenti a informarsi sui canali russi al servizio di Mosca. Per ovviare allo scoglio linguistico, gli *influencer* italiani propongono la traduzione dei post scritti dai reporter russi, oppure appongono sottotitoli in italiano sotto i loro reportage. Per queste ragioni, molti *influencer* filorussi attivi su Facebook e Twitter inseriscono il *link* del loro *account* Telegram sotto ogni post, invitando il pubblico a unirsi al canale per accedere a un'informazione priva di filtri e censure.






*Wordcloud con le parole più utilizzate nei post dei nostri account target su Telegram. Le dimensioni delle parole sono proporzionali alla frequenza.*


*Immagine 2: Wordcloud con le parole più utilizzate nei post dei nostri account target su Telegram e nelle risposte che hanno ricevuto dagli altri utenti.*

Attraverso il monitoraggio sulle tre piattaforme, abbiamo individuato altri *social media* utilizzati per le campagne di disinformazione sulla guerra in Ucraina. Infatti, i post dei nostri *target* contengono spesso *link* in uscita, che rimandano soprattutto ai loro *blog* personali o a canali propagandistici su YouTube, TikTok e Rumble. Si segnala un crescente utilizzo di VKontakte, corrispettivo russo di Facebook, dove alcuni *influencer* filorussi italiani hanno aperto un profilo e caricano contenuti. La piattaforma ha progressivamente perso la sua indipendenza dal controllo statale di Mosca, in particolare dopo la nomina ad amministratore delegato Vladimir Kiriyenko e il bando dei *social media* occidentali dalla Federazione Russa.



## 4 Media Tradizionali

Durante la ricerca abbiamo rilevato come uno dei nostri *target*, B.C., che conta 27.612 *follower* su Twitter e 21,4 *occurrences* giornaliere, sia anche collaboratore di un quotidiano italiano a tiratura nazionale. Dal 2021, la testata pubblica gli editoriali di B.C. sia sulla carta stampata che nell'edizione digitale, firmati usando il suo nome utente di Twitter come pseudonimo. Nessuno degli articoli riguarda la guerra in Ucraina e B.C. sembra essersi ritagliato il suo spazio sul giornale parlando della campagna vaccinale durante la pandemia da Covid-19, con duri attacchi alla comunità scientifica e apologie in difesa dei novax italiani. I suoi articoli vengono spesso scansionati e pubblicati da altri *account* Twitter, soprattutto da O.P. (12.847 *follower*, 31,2 *occurrences* medie giornaliere), *influencer* sovranista che si congratula ed esalta il lavoro giornalistico del collega. La presenza di B.C. sul quotidiano gli conferisce visibilità e grande autorevolezza nelle *community* esposte alla propaganda russa. Inoltre, B.C. ha appena pubblicato un libro basato sul complotto del Nuovo Ordine Mondiale, in cui accusa l'*elite* finanziaria globale, riunita ogni anno al *World Economic Forum* fondato da Klaus Schwab, di aver messo fine all'epoca dei diritti individuali per schiavizzare l'umanità, costringendola - tra le altre cose - a sottoporsi a trattamenti sanitari obbligatori (i vaccini).

Il caso di B.C. testimonia la vicinanza di un *influencer* cospirazionista, novax e filorusso al mondo dell'informazione tradizionale. L'*account* Twitter di B.C. è anonimo e l'identità dell'utente rimane ignota. Guardando i suoi post che hanno ricevuto maggiore *engagement* durante il nostro monitoraggio, si

riconosce lo stile comunicativo tipico dei *troll*: brevi *tweet* provocatori e di forte impatto emotivo per istigare polemiche nei commenti; uso di fatti inventati o non verificabili per rafforzare le proprie opinioni, approfittando della protezione dell'anonimato; uso di *meme* per deridere gli avversari nelle discussioni *online*. Dunque, un *troll* approdato sulla carta stampata, sia come editorialista che come saggista. Peraltro, l'introduzione del suo libro è scritta da un noto giornalista e opinionista televisivo, che siede nel comitato di redazione del quotidiano con cui B.C. collabora. Nell'introdurre il testo, il giornalista non esita a presentare B.C. come un «*troll guerrigliero*».

Sempre su Twitter, l'analisi degli *hashtag* utilizzati dai nostri *target* ha evidenziato l'importanza della televisione per le campagne di disinformazione *online*. In particolare, gli *influencer* che fanno disinformazione sulla guerra seguono attentamente alcuni *talk show*, dai quali prendono degli estratti per condividerli sulle piattaforme *social*. I *talk show* in questione ospitano spesso opinionisti capaci di esprimere posizioni chiare, decise e controverse su tematiche divisive, come l'invio di armi all'Ucraina. Poiché il criterio di selezione degli ospiti è legato allo *share* televisivo della trasmissione, alcuni opinionisti tendono a estremizzare le proprie idee per attirare attenzione e garantirsi un posto fisso nei salotti tv. I loro interventi vengono poi estrapolati dal contesto e pubblicati sui social media da account terzi, tra i quali figurano alcuni dei nostri *target* di Twitter e Telegram. Gli *influencer* filorussi selezionano le dichiarazioni compatibili con la loro narrazione sulla guerra in Ucraina, per dare prova ai propri *follower* della validità delle loro idee. Quando una tesi affine alla propaganda filorussa viene pronunciata in televisione, infatti, acquisisce maggiore credibilità, soprattutto se a pronunciarla è un personaggio considerato autorevole, come un accademico, un giornalista o un politico.

## 5 Narrazioni



La propaganda filorussa sulla guerra in Ucraina presenta delle narrazioni persistenti e capaci di adattarsi di volta in volta alle notizie di attualità. La posizione di fondo sostenuta dagli *influencer* filorussi consiste nel ritenere gli stati NATO e il governo ucraino responsabili per l'inizio del conflitto, nel tentativo di infliggere una sconfitta strategica alla Russia. Secondo tale tesi, il 24 febbraio 2022 la Federazione avrebbe dato inizio a un'«operazione militare speciale» per difendere la propria sicurezza nazionale dall'espansionismo dell'Alleanza Atlantica, pronta ad accogliere l'adesione di Kiev, e per proteggere l'incolumità delle popolazioni dell'Ucraina orientale. Infatti, il conflitto in Donbass viene raccontato come una guerra civile, negando sia il ruolo operativo delle forze speciali russe attive nelle regioni di Donetsk e Lugansk, che il controllo esercitato da Mosca sulle Repubbliche separatiste da maggio 2014, entrambi riconosciuti da una storica sentenza della Corte europea dei diritti dell'uomo (ECHR, 25 gennaio 2023, nos. 8019/16, 43800/14 and 28525/20). Il cosiddetto «regime nazista di Kiev», epiteto usato dagli *influencer* filorussi in riferimento al governo filoeuropeo instaurato dalla rivoluzione Maidan, viene accusato di aver perpetrato un genocidio contro le popolazioni russofone del Donbass. La stessa rivoluzione Maidan viene descritta come orchestrata dai servizi segreti degli Stati Uniti, mentre al governo di Volodymyr Zelensky viene imputato di aver violato gli accordi di Minsk, infrangendo il cessate il fuoco e preparando delle spedizioni punitive contro i separatisti.

La narrazione filorussa sul Donbass è smentita dal rapporto dell'*Office of the UN High Commissioner for Human Rights* sulle vittime civili in Ucraina, che non porta evidenze a sostegno di un presunto genocidio (OHCHR, *Conflict-related civilian casualties in Ukraine*, 2022). Tuttavia, la teoria secondo cui Zelensky avrebbe ordinato un massacro di civili russofoni in Ucraina orientale è stata riportata anche da un'importante testata italiana, come segnalato dalla Senior Fellow dell'Istituto Affari Internazionali Nona Mikhelidze in un dettagliato *debunking* pubblicato su Twitter (e sintetizzato in forma di articolo

dall'associazione *Liberi Oltre le Illusioni*, https://www.liberioltreleillusioni.it/news/articolo/tutte-le-post-verita-dellarticolo-di-ranieri- smontate-da-nona-mikhelidze).

È evidente il tentativo di spostare la rappresentazione del conflitto su un piano etnico e culturale, attraverso l'uso ambiguo della parola "russofono" (madrelingua russo), usata impropriamente dalla propaganda come sinonimo di "filorusso" e di "russo etnico". Stando ai dati del censimento realizzato nel 2001, il russo è la lingua madre del 26% della popolazione ucraina. Della popolazione totale di lingua madre russa, solo il 56% è di etnia russa, mentre il restante 44% comprende ucraini, bielorussi, ebrei, greci, bulgari, moldavi, armeni, tartari, polacchi, tedeschi e tartari di Crimea. Nel suo ultimo libro, *L'Ucraina e Putin. Tra storia e ideologia*, lo storico Andrea Graziosi analizza i limiti di una visione etnolinguistica applicata a un Paese multiculturale come l'Ucraina. Peraltro, non esistono dati che supportino l'assunto sottinteso dalla propaganda moscovita, secondo cui l'intera popolazione ucraina di etnia russa sarebbe sostenitrice delle Repubbliche separatiste e dell'esercito di Putin: lingua, etnia e ideologia non sono sovrapponibili né intercambiabili.

Sui *social media*, il lavoro svolto dai reporter italiani in Donbass serve a documentare, tramite testimonianze dirette, la narrazione filorussa della guerra: sul suo canale Telegram, un *influencer* pubblica reportage sui bombardamenti ucraini sulla città di Donetsk, mostrando gli edifici residenziali colpiti e i corpi inerti delle vittime civili. La città rappresentata dal reporter sembra abitata unicamente da persone disarmate, bambini innocenti, soccorritori e pompieri, pronti a lanciarsi in gesti eroici per salvare i bisognosi dalle macerie.

Un lavoro simile è svolto da una controversa organizzazione umanitaria di volontariato che raccoglie fondi per i bambini del Donbass. È possibile donare il 5x100 alla ODV, che promuove anche una raccolta fondi per ricostruire Mariupol durante l'occupazione russa. Sui suoi *account* Twitter, Facebook, Telegram e VKontakte, l'associazione racconta le sofferenze dei civili colpiti dal fuoco di Kiev e dalle armi occidentali. La presenza di milizie separatiste e contingenti militari e paramilitari russi non viene mai menzionata, al contrario si parla di città occupate dalle truppe ucraine. La guerra in Donbass viene presentata come un insensato massacro di innocenti da parte del governo ucraino, con un capovolgimento di prospettiva che rappresenta l'esercito di Zelensky come aggressore e occupante nelle regioni sud-orientali del Paese.



Le forniture di armi alla resistenza ucraina diventano dunque il mezzo con cui la NATO alimenta il conflitto e allontana ogni prospettiva di pace. Peraltro, prima dell'invio di ogni pacchetto di aiuti militari a Kiev, la propaganda filorussa si è attivata per paventare lo scoppio della terza guerra mondiale. Facendo eco alle continue minacce lanciate dall'ex presidente russo Dmitry Medvedev, sui *social media* si è detto che il Cremlino sarebbe legittimato a usare l'ordigno atomico in caso di un prolungamento della guerra. Quando in Germania si dibatteva sul possibile invio di carri armati Leopard, approvato il 25 gennaio 2023, le *community* filorusse avevano omaggiato l'iniziale reticenza del cancelliere Olaf Scholz. Se i *tank* tedeschi fossero arrivati in Ucraina, sostenevano alcuni, la Germania sarebbe automaticamente entrata in guerra con Mosca. Altri hanno affermato che il passo successivo alle forniture di Leopard sarebbe stato l'invio di unità militari dai Paesi Occidentali. Similmente, quando il governo italiano ha deciso di fornire il sistema missilistico Samp-T all'Ucraina, i filorussi hanno affermato che la difesa aerea italiana sarebbe rimasta sguarnita. Questi tentativi di intimidazione si possono inscrivere in una narrativa più generale, pronunciata anche da un noto opinionista italiano in diretta televisiva: la Federazione Russa non può perdere la guerra perché, se non vincesse con le armi convenzionali, ricorrerebbe alle armi atomiche contro Kiev e i suoi alleati.

Infine, nelle *community* analizzate si è affermata l'idea che, opponendosi all'espansionismo di Mosca, l'Italia tragga solo ripercussioni negative. Il supporto militare alla resistenza ucraina sarebbe

un'imposizione della NATO, ulteriore prova della sudditanza di Roma agli interessi degli Stati Uniti. Ai cittadini italiani ne verrebbe solo l'aumento dei prezzi dell'energia, effetto collaterale delle sanzioni imposte alla Russia, e il pericolo di venire coinvolti in caso di allargamento del conflitto. Questa narrativa si estende all'intera UE, costretta a «rompere secolari convergenze tra politica europea e russa» per sottomissione a Washington. Non si menzionano mai i pericoli per la sicurezza europea causati dall'invasione russa in Ucraina.

Riassumendo, le narrazioni emerse sono le seguenti:

- La NATO è responsabile dello scoppio della guerra, perché il suo espansionismo è una minaccia diretta per i confini e la sopravvivenza della Federazione Russa. L'operazione militare indetta da Mosca è di carattere difensivo.

- Il governo di Kiev è un regime nazista, insediato grazie alla rivoluzione Maidan organizzata dai servizi segreti statunitensi.

- Il governo di Kiev è autore di un genocidio della popolazione russofona in Ucraina orientale. La Russia è intervenuta nella regione per difendere i russofoni dalla violenze ordinate dal presidente Volodymyr Zelensky.

- La guerra in Donbass non è interstatale, ma riguarda la volontà della popolazione russofona di rendersi indipendente da Kiev per unirsi alla Federazione Russa. Il governo ucraino ha violato gli accordi di Minsk per opporsi all'autodeterminazione dei separatisti.

- L'invio di armi occidentali all'Ucraina allontana ogni prospettiva di pace, alimenta il massacro di civili russofoni e avvicina il coinvolgimento diretto dei Paesi Occidentali nel conflitto.



- L'esercito ucraino sostenuto dalla NATO non può sconfiggere il Cremlino, il quale, se non riuscisse a prevalere con gli armamenti convenzionali, ricorrerebbe agli ordigni atomici.

- L'Italia e l'Unione Europea traggono solo conseguenze negative opponendosi all'operazione militare della Federazione Russa. Il sostegno occidentale alla resistenza ucraina è stato imposto dagli Stati Uniti.

# 6 Tattiche di manipolazione dei media

Attraverso l'analisi qualitativa dei dati raccolti su Twitter, Telegram e Facebook, abbiamo individuato le tattiche più comuni impiegate per diffondere disinformazione e propaganda sulla guerra in Ucraina. Ci limitiamo a citarne tre: *recontextualized media, advertising, quoting.*

### a. Recontextualized media

Si parla di *recontextualized media* quando un articolo, intervista, video o audio viene privato del suo contesto originale ed inserito in una nuova cornice narrativa. L'obiettivo è distorcere il contenuto per adattarlo alle narrazioni di disinformazione, che diventano più credibili poiché sembrano supportate dalle pubblicazioni dei media *mainstream* o dalle dichiarazioni di personaggi eminenti. Per fare ciò, non è necessario alterare il media autentico o creare artefatti. Inoltre, gli *account target* selezionati riportano spesso articoli ripresi da emittenti statali russe e consigliano siti *web streaming* dove vedere

in diretta i canali televisivi RT e Pervyj kanal, entrambi oscurati in Europa. Chiariamo proponendo due esempi.

Il 7 dicembre 2023, l'ex-Cancelliera tedesca Angela Merkel ha rilasciato un'intervista alla testata *Die Zeit*, in cui analizza, tra le altre cose, i possibili errori della Germania nelle scelte di politica estera nei confronti della Russia. Nell'articolo, Merkel ammette il fallimento diplomatico degli accordi di Minsk, che non sono riusciti ad avviare un concreto processo di pace tra Russia e Ucraina. Tuttavia, l'ex Cancelliera riconosce che lo stallo abbia impedito a Putin di vincere rapidamente la guerra, permettendo all'Ucraina di prendere tempo per rafforzarsi e difendersi con maggiore efficacia rispetto al 2014. Queste dichiarazioni di Merkel sono state decontestualizzate e pubblicate dall'Ambasciata Russa in Italia sui suoi *account social*, per piegarle a un'interpretazione forzata e tendenziosa. Il canale ufficiale della diplomazia russa ha accusato i Paesi Occidentali di aver ingannato Mosca, per «imbottire il regime di Kiev di armi e prepararlo per i combattimenti». La Russia era stata vittima di «una bufala»: per la prima volta la «leader di un paese del formato Normandia» aveva riconosciuto che «il regime di Kiev e i suoi sponsor occidentali non avevano alcuna intenzione di implementare gli accordi di Minsk».

Anche le parole pronunciate dalla presidente della Commissione Europea alla Conferenza sulla sicurezza di Monaco sono state presentate in modo simile. Il 18 febbraio 2023, Ursula Von Der Leyen ha raccontato l'impegno diplomatico dei vertici europei nei mesi precedenti allo scoppio della guerra. La presidente della Commissione ha ricordato che, di fronte alla possibilità che il Cremlino desse inizio all'invasione, l'Unione Europea e la Casa Bianca avevano iniziato a collaborare già a dicembre 2021 per preparare le sanzioni contro la Russia. Su Telegram, alcuni canali filorussi hanno riportato queste dichiarazioni, sostenendo che Von Der Leyen si fosse fatta sfuggire «la verità». Il fatto che l'Ucraina e l'Unione Europea si fossero preparate all'eventualità della guerra, infatti, viene sistematicamente riportato per deresponsabilizzare la Russia: secondo i filorussi, Mosca avrebbe dato il via all'operazione militare per rispondere alle provocazioni ricevute o difendersi dalle minacce belliche e finanziarie dell'Occidente.



### b. Advertising

Su Facebook, abbiamo incontrato delle pagine attive nella disinformazione filorussa che pagano la piattaforma per sponsorizzare i propri contenuti. Le pubblicità sono iniziate a comparire nella sezione "*Home*" dopo circa 11 ore di ricerca manuale, durante la quale abbiamo interagito con post e pagine sostenitrici del Cremlino. Le prime pubblicità incontrate non contenevano narrazioni di disinformazione, ma riguardavano pagine promotrici di propaganda filorussa o *account* di partiti contrari alle forniture di armi italiane a Kiev. Successivamente, hanno iniziato a comparire contenuti sponsorizzati che promuovevano attivamente teorie del complotto, tesi antivacciniste e pseudoscientifiche.

Ad esempio, una pagina invitava a scoprire le «verità universali» attraverso un video su G. C., giornalista e politico scomparso nel 2020, noto sostenitore delle cospirazioni sulle scie chimiche, sull'attentato dell'11 settembre e su presunti "terremoti artificiali". Nella pubblicità si parlava di come la guerra in Ucraina avesse confermato la profezia di Chiesa sullo scoppio della terza guerra mondiale.

Abbiamo anche incontrato un contenuto sponsorizzato dalla pagina Facebook di uno dei nostri *account target* su Telegram. Il post descriveva il presunto piano degli Stati Uniti per indebolire il governo di Vladimir Putin: dal 2014, Washington avrebbe usato il fronte ucraino e le sanzioni

occidentali per impegnare la Russia senza dover combattere una guerra diretta. Il tutto per colpire il nemico reale, la Cina, privandola della protezione strategica garantita dagli alleati russi. Questi venivano fiaccati grazie al «sangue» degli ucraini e alla crisi economica, inflitta anche all'Unione Europea come contraccolpo delle sanzioni.

### c. Quoting

Dall'analisi qualitativa sulle pubblicazioni dei nostri *target* su Twitter e Telegram, abbiamo riscontrato che, come in parte evidenziato nel paragrafo sui *recontextualized media*, molti post riportano dichiarazioni di personaggi autorevoli ed esterni alle *community* filorusse. Questi si dividono tra i personaggi apprezzati dalle *community* e altri considerati antagonisti, perché promotori della narrazione ufficiale sulla guerra in Ucraina. I post che hanno raggiunto il maggior numero di interazioni contengono spesso virgolettati capaci di attirare l'interesse degli utenti delle piattaforme.

Su Telegram, abbiamo analizzato le *reaction* lasciate dagli utenti sotto i post, per individuare quelle più utilizzate e in riferimento a quali contenuti. Nella lista dei 10 post che hanno ricevuto più *reaction*, abbiamo riscontrato come le citazioni e gli estratti di interviste dei personaggi apprezzati dalla *community* generassero un alto numero di *reaction* associate a emozioni positive (cuori, applausi, like). Tra i personaggi i cui virgolettati hanno ricevuto molte *reaction* di approvazione, si annoverano soprattutto esponenti politici russi, come il ministro degli esteri Lavrov e la sua portavoce Zakharova, e ungheresi, come il presidente Viktor Orban e il ministro degli esteri Péter Szijjártó. Troviamo anche *influencer* novax e giornalisti di estrema destra, opinionisti televisivi e un generale dell'esercito italiano contrario all'invio di armi a Kiev.

Viceversa, i post che riguardano personaggi invisi alla *community* hanno generato un alto numero di *reaction* negative, associate alla rabbia e al disgusto, oppure di derisione. Anche i commenti rispecchiano questa osservazione, perché popolati di insulti e discorsi d'odio. Tra i personaggi considerati negativi, figurano il presidente ucraino Zelensky, giornalisti e *fact-checkers* come Bruno Vespa, Enrico Mentana e David Puente, esponenti politici italiani appartenenti alla maggioranza, soprattutto la premier Giorgia Meloni, e all'ala liberale e di centro-sinistra dell'opposizione, la presidente della Commissione Europea, Ursula Von Der Leyen, e il segretario della NATO, Jens Stoltenberg.



L'obiettivo dei post con un elevato numero di *reaction* negative è degradare gli avversari della *community*. Anche l'analisi degli *hashtag* più utilizzati su Twitter ha confermato questa pratica. Infatti, abbiamo riscontrato l'uso dei cognomi di alcuni personaggi "nemici" della propaganda filorussa per creare degli autentici *tread*, dove insultare e sfogare il disprezzo verso esperti di politica internazionale come Nathalie Tocci, direttrice dell'Istituto Affari Internazionali, e Vittorio Emanuele Parsi dell'Università Cattolica di Milano (#Tocci, #Parsi, #LeComParsate, #ConteParsetti).

## 7 Conclusioni

In conclusione, la ricerca su Twitter, Telegram e Facebook ci ha permesso di identificare gli attori principali nelle *community* filorusse e studiare l'attività degli *influencer* già noti. Si è rilevata l'importanza dei *blog* di (dis)informazione, che si costruiscono credibilità fingendo di svolgere un lavoro giornalistico rigoroso e cercando di presentare i media tradizionali come inaffidabili. I numerosi *influencer*, che si auto-definiscono giornalisti indipendenti, hanno dimostrato la capacità di inserire le narrazioni sulla guerra in Ucraina all'interno di cospirazioni più ampie, spesso a sfondo antisemita. Le *community*

filorusse hanno manifestato grande interesse anche per contenuti non attinenti alla guerra, in particolare per le campagne novax sulla pandemia da Covid-19, i complotti sull'origine artificiale del terremoto in Turchia e Siria, la propaganda contro la liberalizzazione degli alimenti a base di insetti, la difesa dei valori tradizionali dalla cosiddetta «teoria gender».

Il monitoraggio su Twitter ha rilevato delle autentiche battaglie di *meme* tra gruppi coordinati di utenti anonimi filorussi e atlantisti. Il caso del nostro *target* B.C., *account troll* approdato sulla carta stampata, mette in guardia sulle possibilità di collaborazione tra i promotori della disinformazione *online* e i media tradizionali, come gruppi editoriali ed emittenti televisive.

Le narrazioni filorusse sulla guerra hanno evidenziato una particolare attenzione per il conflitto in Donbass. Ipotizziamo che le accuse infondate rivolte da Mosca al governo di Volodymyr Zelensky, riguardo un presunto massacro di civili russofoni in Ucraina orientale e la violazione unilaterale degli accordi di Minsk, mantengano oggi una maggiore credibilità rispetto ad altre narrazioni usate in passato per giustificare l'invasione russa. Ad esempio, nel precedente ciclo di ricerca, il complotto sui *biolabs*, presunti laboratori di armi batteriologiche presenti sul territorio ucraino e finanziati dagli Stati Uniti, era risultato di centrale importanza nella rappresentazione filorussa della guerra in Ucraina. Ad oggi, le teorie sui *biolabs* risultano relegate a una nicchia cospirazionista e hanno perso importanza. La narrazione distorta della guerra in Donbass resta invece un pilastro della disinformazione presente sia sui *social* che sui *mainstream media*. Alla luce di queste considerazioni, sembrerebbe necessario investire in una campagna di informazione sulle vicende del separatismo delle regioni di Lugansk e Donetsk a partire dal 2014, per fare chiarezza sul ruolo del governo di Vladimir Putin nella destabilizzazione dell'Ucraina sud-orientale.

Infine, si segnala la vulnerabilità degli utenti su Telegram e Facebook. I primi possono essere esposti a contenuti sensibili, raffiguranti cadaveri, decapitazioni, abusi avvenuti in zone di guerra, ed entrare in contatto diretto con i canali dei propagandisti militari russi, grazie al lavoro di traduzione svolto dagli *influencer* italiani. Su Facebook, gli utenti rischiano invece di incorrere in teorie cospirazioniste attraverso i *post* sponsorizzati dalla piattaforma. Nonostante l'impegno di Facebook nel bloccare le pubblicità che promuovono disinformazione, il controllo sui contenuti sponsorizzati risulta ancora permeabile alla propaganda filorussa.



**Bibliografia**

*Case of Ukraine and The Netherlands ν. Russia*, No. 8019/16, 43800/14 and 28525/20 (European Court of Human Rights 25 gennaio 2023).

*Clickbait*, in *Merriam Webster Dictionary*. Merriam-Webster, https://www.merriam- webster.com/dictionary/clickbait

Di Noto, Antonio, *No! Zelensky non ha preteso che i figli degli statunitensi vadano a combattere in Ucraina*, Open Online, 2 marzo 2023. https://www.open.online/2023/03/02/frase-zelensky-figli-usa-ucraina- fc/#:~:text=%C2%ABGli%20Stati%20Uniti%20dovranno%20inviare,Zelensky%20da%20nume rosi%20utenti%20social

EUvsDisinfo, *1st EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a framework for networked defence*, febbraio 2023. https://euvsdisinfo.eu/uploads/2023/02/EEAS-ThreatReport-February2023-02.pdf

Financial Times, *Full text of the Minsk agreement*, 12 febbraio 2015. https://www.ft.com/content/21b8f98e-b2a5-11e4-b234-00144feab7de

Fry, Elizabeth, *Persuasion Not Propaganda: Overcoming Controversies of Domestic Influence in NATO Military Strategic Communications,* Defence Strategic Communications 11 (2022), pp. 177–213. https://doi.org/10.30966/2018.RIGA.11.6

Gennaro, Michelangelo, *Le cospirazioni sullo schianto in elicottero del ministro Monastyrskyi*, Italian Digital Media Observatory, 23 gennaio 2023. https://www.idmo.it/2023/01/23/le-cospirazioni-sullo-schianto-in-elicottero-del-ministro-monastyrskyi/

Goodman, Jack, e Olga Robinson, *Putin's mysterious Facebook "superfans" on a mission*, BBC, 11 aprile 2022. https://www.bbc.com/news/blogs-trending-61012398

Graziosi, Andrea, *L'ucraina e Putin. Tra storia e ideologia*, Bari: Laterza, 2022.

Hildebrandt, Tina, e Giovanni Di Lorenzo, *Hatten Sie gedacht, ich komme mit Pferdeschwanz?*, Die Zeit, 7 dicembre 2022. https://www.zeit.de/2022/51/angela-merkel-russland-fluechtlingskrise- bundeskanzler

Mallamaci, Antonino, *Russia e Ucraina, ecco le nuove armi della info-war digitale, Agenda Digitale*, 30 settembre 2022. https://www.agendadigitale.eu/cultura-digitale/russia-e-ucraina-ecco-le- nuove-armi-della-info-war-digitale/

Mastroianni, Filippo, *L'Ucraina, la Russia e la questione linguistica spiegata in tre mappe, Il Sole 24 Ore*, 1 marzo 2022. https://www.infodata.ilsole24ore.com/2022/03/01/lucraina-la-russia-e-la- questione-linguistica-spiegata-in-tre- grafici/#:☒:text=La%20lingua%20ufficiale%20dell'Ucraina,sono%20madrelingua%20di%20altr e%20lingue

Meaker, Morgan, *How the Kremlin Infiltrated Russia's Facebook*, Wired UK, 1 giugno 2022. https://www.wired.co.uk/article/vk-russia-democracy

Mikhelidze, Nona, *Tutte le post verità dell'articolo di Ranieri smontate da Nona Mikhelidze*, Liberi Oltre le Illusioni, 22 maggio 2023. https://www.liberioltreleillusioni.it/news/articolo/tutte-le-post- verita-dellarticolo-di-ranieri-smontate-da-nona-mikhelidze

Nava, Massimo, *La verità della guerra, secondo Merkel*, Corriere della Sera, 16 dicembre 2022. https://www.corriere.it/esteri/22_dicembre_16/verita-guerra-merkel-d4c3efe6-7d38-11ed-93d0-fd9373385b22.shtml

Organisation for Economic Cooperation and Development, *Disinformation and Russia's war of aggression against Ukraine. Threats and governance responses*, 3 novembre 2022. https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of- aggression-against-ukraine-37186bde/

Paul, Christopher, e Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model. Why It Might Work and Options to Counter It*, Rand Corporation, 2016. https://www.rand.org/pubs/perspectives/PE198.html

Petrangeli, Guido, *Info-defense, un network di traduttori sta inondando l'Europa con la propaganda di Mosca*, HuffPost Italia, 28 luglio 2022.https://www.huffingtonpost.it/blog/2022/07/18/news/come_un_network_di_traduttori_sta_inond ando_leuropa_con_la_propaganda_di_mosca-9868602/

State Statistics Committee of Ukraine, *All-Ukrainian population census 2001*, http://2001.ukrcensus.gov.ua/eng/

Technology and Social Change Project, *The Media Manipulation Casebook. Code Book*, Harvard Kennedy School Shorese in Center on Media, Politics and Public Policy, 20 aprile 2021. https://mediamanipulation.org/sites/default/files/media-files/Code-Book-1.2-April-21-2021.pdf

UN Office of the High Commissioner for Human Rights, *Conflict-related civilian casualties in Ukraine*, 27 gennaio 2022. https://ukraine.un.org/sites/default/files/2022-02/Conflict- related%20civilian%20casualties%20as%20of%2031%20December%202021%20%28rev%202 7%20January%202022%29%20corr%20EN_0.pdf

# Sezione giuridica della ricerca

## Contenuti, scopi e traiettoria della ricerca: le nuove frontiere della *compliance* nel mercato digitale

**di A. Gullo, Direttore della ricerca**

La lotta alla disinformazione deve necessariamente incentrarsi sul coinvolgimento proattivo delle piattaforme e sulla *partnership* pubblico-privato. Questo approccio è dettato dall'uso (limitato) che deve essere fatto dello strumento penale in un settore per definizione sensibile, in cui si staglia sullo sfondo la necessità di non limitare la libertà di espressione. Il punto di partenza è che lo *ius terribile* non può essere utilizzato per sanzionare la mera diffusione di notizie false e proteggere di per sé la sola veridicità dell'informazione, a meno che tali condotte non arrechino pregiudizio ad altri beni giuridici meritevoli di tutela penale. Occorre, però, che il mandato in tal senso conferito alle piattaforme non assuma le caratteristiche di una 'delega in bianco'. Al contrario, è necessario che il potere di autonormazione e autoorganizzazione in funzione preventiva delle *corporation* sia esercitato entro i confini di una cornice pubblicistica di riferimento, in grado di delineare con sufficiente precisione le regole del gioco. È questo il nocciolo duro dell'analisi svolta nel corso dei primi due cicli della sezione giuridica di questa ricerca[1]; si tratta adesso di proiettare lo sguardo verso l'attuale orizzonte normativo che, come noto, vive una stagione di cambiamento.



Il riferimento è naturalmente al Regolamento (UE) 2022/2065 relativo al mercato unico dei servizi digitali (*Digital Services Act* - DSA) del 19 ottobre 2022, che ha cercato di rispondere proprio all'esigenza, sopra ricordata, e da più parti evocata, di regolamentare i modelli di *business* digitale nel tentativo di bilanciare il libero sviluppo di simili attività economiche nell'EU *single market* con la tutela dei rilevanti interessi individuali e collettivi (dal benessere psico-fisico della persona, alla tutela dell'integrità dei processi elettorali, fino a salute e sicurezza pubbliche) su cui tali nuove dinamiche sociali e di mercato sono in grado, come noto, di incidere significativamente.

[1] V., per una sintesi, il contributo di apertura della sezione del fascicolo (n. 4/2021) della rivista *Diritto penale contemporaneo – Rivista trimestrale* in cui sono stati pubblicati gli esiti del primo ciclo della ricerca (cui si rinvia, unitamente ai tre lavori pubblicati in tale rapporto finale e richiamati nelle note successive, per tutti i riferimenti anche bibliografici): A. GULLO, G. PICCIRILLI, *Disinformazione e politiche pubbliche: una introduzione,* in *Dir. pen. cont. – Riv. Trim.*, 2021, 4, 248 ss. Il report del secondo ciclo di studi è invece reperibile al seguente link: https://www.esteri.it/wp- content/uploads/2022/09/LUISS-Come-individuare-e-contrastare-operazioni-coordinate-di-disinformazione-in- Italia.pdf

L'obiettivo di fondo è duplice: da un lato, fornire al lettore e alle organizzazioni cui questo studio è rivolto una 'guida ragionata' per muoversi all'interno delle molteplici novità normative introdotte dal Regolamento e per avere un quadro delle peculiari responsabilità di *enforcement* previste a loro carico; dall'altro lato, rimodulare – alla luce di tale importante riforma – le indicazioni di *policy* finali per istituzioni pubbliche e private formulate nel corso dei primi due anni del progetto di ricerca, al fine di aiutare i vari attori del sistema a identificare le migliori pratiche per assicurare un contrasto efficace alle azioni (coordinate e non) di disinformazione.

L'analisi sarà quindi divisa in tre capitoli volti a esaminare le altrettante macro-sezioni d'interesse in cui si articola il DSA, cercando altresì di evidenziarne punti di forza e limiti anche tenuto conto degli esiti dei precedenti cicli dell'indagine.

La prima parte[2] si concentrerà sul regime di responsabilità dei *provider* e su alcuni specifici obblighi di *compliance* gravanti su tali operatori soprattutto per quanto attiene alla cooperazione con le autorità pubbliche. Si avrà qui modo di constatare tra l'altro come, a fronte della decisione di confermare quella che è ormai una impostazione consolidata della materia, e cioè l'assenza di obblighi generali di sorveglianza a carico dei fornitori, il DSA preveda alcune novità in punto sia di definizione di alcuni singoli profili della c.d. esenzione condizionata da responsabilità degli operatori, sia in termini, *inter alia*, di nuovi obblighi di attivazione (ad es. con riferimento alla doverosa notifica di sospetti reati che comportino una minaccia per la vita o la sicurezza di una o più persone, di cui il *provider* venga a conoscenza, ai sensi e per gli effetti dell'art. 18 del Regolamento).

Il secondo contributo[3], poi, sarà dedicato allo studio dell'impatto del DSA sulle attività di *private enforcement* dei soggetti regolati rispetto alla moderazione dei contenuti immessi in rete dagli utenti. A differenza di quanto accaduto per il modello di responsabilità del provider, da questo angolo visuale le innovazioni sono molte e di grande rilievo, avendo qui il legislatore europeo cercato di costruire quella cornice normativa pubblicistica, cui pocanzi si alludeva, entro la quale le piattaforme esercitano la loro potestà di regolare, tra l'altro, il dibattito pubblico e il confronto politico che si svolge nelle rispettive warene digitali.



Obiettivo, quest'ultimo, che viene perseguito scommettendo sui paradigmi, sulle prassi, sulle metodiche della *corporate compliance*, con la significativa decisione di diversificare le *due diligence obligation* degli operatori attraverso una peculiare struttura di adempimenti a strati progressivi, in cui, nel passaggio da un livello all'altro, il regolatore eurounitario stabilisce man mano obblighi più stringenti al crescere dell'importanza strategica del soggetto regolato (che si aggiungono, e non si sostituiscono a quelli dei livelli precedenti): dalle previsioni minimali valide per tutti i prestatori di servizi intermediari fino all'anello finale delle misure concernenti esclusivamente le c.d. VLOPs (*Very Large Online Platforms*) e i c.d. VLOSEs (*Very Large Online Search Engines*). Si va, a seconda dei casi, dagli obblighi in punto di definizione di termini e condizioni del servizio, di predisposizione di meccanismi di *notice and action* e di sistemi interni di gestione dei reclami, fino a quelli di valutazione e gestione dei rischi a carattere sistemico legati ai servizi digitali, sottoposizione ad *audit* indipendenti, istituzione di una specifica funzione aziendale di DSA *compliance*, e via discorrendo.

[2] V. il cap. 1 di questa di L. D'Agostino, *Disinformazione e obblighi di* compliance *degli operatori del mercato digitale alla luce del nuovo* Digital Services Act.

[3] Cfr. E. Birritteri, *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* (cap. 2 di questa sezione).

Questa scelta, per certi versi, è esemplificativa della natura 'liquida' della *compliance*, capace di imporsi sempre più come modello di regolazione vincente in diversi settori e a carattere trasversale (costituendo la cifra distintiva oramai di numerosi ambiti di disciplina, tra cui sicurezza sul lavoro, *privacy*, responsabilità da reato degli enti). Ciò, peraltro, secondo cadenze che vedono sempre più il settore di volta in volta toccato dall'innesto della logica della *compliance* preventiva conformarsi alle note distintive di questo particolare meccanismo di gestione del rischio, latamente inteso, piuttosto che il contrario. Insomma, è l'ambito in cui la *compliance* viene importata a essere plasmato da queste metodologie – fatte di processi e procedure, analisi e gestione del rischio, monitoraggi tramite un sistema strutturato di controlli e revisioni –, che invece percorrono 'indenni' gli ordinamenti e i contesti in cui vengono applicate, senza mutare il proprio DNA.

L'ultima sezione della ricerca[4], infine, è dedicata all'*enforcement* pubblico del Regolamento, sia per ciò che concerne i poteri assegnati agli Stati membri, sia avuto riguardo a quelli conferiti alla Commissione europea, che assume il ruolo di interlocutore privilegiato per i procedimenti sanzionatori riguardanti le piattaforme online e i motori di ricerca online di 'dimensioni molto grandi'. Come si vedrà, anche da tale versante il 'vento del cambiamento' ha soffiato forte, dal momento che la riforma cerca di sperimentare paradigmi punitivi peculiari, ispirati talvolta anche al modello ingiunzionale e alla volontà di testare forme più o meno strutturate di soluzioni negoziali in relazione all'inosservanza del DSA, in un certo senso non dissimili da prassi largamente in uso in alcuni ordinamenti sul terreno della *corporate criminal liability*.

Soltanto l'esperienza applicativa potrà dirci se quello imboccato dal legislatore europeo sarà un percorso in grado di dare i frutti sperati. Il compito che ci si proponeva, del resto, non era e non sarà semplice specie allorquando, dalla prospettiva della *law in the books*, le nuove regole unionali si confronteranno con le dinamiche applicative.



Senza dubbio, però, il DSA colma finalmente una lacuna che, unitamente alle prospettive che oggi si stanno aprendo avuto riguardo *all'Artificial Intelligence Act*, rende l'Unione europea – e il suo *acquis* normativo che in questi casi assume carattere quasi pioneristico – un punto di riferimento fondamentale nello scenario globale.

[4] V. R. Sabia, *L'*enforcement *pubblico del* Digital Services Act *tra Stati membri e Commissione europea: implementazione, monitoraggio e sanzioni* (cap. 3 di questa sezione).

# Capitolo 1

## Disinformazione e obblighi di *compliance* degli operatori del mercato digitale alla luce del nuovo *Digital Services Act*

**di L. D'Agostino**

SOMMARIO

# 1

## 1 Cenni introduttivi su oggetto, ambito di applicazione e definizioni del DSA

Lo scorso 27 ottobre 2022 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il Regolamento 2022/2065/UE relativo al mercato dei servizi digitali (c.d. *Digital Services Act*, DSA) che, sebbene già in vigore, sarà applicabile[1] a decorrere dal 17 febbraio 2024. Il nuovo Regolamento rientra nel pacchetto di misure per l'attuazione della strategia europea per il digitale, che comprende ambiti piuttosto vasti e variegati[2]. L'*iter* legislativo è stato al centro di un accesso dibattito politico, che ha condotto alla formulazione di numerosi emendamenti al testo rallentando di fatto l'approvazione finale. Il DSA ha quale principale oggetto la rivisitazione dell'intera disciplina dei servizi digitali nell'Unione, con particolare riguardo ai c.d. "servizi di intermediari"[3] di contenuti, prodotti e servizi, messi a disposizione degli utenti della rete[4]. L'obiettivo è quello di incentivare la crescita del mercato interno e porre le basi per un ambiente digitale sicuro ed affidabile a garanzia dei diritti degli utenti[5], a fronte dei profondi mutamenti della tecnologia dell'ultimo ventennio. L'affermazione di nuovi modelli di *business* e servizi innovativi, quali i *social network* e le piattaforme online[6], rendeva indifferibile – secondo la Commissione – la rivisitazione della disciplina dettata dalla Direttiva 2000/31/CE sul commercio elettronico, che nel corso degli anni era stata in parte "superata" dai legislatori nazionali.



[1] Tenuto conto della complessità della normativa e dei nuovi, numerosi adempimenti a carico del *provider*, il legislatore europeo ha differito la data di efficacia delle disposizioni del DSA, al fine di permettere ai destinatari della disciplina di conformarsi ad essa. Cfr. Art. 93 DSA

[2] Nei primi mesi del 2020 la Commissione europea aveva presentato un pacchetto di proposte per promuovere e sostenere la transizione digitale, preannunciando la presentazione di una proposta di Regolamento in materia di mercati e servizi digitali. Nella strategia era corredata da una comunicazione quadro circa le iniziative da intraprendere per il potenziamento della connettività, per incentivare le imprese e potenziare le competenze digitali degli europei. Per approfondimenti v. *La nuova strategia dell'UE per il digitale*, Dossier della Camera dei Deputati n° 32 del 30 aprile 2020, in https://documenti.camera.it

[3] Ai sensi dell'art. 3, par. 1, lett. g) è "servizio intermediario" qualsiasi servizio della società dell'informazione che consiste nel semplice trasporto di dati (*mere conduit*), nella memorizzazione temporanea (*caching*), o nella memorizzazione stabile (*hosting*). Per approfondimenti sulle figure di *provider* sia consentito rinviare a D'Agostino L., *Disinformazione e responsabilità delle piattaforme. Obblighi di attivazione e misure di compliance*, in *Diritto Penale Contemporaneo – Rivista Trimestrale*, 2021, 4, 285 ss.

[4] Nel dettaglio, il Regolamento si applica ai servizi intermediari offerti a destinatari «il cui luogo di stabilimento si trova nell'Unione o che sono ubicati nell'Unione, indipendentemente dal luogo di stabilimento dei prestatori di tali servizi intermediari». La definizione di "servizio della società dell'informazione" è contenuta nell'art. 1, par. 1, lett. b) della Direttiva 2015/1535/UE: «qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi».

[5] Cfr. Considerandum n. 2 e 3 DSA.

[6] Il mutamento più significativo è consistito nell'espansione della c.d. *platform economy*, che ha portato alla nascita di nuove Big Tech Companies (es. Meta, Amazon). Le piattaforme di grandi dimensioni rappresentano oggi il principale mezzo per la diffusione di contenuti illeciti e/o per la vendita *online* di beni o servizi illegali, in quanto fungono da "aggregatori" per molti altri operatori commerciali.

Particolarmente avvertita era l'esigenza di imporre in capo ai *provider* specifici obblighi di condotta per prevenire la diffusione di contenuti illegali e il fenomeno della disinformazione online; ciò aveva condotto all'emanazione di normative nazionali diversificate e "asimmetriche", che mal si conciliavano con il carattere transfrontaliero di Internet e delle tecnologie informatiche. In buona sostanza, il nuovo Regolamento interviene allo scopo di uniformare le normative nazionali in un contesto socioeconomico caratterizzato dalla presenza di piattaforme e aggregatori di mercato, sul presupposto dell'esistenza di nuovi e rilevanti rischi derivanti dall'attività di tali soggetti. Pur confermando, in generale, l'(ir)responsabilità dei prestatori di servizi intermediari[7], il legislatore europeo ha introdotto una disciplina articolata sui c.d. obblighi di diligenza rivolti a determinate categorie di *provider*[8], prevendendo altresì un articolato apparato sanzionatorio e una specifica disciplina di attuazione del DSA[9].

Circa l'ambito soggettivo di applicazione, il Regolamento 2022/2065/UE si rivolge a figure di *provider* diverse per tipologia e per dimensioni, secondo uno schema "a piramide inversa"[10]: il soggetto che si trovi al livello più alto dovrà osservare, oltre alle disposizioni specifiche per la propria attività, anche quelle dettate per i soggetti collocati ai vertici inferiori. Mentre alcune disposizioni si applicano a tutti coloro che prestano servizi intermediari[11], altre soltanto ai *provider* di servizi di *hosting*[12]. A un livello superiore si collocano le piattaforme online, una *species* del più ampio *genus* degli *hosting provider*, la cui attività si caratterizza per la diffusione al pubblico delle informazioni memorizzate[13]; ad esse sono rivolte disposizioni aggiuntive finalizzate a contenere i rischi derivanti dalla pubblicazione di *user-generated contents*[14].

Vi sono poi disposizioni applicabili alle piattaforme online per la conclusione di contratti a distanza con operatori commerciali terzi, al fine di tutelare gli utenti nella fruizione di servizi di *marketplace online*[15].

[7] Sul tema di recente Braschi S., *Il nuovo Regolamento sui servizi digitali: quale futuro per la responsabilità degli Internet Service Provider?*, in *Diritto penale e processo*, 2023, 3, 367-377.

[8] Capo II (artt. 4-10) e III (artt. 11-48) DSA.

[9] Capo IV, artt. 49 e seguenti DSA.

[10] La metafora è utilizzata da Tassone B., *L'impatto del DSA sull'ordinamento italiano*, in *Diritto di Internet*, 2023, 1, 6 ss. L'architettura del nuovo Regolamento può anche essere descritta come un sistema di cerchi concentrici, in cui ciascun soggetto collocato nella circonferenza esterna è tenuto a rispettare tutte le disposizioni rivolte ai soggetti collocati nei perimetri interni.

[11] Si veda in particolare la prima sezione del Capo III, che pone in capo a tutti gli intermediari l'obbligo di designare un punto di contatto unico, e di stabilire termini e condizioni contrattuali conformi al DSA (art. 14). Essi sono inoltre tenuti a pubblicare, almeno una volta all'anno, relazioni chiare e facilmente comprensibili sulle attività di moderazione dei contenuti (art. 15).

[12] Sugli *hosting provider* gravano, oltre ai doveri previsti in generale per tutti gli intermediari, anche altri obblighi, tra cui quello di predisporre meccanismi di segnalazione di contenuti illegali (art. 16), di fornire una motivazione sulle restrizioni imposte agli utenti (art. 17), e di notificare il sospetto che si stia per commettere un reato (art. 18).

[13] Si prevede tuttavia una deroga qualora tale attività sia «una funzione minore e puramente accessoria di un altro servizio o funzionalità minore del servizio principale e, per ragioni oggettive e tecniche, non possa essere utilizzata senza tale altro servizio e a condizione che l'integrazione di tale funzione o funzionalità nell'altro servizio non sia un mezzo per eludere l'applicabilità del presente regolamento» (art. 3, par. 1, lett. i). Ad esempio, la sezione relativa ai commenti di un quotidiano online potrebbe rientrare nella deroga, ove sia evidente che è accessoria al servizio principale rappresentato dalla pubblicazione di notizie sotto la responsabilità editoriale dell'editore.

[14] Trattasi in particolare dell'obbligo di predisporre un sistema interno di gestione dei reclami (art. 20), di attuare misure di protezione contro gli abusi (art. 23), e di pubblicare informazioni sugli esiti delle attività di moderazione. Le piattaforme sono inoltre destinatarie delle disposizioni in materia di pubblicità (art. 26) e trasparenza dei sistemi di raccomandazione (art. 27).

[15] Figurano in particolare gli obblighi di tracciabilità degli operatori commerciali (art. 30) e di predisposizione di interfacce adeguate per assolvere alle informazioni precontrattuali e assicurare la conformità e la sicurezza dei prodotti (art. 31). Tali piattaforme dovranno anche informare l'utente laddove riscontrino che un prodotto o servizio illegale è stato offerto da un operatore commerciale per il tramite dei propri servizi (art. 32).

Al quinto e ultimo livello della piramide si collocano le piattaforme online di grandi dimensioni (c.d. VLOP) e i motori di ricerca i quali, a causa delle proprie dimensioni[16], sono tenuti a prevenire e mitigare la gestione i rischi sistemici relativi alla propria attività[17].

Il presente contributo vuole fornire, senza pretese di esaustività, una panoramica dei principali obblighi di *compliance* introdotti dal nuovo Regolamento a carico dei prestatori di servizi, con particolare riguardo alle disposizioni contenute nel Capo III.

## 2 Responsabilità ed obblighi dei prestatori di servizi intermediari alla luce del DSA: inquadramento generale

Conviene anticipare che le disposizioni contenute nel Capo II sulla "responsabilità dei prestatori di servizi intermediari" si pongono in una linea di sostanziale continuità con la disciplina previgente. Analogamente all'assetto normativo delineato dalla Direttiva 2000/31/CE[18], il nuovo Regolamento si ispira al regime c.d. di responsabilità limitata del *provider*, fondato sull'assenza di un dovere generalizzato di sorveglianza e sul modello del *notice and take down*.

Per l'attività di semplice trasporto (*mere conduit*), si prevede che il prestatore non sia responsabile delle informazioni trasmesse alla triplice condizione che: «non dia origine alla trasmissione; non selezioni il destinatario della trasmissione; e non selezioni né modifichi le informazioni trasmesse»[19].

Per l'attività di memorizzazione intermedia e temporanea di informazioni effettuata allo scopo di rendere più efficace il suo successivo inoltro ad altri destinatari che ne hanno fatto richiesta (*caching*), è dettata una disciplina più articolata a mente della quale il prestatore non è responsabile purché: «non modifichi le informazioni; si conformi alle condizioni di accesso alle informazioni; si conformi alle norme sull'aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore; non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni; e agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso alle stesse, non appena venga effettivamente a conoscenza del fatto che le informazioni all'origine della trasmissione sono state rimosse dalla rete o che l'accesso alle informazioni è stato disabilitato, oppure che un organo giurisdizionale o un'autorità amministrativa ha ordinato la disabilitazione dell'accesso a tali informazioni o ne ha disposto la rimozione» (art. 5 DSA). Disposizioni analoghe disciplinano l'attività di memorizzazione di informazioni fornite dal destinatario del servizio (*hosting*), rispetto alla quale la esimente di responsabilità opera a condizione che il prestatore: «non sia effettivamente a conoscenza delle attività o dei contenuti



[16] Le disposizioni della Sezione V si applicano alle sole piattaforme online e ai motori di ricerca che hanno un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a 45 milioni e che sono designati come piattaforme online di dimensioni con atto della Commissione europea.

[17] Soltanto in capo a tali soggetti sono posti obblighi *risk assessment/management* (artt. 34 e 35), di risposta alle crisi (art. 36) e di effettuazione di audit periodici (art. 37). Si prevedono inoltre misure di *compliance* più incisive per quanto riguarda, ad esempio, la trasparenza nelle pubblicità (art. 39), l'accesso ai dati (art. 40).

[18] Cfr. artt. 12-15 (Sezione IV, Capo II)

[19] Con la precisazione che le attività di trasmissione e di fornitura di accesso includono la memorizzazione automatica, intermedia e transitoria delle informazioni, a condizione che questa serva solo alla trasmissione sulla rete di comunicazione e che la sua durata non ecceda il tempo ragionevolmente necessario a tale scopo (Art. 4 DSA).

illegali e, per quanto attiene a domande risarcitorie, non sia consapevole di fatti o circostanze che rendono manifesta l'illegalità dell'attività o dei contenuti; oppure non appena venga a conoscenza di tali attività o contenuti illegali o divenga consapevole di tali fatti o circostanze, agisca immediatamente per rimuovere i contenuti illegali o per disabilitare l'accesso agli stessi» (art. 6 DSA). Anche questa norma, come le precedenti, non ha ricevuto significativi cambiamenti rispetto al testo della Direttiva, dal quale si differenzia unicamente in relazione alla responsabilità prevista dalla normativa in materia di protezione dei consumatori, per le piattaforme online che consentono ai consumatori di concludere contratti a distanza con operatori commerciali. Qualora tali piattaforme online inducano il consumatore medio a ritenere che il prodotto o il servizio acquistato online sia fornito dalla piattaforma stessa o da un operatore commerciale che agisce sotto l'autorità o il controllo del *provider*, non troverà applicazione la predetta esimente di responsabilità[20].

Quale che sia la specifica attività svolta dal prestatore, il DSA ripropone la clausola generale per cui gli organi giurisdizionali e le autorità amministrative possono esigere che il prestatore del servizio impedisca o ponga fine a una violazione[21].

Per quanto la formulazione delle disposizioni in esame non abbia subito rilevanti modifiche rispetto al passato, il legislatore italiano sarà tenuto ad adeguare l'ordinamento interno in considerazione della diretta applicabilità del Regolamento. In linea con quanto già avvenuto in casi analoghi[22], la via più semplice sarà quella di abrogare *sic et simpliciter* le disposizioni del Codice del commercio elettronico che trovano oggi compiuta disciplina nel DSA, tra cui quelle relative alla responsabilità del *provider* (artt. 14 e seguenti).

## 2.1 Assenza di obblighi generali di sorveglianza ed esecuzioni di ordini di contrastare contenuti illegali e fornire informazioni: il nuovo "vecchio" impianto generale



All'art. 8 il nuovo Regolamento ribadisce il principio generale secondo cui «ai prestatori di servizi intermediari non è imposto alcun obbligo generale di sorveglianza sulle informazioni che tali prestatori trasmettono o memorizzano, né di accertare attivamente fatti o circostanze che indichino la presenza di attività illegali»[23]. Dalla prospettiva penalistica tale disposizione viene richiamata per escludere la

[20] Opera in tal caso una sorta di presunzione, considerandosi come se il prodotto o il servizio siano stati resi direttamente dalla piattaforma, e non da un operatore terzo. Il *provider* non potrà pertanto invocare a propria discolpa (ad es. in caso di vendita di beni illegali o contraffatti) di non essere stato effettivamente a conoscenza dell'illiceità delle attività o dei contenuti. Si tratta di una disposizione all'apparenza problematica, specialmente laddove venga in rilievo la responsabilità penale dei soggetti coinvolti. A tal fine non è chiaramente sufficiente il mero dato esteriore dell'apparenza di un prodotto "come se fosse proprio del provider", dovendosi accertare l'esistenza in concreto dell'elemento soggettivo de reato (monosoggettivo o concorsuale).

[21] É stato invece soppresso l'inciso – contenuto dell'art. 14, par. 3, della Direttiva – che riconosceva agli Stati membri la possibilità di «definire procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime». L'eliminazione è probabilmente frutto di un coordinamento con altre disposizioni del DSA (cfr. art. 14 ss.), che impongono obblighi di compliance in capo a tutti gli intermediari.

[22] Può citarsi, ad esempio, l'adeguamento al Regolamento 679/2016/ UE attuato con D. Lgs. 101/2018, con cui il legislatore italiano ha abrogato le disposizioni del Codice della privacy adottate in recepimento della precedente Direttiva 46/95/CE.

[23] Tale disposizione riproduce senza significative novità il disposto dell'art. 15 della Direttiva 2000/31/CE, secondo cui «nella prestazione dei servizi di cui agli articoli 12, 13 e 14, gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite». Cfr. art. 17 D. Lgs. 70/2003

sussistenza di una posizione di garanzia in capo al *provider*, che dunque non potrà rispondere per omesso impedimento del reato commesso dall'utente[24]. Nell'impianto normativo precedente tale principio era temperato dalla previsione di un dovere di collaborazione con la pubblica autorità, laddove il *provider* venga a conoscenza di presunte attività o informazioni illecite, dovendo comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi[25].

Circa i doveri di attivazione del *provider* la disciplina dettata dal DSA appare decisamente più analitica. Si precisa, anzitutto, che gli intermediari non perdono la loro veste di "neutralità" per il solo fatto di svolgere, in buona fede e in modo diligente[26], indagini volontarie di propria iniziativa o di adottare altre misure volte a individuare, identificare e rimuovere contenuti illegali o a disabilitare l'accesso agli stessi. Parimenti l'esenzione di responsabilità non viene meno nel caso in cui essi adottino misure interne per conformarsi alle prescrizioni del diritto dell'Unione e del diritto nazionale[27].

Le novità più significative sono contenute negli articoli 9 e 10 aventi ad oggetto, rispettivamente, gli ordini di contrastare i contenuti illegali e di fornire informazioni. Il primo impone agli ISP di informare senza indebito ritardo l'autorità delle iniziative intraprese per contrastare[28] uno o più specifici contenuti illegali, specificando se e quando è stato dato seguito all'ordine. Per esigenze di chiarezza nelle relazioni con l'intermediario, il nuovo Regolamento ha cura di precisare che l'ordine deve essere motivato sugli elementi di diritto da cui si desume l'illiceità del contenuto, con rinvio a una o più disposizioni specifiche del diritto nazionale o unionale. Esso deve inoltre includere sufficienti elementi per individuare con esattezza e localizzare i contenuti illegali (quali, ad es., uno o più URL esatti e, se necessario, informazioni supplementari). Inoltre, per garantire una tutela effettiva dei diritti del *provider* e dell'utente, l'ordine in questione deve contenere una informativa sui meccanismi di ricorso a disposizione degli interessati[29]. Graverà sul *provider* l'onere di informare l'utente, immediatamente dopo l'esecuzione dell'ordine o nel diverso termine in esso stabilito, indicando le motivazioni addotte dall'Autorità e i mezzi di impugnazione esperibili.



[24] Per approfondimenti sull'assenza dell'obbligo generale si sorveglianza sia consentito rinviare a L. D'Agostino, *Disinformazione e responsabilità delle piattaforme. Obblighi di attivazione e misure di compliance*, cit., 290. In letteratura v. anche F. Resta, *La responsabilità penale del provider: tra laissez faire ed obblighi di controllo*, in *Giurisprudenza di merito*, 2010, 9, 1715 ss.; A. Ingrassia, *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?* in L. Luparia (a cura di), *Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012, 15 ss; R. Bocchini, *La responsabilità di Facebook per la mancata rimozione dei contenuti illeciti*, in *Responsabilità civile e previdenza*, 2017, 536 ss.; B. Panattoni, *Il sistema di controllo successivo: obbligo di rimozione dell'ISP e meccanismi di notice and take down*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2018, 5, 249 ss.

[25] Ai sensi dell'art. 17, comma 2, D. Lgs. 70/2003 il prestatore è infatti tenuto: (i) ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione; (ii) a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi.

[26] Secondo S. Braschi, *Il nuovo Regolamento sui servizi digitali: quale futuro per la responsabilità degli Internet Service Provider?*, cit., 370, il significato di questa previsione risulta più chiaro alla luce di quella giurisprudenza che ha valorizzato l'adozione di meccanismi di filtraggio preventivi per affermare il carattere non neutrale dell'attività svolta dal *provider*, così da far venire meno l'esenzione di responsabilità previsto dalla direttiva 31/2000/CE.

[27] Cfr. art. 7 DSA.

[28] Si ritiene che la nozione di "contrastare" i contenuti illegali abbia contenuto ampio, e come tale legittimi la richiesta dell'autorità di rimozione del contenuto o la disabilitazione dell'accesso.

[29] Viene inoltre precisato che l'autorità emittente è tenuta a indicare l'ambito di applicazione territoriale dell'ordine, in misura strettamente necessaria per conseguire l'obiettivo. L'ordine sarà trasmesso in una delle lingue dichiarate dal prestatore dei servizi intermediari, ed è inviato al punto di contatto designato conformemente all'art. 11 DSA.

La medesima procedura si applica anche nel caso in cui l'intermediario sia raggiunto da un ordine di fornire informazioni *ex* art. 10 DSA[30]. In questi casi dovrà avvisare l'autorità emittente sulle misure intraprese, informando contestualmente l'utente sulle motivazioni contenute nell'ordine e sulla possibilità di presentare un ricorso.

A chiusura delle disposizioni si prevede che «le condizioni e le prescrizioni di cui al presente articolo non pregiudicano il diritto civile e il diritto processuale penale nazionale»[31]. Tale clausola di salvaguardia dà adito a dubbi sulle conseguenze della violazione delle regole procedurali sopra descritte. La *ratio* della disposizione appare quella di evitare interferenze con materie strettamente domestiche; così, ad esempio, non potrebbe determinarsi alcuna causa di invalidità o illegittimità delle prove ottenute dalla pubblica autorità in spregio alle garanzie previste dagli articoli in commento. Parimenti, gli ordini di fornire informazioni e contrastare contenuti illegali sembrerebbero "derogabili", laddove l'autorità agisca in ossequio alle norme processuali penali nazionali.

## 2.2 Obblighi in punto di definizione di termini e condizioni, trasparenza, *notice and action* (rinvio)

Il Capo III del Regolamento introduce nuovi adempimenti per tutti i prestatori di servizi intermediari, tra cui quello di designare "punti di contatto" per le comunicazioni con le autorità degli Stati membri (art. 11) e con gli utenti del servizio (art. 12), e di nominare rappresentanti legali[32].

Il DSA definisce poi i doveri di diligenza per un ambiente online trasparente e sicuro, tra cui spicca l'obbligo per tutti i *provider* di prevedere nelle condizioni generali di contratto le restrizioni sui contenuti caricati dagli utenti, con indicazione specifica delle procedure e delle misure utilizzate ai fini della moderazione dei contenuti (art. 14). Quanto agli obblighi informativi, si prevede che tutti i prestatori di servizi – eccetto quelli che si qualificano come microimprese o piccole imprese – debbano pubblicare almeno una volta all'anno un *report* sulle attività di moderazione dei contenuti, che includa anche il numero di segnalazioni ricevute dalle autorità e dagli utenti per ciascuna tipologia di contenuto illegale, le eventuali azioni intraprese a seguito della notifica, nonché il numero dei reclami presentati dagli utenti (art. 15).

Se il *provider* offre servizi di *hosting*, dovrà dotarsi anche di meccanismi di *notice and action* per consentire a qualsiasi soggetto di denunciare la presenza di contenuti illegali. La segnalazione dell'utente fa sorgere, per espressa previsione dell'art. 16, par. 3, DSA, «una conoscenza o consapevolezza effettiva ai fini dell'articolo 6 in relazione alle specifiche informazioni in questione qualora consentano a un prestatore diligente di servizi di memorizzazione di informazioni di individuare l'illegalità dell'attività o informazione senza un esame giuridico dettagliato». Il legislatore ha tentato così di risolvere, almeno



[30] Anche l'ordine di fornire informazioni deve essere motivato con riferimento all'obiettivo perseguito con la richiesta, e delle ragioni per cui esso è un adempimento necessario e proporzionato per accertare il rispetto del diritto dell'Unione o del diritto nazionale. L'ordine contiene inoltre informazioni chiari per identificare l'utente, anche mediante riferimento a nomi di *account* o altri elementi identificativi univoci.

[31] Artt. 9, par. 6 e 10, par. 6, DSA.

[32] Il rappresentante nominato dovrà assicurare la cooperazione con le autorità competenti degli Stati membri, la Commissione e il comitato. Egli potrà essere ritenuto responsabile – per espressa previsione dell'art. 13 DSA – del mancato rispetto degli obblighi derivanti dal presente regolamento, «fatte salve le responsabilità e le azioni legali che potrebbero essere avviate nei confronti del prestatore di servizi intermediari».

in parte, i dubbi sull'interpretazione del requisito della "conoscenza effettiva"[33]; in sostanza il DSA pare aver disciplinato i presupposti soggettivi della responsabilità dell'*hosting provider*, precisando che l'invio di una segnalazione da parte dell'utente permetta di acquisire una conoscenza effettiva, da cui deriva l'obbligo per l'intermediario di immediata rimozione del contenuto segnalato.

In sede di primo commento[34] si è osservato come la norma possa avere significative ricadute in punto di responsabilità, rendendo di fatto inapplicabili quelle disposizioni che subordinano l'obbligo di attivazione del *provider* alla previa emanazione di un ordine dell'Autorità[35].

Si prevede inoltre, per il caso in cui l'utente violi i termini e condizioni del servizio, oppure sia riscontrata la presenza di contenuti illegali, l'obbligo di fornire a quest'ultimo una motivazione chiara e specifica. Poiché tali disposizioni saranno esaminate nella sezione dedicata alle attività di *private enforcement*, si rinvia agli approfondimenti svolti in quella sede[36].

## 2.3 Focus sulla notifica di sospetti di reati *ex* art. 18 DSA

Sebbene l'intermediario non sia tenuto a ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite, il Regolamento gli impone specifici obblighi di denunzia all'autorità laddove venga a conoscenza «di informazioni che fanno sospettare che sia stato commesso, si stia commettendo o probabilmente sarà commesso un reato che comporta una minaccia per la vita o la sicurezza di una o più persone»[37]. In tal caso dovrà l'*hosting provider* dovrà fornire, senza indugio, tutte le informazioni in suo possesso.

È bene osservare come il legislatore europeo abbia circoscritto tale obbligo entro contorni ben precisi, probabilmente allo scopo di evitare che gli intermediari del web diventino figure istituzionalmente incaricate di denunciare possibili reati alle autorità statali. Il dovere di segnalazione sorge soltanto rispetto ai delitti più gravi, che offendono beni dell'individuo (es. la vita, l'incolumità personale), ovvero della collettività (ordine pubblico, incolumità pubblica), che siano in corso di esecuzione, si siano già



[33] La Corte di Giustizia, chiamata a pronunciarsi in via pregiudiziale, ha rimesso ai giudici nazionali la valutazione sulla "neutralità" dell'*hoster* in base alle specifiche circostanze del caso. Nell'ordinamento italiano il concetto di "effettiva conoscenza" ha sollevato diverse problematiche applicative, tanto in sede civile quanto in sede penale. Secondo una linea interpretativa – oggi smentita dalla disposizione in commento – affinché venga meno la limitazione di responsabilità *ex* art. 16, D. Lgs. 70/2003 è necessario che l'*hosting provider* abbia preso conoscenza del contenuto illecito su comunicazione delle autorità competenti. In argomento v. L. Bugiolacchi, *Ascesa e declino della figura del provider «attivo»? Riflessioni in tema di fondamento e limiti del regime privilegiato di responsabilità dell'hosting provider*, in *Responsabilità civile e previdenza*, 2015, 4, 1261 ss.; G.P. Accinni, *Profili di responsabilità penale dell'hosting provider "attivo"*, in *Archivio penale*, 2017, 2, 1 ss.

[34] Secondo Braschi, *Il nuovo Regolamento sui servizi digitali: quale futuro per la responsabilità degli Internet Service Provider?*, cit., 374, sarebbe opportuno che, in sede di attuazione, il legislatore italiano introducesse una specifica previsione diretta a regolare l'ipotesi in cui l'*hosting provider* ometta di rimuovere immediatamente il contenuto illecito oggetto di segnalazione. L'autrice ritiene inoltre che il DSA apra alla possibilità di configurare una responsabilità di tipo strutturalmente colposo in capo al fornitore di servizi di memorizzazione che ometta di eliminare i contenuti illeciti segnalati dall'utente.

[35] Cfr. Art. 16, comma 2, lett. b) D. Lgs. 70/2003 secondo cui «il prestatore non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore: [...] b) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso»

[36] *Infra*, cap. 2 (par. 1.1 e ss.).

[37] L'intermediario dovrà rivolgersi alle autorità giudiziarie o di contrasto dello Stato membro interessato, ovvero, laddove non sia possibile individuarlo, ad Europol o alle autorità di contrasto dello Stato membro in cui risiede il rappresentante legale del *provider* (art. 18, par. 2, DSA). La disposizione precisa, inoltre, che è "interessato" lo Stato membro in cui si sospetta che sia stato commesso, si stia commettendo o sarà probabilmente commesso, ovvero lo Stato membro in cui risiede o si trova il presunto autore del reato, oppure lo Stato membro in cui risiede o si trova la vittima del presunto reato.

commessi, oppure saranno commessi nel futuro. La giurisprudenza dovrà chiarire se in tale concetto possano rientrare anche quei reati di pericolo che, soltanto indirettamente, tutelano la sicurezza dell'individuo (ad. es. i discorsi di incitamento all'odio o l'istigazione a commettere delitti)[38].

Il nuovo Regolamento non precisa quali siano gli indici da cui l'ISP può, ragionevolmente, desumere il sospetto di commissione di un reato. In mancanza di diverse indicazioni legislative deve ritenersi, anche in ragione della gravità dei reati in questione, che il *provider* debba informare l'autorità laddove sia a conoscenza di una qualsiasi notizia, senza che sia chiamato a svolgere alcun vaglio preventivo di fondatezza sull'avvenuta o presumibile commissione dell'illecito. La disposizione non richiede infatti che l'intermediario abbia un "fondato" sospetto di commissione del reato: è dunque opportuno che ogni accertamento in merito sia svolto dall'autorità giudiziaria o da quella di pubblica sicurezza.

La denuncia potrà essere fatta in qualunque forma, purché sia inoltrata "senza indugio". Sebbene il DSA non preveda specifiche sanzioni per l'inosservanza di tale obbligo, l'eventuale violazione sarà punita dagli Stati membri ai sensi dell'art. 52 DSA[39].

## 3 Disposizioni aggiuntive applicabili alle piattaforme online: il sistema di gestione dei reclami

Le disposizioni contenute nelle Sezioni III e IV del Capo III introducono adempimenti ulteriori e supplementari in capo alle piattaforme *online*[40], con esclusione delle micro e piccole imprese. Come precisato in apertura, tali obblighi vanno a cumularsi – e non si sostituiscono – a quelli previsti nei paragrafi precedenti. In particolare, l'art. 20 del DSA impone a questa categoria di intermediari l'obbligo di predisporre un sistema elettronico di gestione dei reclami rispetto a tutte le sanzioni applicabili nei confronti dell'utente (es. rimozione del contenuto, sospensione o cancellazione dell'*account*), tale da istituire un pronto rimedio per far vale i suoi diritti[41].



Al tempo stesso, la norma chiarisce che le piattaforme non devono assumere decisioni solo sulla base di strumenti automatizzati, ma devono avvalersi di una supervisione umana. Si tratta di un aspetto che è stato oggetto di ampio dibattito durante l'*iter* legislativo, poiché si temeva che l'implementazione di meccanismi di controllo umano potesse rivelarsi eccessivamente onerosa[42]. Tuttavia, in un'ottica di bilanciamento dei contrapposti interessi, è prevalsa la necessità di apprestare una tutela efficace dei diritti degli utenti.

---

[38] Il tema della responsabilità dell'ISP in caso di reati di istigazione è oggetto di dibattito. In dottrina v. V. Nardi, *I discorsi d'odio nell'era digitale: quale ruolo per l'Internet service provider?*, in *Diritto Penale Contemporaneo*, 7 marzo 2019, 17 ss.

[39] La norma prevede che gli «*Stati membri stabiliscono le norme relative alle sanzioni applicabili in caso di violazione del presente regolamento da parte dei fornitori di servizi intermediari che rientrano nella loro competenza*». Ai sensi dell'art. 52, par. 3, l'importo massimo delle sanzioni pecuniarie che possono essere irrogate in caso di inosservanza è pari al 6 % del fatturato annuo mondiale del fornitore di servizi intermediari interessato nell'esercizio finanziario precedente. *Amplius*, v. Sez. IV, § 2.1.2.

[40] Sulla definizione di piattaforma online v. *supra*, § 1

[41] I sistemi interni di gestione dei reclami devono essere di facile accesso e uso e consentire la presentazione di reclami sufficientemente precisi e adeguatamente motivati. La procedura di reclamo consiste in una sorta di "riesame in autotutela": laddove la piattaforma raccolga sufficienti elementi per ritenere che la decisione assunta in precedenza (es. di non dare seguito alla segnalazione), il prestatore di servizi dovrà annullare tale decisione.

[42] La documentazione dell'iter legislativo è disponibile sul sito istituzionale: https://eur-lex.europa.eu

## 3.1 La risoluzione extragiudiziale delle controversie e i segnalatori attendibili (rinvio)

Il nuovo Regolamento dedica ampio spazio alle procedure di risoluzione alternativa delle controversie. Poiché il tema sarà esaminato *funditus* in altra sede[43], ci limiteremo a fornire un quadro sommario della disciplina. L'art. 21 DSA permette a ciascun utente di ricorrere a un organismo di risoluzione extragiudiziale delle controversie[44], per "impugnare" le decisioni assunte dalle piattaforme sulle segnalazioni presentate ovvero in sede di reclamo. A tal fine è onere della piattaforma informare i propri utenti in merito alla possibilità di avviare le procedure di ADR. Resta però ferma la possibilità di rifiutare il contraddittorio dinanzi all'organismo, qualora la piattaforma ritenga che la questione sia ormai decisa a livello interno. Gli esiti della procedura[45] non sono vincolanti per le Parti, e non limitano o precludono in alcun modo il diritto di avviare contenziosi dinanzi a un giudice nazionale. Gli organismi sono "certificati" dal Coordinatore dei servizi digitali su base nazionale, che supervisiona anche il loro corretto funzionamento e l'andamento delle procedure di risoluzione stragiudiziale delle controversie.Il Regolamento introduce anche una nuova figura, che assumerà un ruolo centrale nel contrasto alla diffusione di contenuti illegali: il c.d. "segnalatore attendibile" *ex* art. 22 DSA. Tale qualifica è riconosciuta dal Coordinatore dei servizi digitali dello Stato a chi dimostri di soddisfare determinate condizioni[46]. L'attività di questi soggetti è funzionale a una tutela più incisiva i diritti degli utenti; alle segnalazioni presentate dai segnalatori attendibili è infatti data priorità, dovendo essere "trattate e decise senza indebito ritardo".

## 3.2 Misure contro gli abusi, pubblicità e trasparenza dei sistemi di raccomandazione



Nel caso in cui rilevino la presenza di contenuti manifestamente illegali, le piattaforme *online*, dopo aver rivolto all'utente un avviso preventivo, devono sospendere *l'account* per un periodo di tempo ragionevole. Analogamente, la sospensione può essere irrogata nei confronti di enti o persone fisiche che con frequenza presentano segnalazioni o reclami manifestamente infondati[47].

---

[43] V. *infra* (cap. 2 della presente sezione, parr. 3.2 e 3.3).

[44] Si tratta di enti che assicurano l'imparzialità di giudizio e l'indipendenza dalle Parti. I membri dovranno possedere le competenze necessarie, in relazione agli ambiti considerati (es. contenuti illegali o applicazione delle condizioni generali delle piattaforme online). Si potrà accedere all'ADR direttamente online, presentando i necessari documenti giustificativi online, secondo regole procedurali chiare, eque, facilmente e pubblicamente accessibili.

[45] Gli organismi rendono la decisione entro un periodo di tempo ragionevole e, comunque, non oltre 90 giorni dal ricevimento del reclamo. In caso di controversie molto complesse, è possibile disporre la proroga di tale termine. Se la controversia è decisa a favore del destinatario del servizio, la piattaforma online dovrà sostenere tutti i costi della procedura, rimborsandoli al destinatario. Se al contrario la lite è risolta in favore della piattaforma online, l'utente non è tenuto a rimborsare i diritti e le altre spese sostenute dal *provider*, salvi i casi di mala fede nell'intraprendere l'azione.

[46] Si prevedono in particolare tre condizioni cumulative: a) disporre di capacità e competenze particolari ai fini dell'individuazione, dell'identificazione e della notifica di contenuti illegali; b) essere indipendente da qualsiasi fornitore di piattaforme online; c) svolgere le proprie attività al fine di presentare le segnalazioni in modo diligente, accurato e obiettivo

[47] Ai sensi dell'art. 23 DSA, nel decidere in merito a una sospensione, i fornitori di piattaforme online devono tener conto di tutti i fatti e le circostanze del caso concreto, tra cui a) il numero, in termini assoluti, di contenuti manifestamente illegali o di segnalazioni o reclami manifestamente infondati presentati entro un determinato arco temporale; b) la relativa proporzione rispetto al numero totale di informazioni fornite o di segnalazioni presentate entro un determinato arco temporale; c) la gravità degli abusi, compresa la natura dei contenuti illegali, e delle relative conseguenze; d) ove sia possibile identificarla, l'intenzione del destinatario del servizio, della persona, dell'ente o del reclamante.

Tanto i presupposti applicativi delle misure di sospensione, quanto la durata delle stesse, dovranno essere disciplinati nelle condizioni generali del servizio, così da fornire agli utenti una informativa chiara sulle *policy* adottate dalle piattaforme. Esse devono inoltre assolvere a obblighi informativi ulteriori rispetto a quelli previsti per tutti i *provider*[48], dovendo includere nelle relazioni periodiche anche i dati relativi al numero e agli esiti delle controversie sottoposte agli organismi di risoluzione extragiudiziale, nonché il numero di sospensioni imposte *ex* art. 23 DSA. I gestori delle piattaforme sono tenuti a organizzare e gestire le interfacce online in modo tale da non indurre in errore i destinatari dei loro servizi o da alterare la loro capacità di prendere decisioni libere e informate (art. 25). Con riferimento alle inserzioni pubblicitarie mostrate sulle interfacce del sito, essi provvedono affinché, per ogni singolo annuncio individui in modo chiaro il soggetto nel cui interesse viene presentata la pubblicità e i parametri c.d. "di *microtargeting*" utilizzati per determinare l'utente al quale viene presentata. L'utente avrà anche facoltà di rivolgersi alla piattaforma per conoscere se un certo contenuto contenga comunicazioni commerciali[49]. Il nuovo Regolamento pone inoltre un espresso divieto per i fornitori di piattaforme online di presentare pubblicità basate sulla profilazione[50], utilizzando dati personali sensibili[51]. Ulteriori obblighi riguardano le sole piattaforme online che si avvalgono di sistemi di raccomandazione[52]. Esse dovranno specificare, nelle loro condizioni generali, i principali parametri utilizzati da tali sistemi, nonché l'esistenza di impostazioni o opzioni attraverso cui l'utente può modificare o influenzare tali parametri. Qualora siano disponibili diverse opzioni in grado di determinare l'ordine delle informazioni presentate ai destinatari del servizio (es. *post* in un *feed* della *home*), il *provider* renderà disponibile anche una funzionalità che permetta di selezionare e modificare in qualsiasi momento l'opzione prescelta[53].

## 3.3 Protezione online dei minori

Il nuovo Regolamento introduce alcune disposizioni a tutela della sicurezza dei minori nell'accesso ai servizi della società dell'informazione. È fatto espresso divieto ai gestori delle piattaforme di mostrare pubblicità basata sulla profilazione, se vi è motivo di ritenere che il destinatario del servizio sia un minorenne; essi non saranno tuttavia tenuti a effettuare indagini specifiche, mediante il trattamento di "dati personali ulteriori" al fine di stabilire se il destinatario del servizio sia effettivamente un minore di età[54].



[48] Art. 15 DSA, v. *supra* par. 2.2.

[49] In caso di presentazione di una simile richiesta, il *provider* dovrà attivarsi affinché anche gli altri destinatari del servizio possano comprendere in modo chiaro, inequivocabile e in tempo reale, che il contenuto in questione contiene comunicazioni commerciali.

[50] Come definita dall'art. 4, punto 4), del regolamento (UE) 2016/679 «*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*».

[51] Trattasi in particolare dei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

[52] Ai sensi dell'art. 3, par. 1, lett. s) DSA è tale ogni «sistema interamente o parzialmente automatizzato che una piattaforma online utilizza per suggerire informazioni specifiche, tramite la propria interfaccia online, ai destinatari del servizio o mettere in ordine di priorità dette informazioni anche quale risultato di una ricerca avviata dal destinatario del servizio o determinando in altro modo l'ordine relativo o l'importanza delle informazioni visualizzate».

[53] Tale funzionalità è direttamente e facilmente accessibile in una sezione dell'interfaccia online (cfr. art. 27 GDPR).

[54] Per agevolare l'applicazione dell'art. 28 DSA, la Commissione potrà emanare orientamenti rivolti ai fornitori di piattaforme online, individuando le «misure adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori sul loro servizio».

# 4 Gli obblighi supplementari a carico delle *very large online platforms*: cenni introduttivi

È noto come le piattaforme *online* di dimensioni molto grandi[55] e i motori di ricerca[56] assumano oggi un ruolo cruciale nell'ecosistema digitale, favorendo non soltanto la diffusione di informazioni e contenuti, ma anche la conclusione di commerciali *online* su ampia scala. Per tali operatori il DSA ha introdotto ulteriori adempimenti rispetto a quelli applicabili a tutti gli intermediari di servizi, allo scopo di apprestare una tutela efficace per i diritti fondamentali sanciti nella Carta dei diritti fondamentali e contrastare le condotte illegali commesse *online*. L'applicazione delle norme della Sezione 5 presuppone la designazione, ad opera della Commissione, degli operatori economici che raggiungono i limiti dimensionali stabiliti dal Regolamento[57]. La decisione è assunta in ragione dei dati che sono stati forniti direttamente dal *provider*[58], oppure sulla base delle altre informazioni disponibili; in questa ipotesi l'operatore economico potrà presentare osservazioni entro dieci giorni lavorativi dal ricevimento della bozza di decisione.

## 4.1 Obblighi in punto di *risk assessment, mitigations of risks, crisis response mechanism, independent audit* e istituzione di una funzione aziendale di *compliance* (rinvio)

Agli intermediari di più grandi dimensioni è imposto un dovere di *compliance* basato sulla valutazione dei rischi, fin da momento della progettazione e successivamente almeno una volta all'anno. L'analisi deve tener conto, in particolare, del rischio di diffusione di contenuti illegali e dei possibili effetti negativi, attuali o prevedibili, al fine di adottare le opportune misure di attenuazione[59]. I documenti contenenti gli esiti della valutazione sono conservati per almeno tre anni e, su richiesta, dovranno essere forniti alla Commissione e al coordinatore dei servizi digitali del luogo di stabilimento. Il DSA fornisce un elenco soltanto esemplificativo degli adempimenti che i soggetti obbligati potranno adottare, lasciando a quest'ultimi – secondo la logica della c.d. *accountability* – l'individuazione delle misure in concreto più adeguate[60]. Vi è tuttavia una deroga



[55] Si utilizza per indicare tali operatori anche l'acronimo VLOP (*Very Large Online Platforms*).

[56] Il motore di ricerca online è definito come «un servizio intermediario che consente all'"utente di formulare domande al fine di effettuare ricerche, in linea di principio, su tutti i siti web, o su tutti i siti web in una lingua particolare, sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, richiesta vocale, frase o di altro input, e che restituisce i risultati in qualsiasi formato in cui possono essere trovate le informazioni relative al contenuto richiesto» (Art. 3, par. 1, lett. j DSA).

[57] Per i limiti dimensionali v. *supra*, nota n. 16.

[58] Ai sensi dell'art. 24, par. 2 e 3, DSA «[...] i fornitori pubblicano per ciascuna piattaforma online e ciascun motore di ricerca online, in una sezione disponibile al pubblico della loro interfaccia online, informazioni sul numero medio mensile di destinatari attivi del servizio nell'Unione, calcolato come media degli ultimi sei mesi [...]. 3. I fornitori di piattaforme online e di motori di ricerca online comunicano al coordinatore dei servizi digitali del luogo di stabilimento e alla Commissione, su loro richiesta e senza indebito ritardo, le informazioni di cui al paragrafo 2, aggiornate al momento di tale richiesta. Tale coordinatore dei servizi digitali oppure la Commissione può chiedere al fornitore della piattaforma online e del motore di ricerca online di fornire informazioni supplementari per quanto riguarda il calcolo di cui a tale paragrafo, comprese spiegazioni e giustificazioni in merito ai dati utilizzati. Tali informazioni non contengono dati personali».

[59] In particolare, si richiama l'attenzione ai rischi per l'esercizio dei diritti fondamentali della persona, al rispetto della vita privata e familiare, alla tutela dei dati personali, alla libertà di espressione e di informazione, inclusi la libertà e il pluralismo dei media, al divieto di discriminazione, al rispetto dei diritti del minore, nonché alla tutela dei consumatori.

[60] Una volta identificati i rischi sistemici, le piattaforme e i motori di ricerca devono adottare, ex art. 35 DSA, misure di mitigazione ragionevoli, efficaci e proporzionate. Tali misure possono comprendere, tra l'altro, l'adeguamento delle caratteristiche o del

in caso di eventi eccezionali (es. guerre, pandemie etc.) da cui derivi il rischio di un utilizzo improprio delle piattaforme per la diffusione di informazioni false o contenuti illegali; in tal caso la Commissione europea potrà inoltre elaborare protocolli di gestione della crisi e imporre agli intermediari l'adozione di misure nei limiti definiti dalle disposizioni in merito di meccanismi di risposta alle crisi[61]. Tali operatori sono anche tenuti a predisporre un sistema di controlli esterni, attraverso l'espletamento di *audit* indipendenti e a istituire una funzione aziendale di *compliance*. Si rinvia sul punto agli approfondimenti svolti nel prosieguo della trattazione[62].

## 4.2 Focus sulle misure aggiuntive in punto di sistemi di raccomandazione, pubblicità, accesso ai dati e controllo, trasparenza

Si è detto in precedenza che, qualora utilizzino sistemi di raccomandazione, le piattaforme *online* sono tenute a specificare, nelle condizioni generali, i principali parametri utilizzati, nonché qualunque opzione che consenta all'utente di modificare tali parametri[63]. Per i *provider* di grandi dimensioni il DSA introduce l'obbligo ulteriore di assicurare «almeno un'opzione per ciascuno dei loro sistemi di raccomandazione, non basata sulla profilazione» (art. 38 DSA). Viene in tal modo riconosciuto agli utenti, sia pur indirettamente, il diritto di scegliere una o più opzioni alternative rispetto alla profilazione, fondate ad esempio sulla previa selezione di ambiti o tematiche di interesse. Si tratta di una novità degna di nota, se solo di considera che, nello scenario attuale, il destinatario del servizio "deve" accettare la profilazione, quale unica condizione per l'accesso a molti servizi online o *social network*. Quanto alla trasparenza nell'ambito della pubblicità *online*, le VLOP che presentano annunci sulle loro interfacce devono compilare e rendere accessibile al pubblico un registro in cui è indicato il contenuto delle pubblicità, il nominativo del soggetto per conto del quale viene presentata e di quello che ha pagato l'annuncio. Nel registro è anche annotato il periodo durante il quale è stata presentata la pubblicità e il novero di soggetti a cui era rivolto, nonché i parametri utilizzati per individuare i destinatari[64]. Vi sono poi ulteriori informazioni che, a richiesta, il *provider* dovrà fornire alla Commissione o al coordinatore dei servizi digitali per valutare la corretta osservanza delle disposizioni del DSA; tra queste sono compresi i dati in merito alla progettazione, alla logica, al funzionamento e alla sperimentazione dei sistemi algoritmici. Le autorità di regolamentazione possono ordinare l'accesso ai dati anche a beneficio dei "ricercatori abilitati"[65], allo scopo di condurre ricerche che contribuiscano al rilevamento dei rischi sistemici nell'Unione. In ogni caso, trattandosi di informazioni particolarmente sensibili e coperte da *trade secret*, il Regolamento pone alcune cautele a garanzia degli intermediari interessati[66].



funzionamento dei loro servizi; la revisione delle condizioni generali del servizio e delle procedure di moderazione dei contenuti; l'adozione di *policy* specifiche sulla rimozione dei contenuti oggetto di segnalazione; l'utilizzo di sistemi algoritmici; l'avvio di strumenti di cooperazione con i segnalatori attendibili; l'adesione a codici di condotta e i protocolli di crisi etc.

[61] V. *infra* cap. 2, par. 4.3.

[62] *Infra*, cap. 2, par. 4.

[63] Cfr. Art. 27 DSA.

[64] L'art. 39 DSA impone alle piattaforme di rendere pubblici anche il numero totale dei destinatari raggiunti dall'annuncio pubblicitario e, ove opportuno, i dati aggregati relativi al gruppo o ai gruppi di destinatari ai quali la pubblicità era indirizzata. Tali dovranno essere conservati fino a un anno dopo la data dell'ultima presentazione dell'annuncio medesimo.

[65] Tali soggetti sono accreditati soltanto laddove soddisfino alcuni requisiti di sicurezza e protezione dei dati indicati dall'art. 40, par. 8, DSA.

[66] Ai sensi dell'art. 40, par. 2 ss. del DSA le Autorità devono tener conto dell'interesse dei *provider* alla protezione delle informazioni riservate e dei segreti commerciali. Qualora la richiesta sia formulata per finalità di ricerca, l'intermediario

## 5 Gli obblighi delle piattaforme online che consentono ai consumatori di concludere contratti a distanza con gli operatori commerciali

Alcune disposizioni del nuovo Regolamento si applicano alle piattaforme online che consentono ai consumatori di concludere contratti a distanza con operatori commerciali[67]. A tutela dei consumatori si prevede che, qualora tali operatori intendano pubblicizzare o offrire prodotti o servizi, dovranno fornire al gestore della piattaforma i dati identificativi dell'impresa (es. denominazione, estremi dell'iscrizione nel registro delle imprese, dettagli relativi al conto di pagamento), oltre a un'autocertificazione relativa alla conformità dei prodotti o servizi offerti alle norme dell'Unione[68]. Il *provider* dovrà vagliare l'attendibilità e la completezza delle informazioni trasmesse, prima di permettere all'operatore commerciale di concludere contratti. Se l'operatore commerciale, alla data di entrata in vigore del DSA, è già operativo sulla piattaforma, dovrà fornire senza ritardo le predette informazioni per non incorrere in una misura di sospensione da parte del *provider*. Le piattaforme sono altresì tenute a organizzare la propria interfaccia online in modo da consentire agli operatori commerciali di adempiere all'obbligo di informativa precontrattuale previsto dalla normativa consumeristica[69].

Inoltre, qualora la piattaforma venga a conoscenza della promozione – attraverso il proprio servizio – di beni o servizi illegali dovrà avvisare prontamente i consumatori che li abbiano acquistati. Qualora il *provider* non disponga dei recapiti di tutti i consumatori interessati, dovrà rendere pubbliche le informazioni concernenti il bene o servizio illegale, l'identità dell'operatore commerciale, e l'esistenza di eventuali mezzi di ricorso. Tale obbligo è circoscritto agli acquisti effettuati nei sei mesi precedenti alla conoscenza dell'illegalità.



## 6 Le norme del DSA in tema di codici di condotta e protocolli di crisi (artt. 44-48)

Merita da ultimo attenzione la Sezione VI del Capo III, che offre una disciplina trasversale per garantire la diffusione delle *best practices* e la creazione di norme di *soft law*. Mediante le norme di questo capo il legislatore ha inteso incoraggiare l'elaborazione di norme volontarie per l'attenuazione dei rischi sistemici soprattutto da parte degli intermediari di grandi dimensioni. In particolare, sarà compito della

interessato può chiedere al coordinatore dei servizi digitali di modificare la richiesta, ove ritenga che l'accesso ai dati comporterebbe notevoli vulnerabilità per la sicurezza del servizio o per la protezione delle informazioni riservate, in particolare dei segreti commerciali.

[67] È prevista tuttavia una deroga per le piattaforme che si qualificano come microimprese o piccole imprese quali definite nella raccomandazione 2003/361/CE.

[68] Il gestore della piattaforma dovrà conservare le informazioni ottenute dall'operatore commerciale per un periodo di sei mesi dalla conclusione del rapporto contrattuale. Tali informazioni possono essere divulgate a terzi solo se previsto dal diritto applicabile, oppure in caso di ordini emessi dalle autorità competenti degli Stati membri o dalla Commissione europea. Alcune informazioni sono tuttavia soggette a pubblicazione sulla interfaccia online della piattaforma (es. dati identificativi dell'impresa), al fine di poter essere facilmente consultate dagli utenti.

[69] Cfr. Art. 20 della Direttiva 2019/771/UE del Parlamento europeo e del Consiglio relativa a determinati aspetti dei contratti di vendita di beni. Nel dettaglio l'art. 31 DSA prevede che la piattaforma debba assicurarsi che siano forniti al consumatore almeno le informazioni per l'individuazione chiara e inequivocabile dei prodotti o dei servizi offerti; per l'identificazione del commerciante; e, se del caso, le informazioni relative all'etichettatura e alla marcatura di sicurezza e conformità dei prodotti.

Commissione predisporre codici di condotta al fine di contribuire alla corretta applicazione del DSA, tenendo conto in particolare delle sfide specifiche connesse alla lotta ai diversi tipi di contenuti illegali. Nell'elaborazione di tali codici sono coinvolti attivamente anche i prestatori di servizi, che potranno in tal modo aderire su base volontaria all'impegno di adottare misure specifiche di attenuazione dei rischi nonché di condividere gli esiti delle valutazioni sulle misure adottate.

Per quanto l'adesione ai codici di condotta sia facoltativa, il Considerando n. 104 prevede che, dal rifiuto ingiustificato della piattaforma o del motore di ricerca di aderire ad un codice di condotta, la Commissione europea possa trarre argomenti di valutazione per stabilire se il *provider* abbia violato gli obblighi imposti dal Regolamento[70].

Allo scopo di assicurare il rispetto degli obblighi in materia di trasparenza, si prevede l'elaborazione di codici di condotta anche nella pubblicazione di inserzioni pubblicitarie *online*.

Vi sono, infine, i protocolli volontari di crisi, predisposti per far fronte a circostanze straordinarie. Tali protocolli avranno validità limitata nel tempo, e si aggiungono ai meccanismi di risposta alle crisi di cui all'art. 36. Più precisamente, essi sono diretti a coordinare una risposta collettiva, transfrontaliera e rapida per le ipotesi in cui sorga l'esigenza di diffondere velocemente informazioni affidabili, ovvero, di arginare la rapida circolazione di contenuti illegali o condotte di disinformazione[71].

# 7 Rilievi conclusivi



Il DSA rappresenta un ambizioso tentativo di rimodulare la responsabilità degli intermediari del web a fronte del loro mutato ruolo nella moderazione e nella fruizione dei contenuti online. Tale obiettivo non sembra tuttavia riflettersi nelle disposizioni sul regime di responsabilità (Capo II), che si collocano nel medesimo alveo della direttiva 2000/31/CE, in gran parte invariate.

Risulta in particolare immutata la distinzione tra *hosting* attivo e passivo – interpretato alla luce delle pronunce della Corte di Giustizia – come criterio per l'esenzione di responsabilità. Si tratta di una posizione discutibile, che non offre garanzie di maggiore certezza e conoscibilità del diritto rispetto alla disciplina previgente. Una scelta per molti versi distonica rispetto alle esigenze alla base dell'intervento riformatore, che muovevano dall'assunto di una progressiva "perdita di neutralità" dei *provider*. Invero, le attività di filtraggio, selezione e profilazione dei contenuti a scopo di lucro sono tuttora considerati un'attività di natura puramente tecnica e passiva che, come tale, non dovrebbe radicare una "conoscenza effettiva" dei contenuti illegali in capo all'intermediario.

Da questa prospettiva, assume rilevanza la sola segnalazione da parte dell'utente che fa sorgere «*una conoscenza o consapevolezza effettiva [...] qualora consenta a un prestatore diligente di servizi di individuare l'illegalità dell'attività o informazione senza un esame giuridico dettagliato*» (art. 16, par. 3, DSA). Il legislatore ha in tal modo allentato le maglie di un regime di (ir)responsabilità che, in linea di principio, rimane ancora molto solido.

[70] Per contro, la mera partecipazione a un determinato codice di condotta e la sua attuazione non dovrebbero di per sé presupporre la conformità al presente regolamento (cons. n. 104 DSA).

[71] Cfr. Considerando n. 108 DSA.

Appaiono decisamente più significative le novità relative ai doveri di attivazione e *compliance* in capo ai fornitori di servizi di hosting e alle piattaforme (Capo III DSA). I nuovi obblighi (ad. es. in relazione ai meccanismi di informazione e azione), si pongono in linea con un approccio normativo fondato sulla segnalazione delle violazioni e sulla pronta rimozione di contenuti illeciti. Viene inoltre valorizzata la leva preventiva per impedire che l'attività degli intermediari del web possa fungere da catalizzatore di condotte dannose o pericolose per gli utenti e la collettività. In questa direzione il legislatore europeo ha, condivisibilmente, imposto ai provider di definire in modo chiaro i termini e le condizioni del servizio, di approntare un sistema disciplinare e di segnalazione, e di collaborare a stretto contatto con le Autorità; a questi si aggiungono, per le piattaforme di dimensioni molto grandi, gli obblighi di valutazione e contenimento dei rischi sistemici e altre misure di *compliance* rafforzata.

In sostanza il DSA ha segnato un reale cambiamento di passo nell'attività degli intermediari del web attraverso l'introduzione di precise regole di condotta nel rapporto con gli utenti e con le autorità pubbliche. Sul piano della responsabilità si registra un cambio di prospettiva: da un sistema fondato (unicamente) sulle limitazioni all'esonero da responsabilità, si passa a un modello basato sulle sanzioni amministrative applicabili in caso inosservanza degli obblighi di *compliance*.

# Capitolo 2

## 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

**di E. BIRRITTERI**

SOMMARIO

# 2

## 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, rappresentano 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. – in grado di 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].



[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 *Dir. pen. cont. – Riv. Trim.*, 2021, 4, 304 ss.

[2] V. A. Gullo, G. Piccirilli, *Disinformazione e politiche pubbliche: una introduzione*, in *Dir. pen. cont. – Riv. Trim.*, 2021, 4, 248 ss.

[3] Cfr. ancora A. Gullo, G. Piccirilli, *Disinformazione e politiche pubbliche*, cit., 249.

[4] Necessità che abbiamo ribadito anche all'esito del secondo ciclo della ricerca: v. il report del 2022, reperibile al seguente link: https://www.esteri.it/wp-content/uploads/2022/09/LUISS-Come-individuare-e-contrastare-operazioni- coordinate-di-disinformazione-in-Italia.pdf.

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 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].



[5] Per un primo inquadramento generale v. anche B. Tassone, *Riflessioni introduttive,* in *Dir. Internet*, 2023, 1, 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*, 2023, 15(1), 83 ss.

[6] Cfr. il considerando n. 2 del Reg. UE 2022/2065 (corsivo nostro).

[7] V. sempre il considerando n. 2 del Reg. UE 2022/2065.

[8] Così il considerando n. 3 del Reg. UE 2022/2065.

[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».

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 dei livelli 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.

## 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 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.

[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 *Dir. Internet*, 2023, 1, 21.

[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.

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 comma 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 moderazione 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].



[14] È significativo evidenziare come ai sensi del considerando n. 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».

[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*, 2023, 48, 6.

[16] Vedi testualmente l'indicazione di *policy* n. 20, nella versione del report della ricerca del 2022, reperibile al seguente link: https://www.esteri.it/wp-content/uploads/2022/09/LUISS-Come-individuare-e-contrastare-operazioni- coordinate-di-disinformazione-in-Italia.pdf.

[17] Sul punto v. anche 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 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

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 passaggio 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 *obbligation* 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».

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] Per una paronamica v. anche G. Buttarelli, *La regolazione delle piattaforme digitali: il ruolo delle istituzioni pubbliche,* in *Gior. dir. amm.,* 2023, 1, 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: cfr. L. Torchia, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in *Riv. trim. dir. pubbl.*, 2022, 4, 1108.

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 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*.



[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».

[24] In argomento rinviamo integralmente alla disamina svolta in dettaglio nel cap. 1 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 *Dir. pen. proc.*, 2023, 3, 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».

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 *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

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

[27] Qualche chiarimento sul punto è offerto dal considerando n. 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)».

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 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 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].



[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».

[30] In argomento v. anche i rilievi di 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».

[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 *Riv. trim. dir. pubbl.*, 2022, 4, 998. Diffusamente cfr. anche G. Alpa, *Sul potere contrattuale delle piattaforme digitali*, in *Contr. impr.*, 2022, 721 ss.

# 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 2003/361/CE, 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 obbligation* 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 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

[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».

[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».

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 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].

---

[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 *Arch. pen.*, 1, 17 ss.; G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Dir. pen. cont. – Riv. Trim.*, 2020, 4, 75 ss.

[36] Per ogni dettaglio v. 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

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 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, 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



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 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 contraddittorio 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).

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 vedersi 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 n. 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



[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 *Dir. Internet*, 2023, 1, 39 ss. V. altresì A.M. Felicetti, *La risoluzione extragiudiziale delle dispute nei mercati digitali: alcune novità dall'Europa*, in *Riv. trim. dir. proc. civ.*, 2023, 1, 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 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

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].

## 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».



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*, 2020, 1, 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 *Riv. trim. dir. pubbl.*, 2022, 4, 1031 ss.

[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 contraddittorio 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».

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]) 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 obbligation* 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

[48] Cfr. nel dettaglio, anche per ogni ulteriore riferimento, il cap. 3 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 AliExpress; Amazon Store; Apple AppStore; Booking.com; Facebook; Google Play; Google Maps; Google Shopping; Instagram; LinkedIn; Pinterest; Snapchat; TikTok; Twitter; Wikipedia; YouTube; Zalando): cfr. la seguente pagina web https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413.

[50] V. *supra* par. 1 per tutti i necessari rinvii.

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

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 espressione 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 n. 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 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

[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.

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, appare proporzionata alla loro 'potenza di fuoco' sul mercato globale e un bilanciamento tutto sommato più che ragionevole tra i vari interessi contrapposti[60]. 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].

---

[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 *Sist. pen.*, 11 gennaio 2022.

[60] In generale, sull'approccio del DSA in punto di bilanciamento tra i vari interessi contrapposti, v. G. Caggiano, *La proposta di* Digital Services Act *per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, in *Annali AISDUE*, 2021, 1, 28.

[61] Cfr. ancora il capitolo 4 del presente report.

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

## 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].

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].



[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».

[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

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 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].

---

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 *taylor made*.

[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

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'implementazione 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 n. 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 adottare una decisione «che impone»



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, *passim*.

[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 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.

[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

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].

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»,

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; 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 2 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 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».

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 innescare 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



[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».

[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 *Dir. Internet*, 2023, 1, 32, ove si 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».

«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 del decisore 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.

## 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.



[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».

[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

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 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].

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 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*, 2021, 43, 1.

## 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 officers*', 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 alla figura dell'*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 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 effettività.

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



[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 al seguente link: https://www.borsaitaliana.it/comitato-corporate-governance/codice/2018clean.pdf.

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, iniziative 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

[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.

[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*, 2021, 10(4), 2 ss.

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 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.

[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 il DSA «the DSA il 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*, 2023, 4(1), 53 ss.

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

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

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 rilevato[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 e necessario 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.



[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».

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

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

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

# Capitolo 3

## L'*enforcement* pubblico del *Digital Services Act* tra Stati membri e Commissione europea: implementazione, monitoraggio e sanzioni

**di R. SABIA**



SOMMARIO

# 3

## 1 L'*enforcement* pubblico del *Digital Services Act*: un inquadramento generale

Il *Digital Services Act* (DSA)[1], pubblicato nella Gazzetta ufficiale dell'Unione europea a ottobre 2022, rappresenta il più grande cambiamento di regole, da vent'anni a questa parte, per la responsabilità degli intermediari *online*, recando un nuovo e composito quadro normativo che – attraverso l'introduzione di rilevanti obblighi e doveri di diligenza a carico dei *provider* – ha l'obiettivo di contemperare esigenze diverse: approntare una risposta ai rischi causati da contenuti generati dagli utenti, proteggere i diritti fondamentali, con particolare riguardo alla libertà di espressione, trovare soluzioni ai limiti pratici della moderazione dei contenuti su scala[2].

Tale intervento si inscrive nell'ambito della strategia dell'Unione europea volta a gettare le basi, anticipando altri Paesi del mondo, per l'affermazione di una «compiuta politica pubblica digitale», perseguendo sia il consolidamento della *leadership* globale nel settore della regolazione delle piattaforme, sia il contenimento del proliferare di discipline nazionali in materia – come ad esempio quelle tedesca o francese – che potrebbero condurre a una problematica disomogeneità di approcci nel mercato interno[3].



Come è stato bene messo in evidenza in altre sezioni di questa ricerca, il DSA – pur ponendosi, per diversi profili, in continuità con la pregressa disciplina contenuta nella Direttiva 2000/31/CE sul commercio elettronico, come accade ad esempio in relazione alla responsabilità del *provider*[4] – introduce innovazioni degne di nota specialmente sul terreno degli obblighi di *due diligence* posti in capo agli intermediari di servizi digitali, soprattutto per ciò che concerne le restrizioni alle informazioni condivise dagli utenti[5].

---

[1] 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). Per una recente panoramica sulla nuova normativa v. il volume collettaneo a cura di A. Von Ungern-Sternberg, *Content Moderation in the EU: The Digital Services Act, Trier Studies on Digital Law*, Trier, 2023, nonché quello a cura di J. Van Hoboken e altri, *Putting the Digital Services Act into Practice: Enforcement, Access to Justice, and Global Implications*, Berlin, 2023. Nella dottrina italiana, v. i diversi contributi pubblicati nel fascicolo n. 1/2023 di *Dir. internet*.

[2] Questa la sintesi efficace di P. Church, C. Pehlivan, *The Digital Services Act (DSA): A New Era for Online Harms and Intermediary Liability*, in *Global Privacy Law Review*, 2022, 4, 1, 53, i quali si definiscono appunto il DSA «the biggest shake up to the rules for online intermediary liability in twenty years».

[3] G. Buttarelli, *La regolazione delle piattaforme digitali: il ruolo delle istituzioni pubbliche*, in *Giorn. dir. amm.*, 2023, 1, 120, richiama in particolare il *NetzDG* tedesco del 2017 in tema di obblighi di rimozione dei contenuti illeciti *online* e la *Loi Avia* francese del 2020.

[4] V. *supra* (cap. 1). il contributo di L. D'Agostino, *Disinformazione e obblighi di* compliance *degli operatori del mercato digitale alla luce del nuovo* Digital Services Act.

[5] Del tema si occupa E. Birritteri, *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, supra* (cap. 2).

Sul punto, occorre ricordare che si tratta di doveri asimmetrici[6], a pervasività crescente e progressiva in rapporto alla natura dei servizi prestati e alle dimensioni del fornitore, arrivando il Regolamento, con specifico riferimento alle c.d. *very large online platforms* – ossia quelle aventi più di quarantacinque milioni di utenti attivi medi mensili nell'Unione – a stabilire regole *ad hoc* nel Capo III, sezione 5 del DSA, su cui vigila in via esclusiva, come si vedrà, la Commissione europea[7].

Questa opzione di *policy* muove dalla presa d'atto dell'insufficienza delle sole misure di autoregolazione da parte delle piattaforme per limitare la diffusione di *harmful content* e dalle criticità connesse ai caratteri che detta *self-regulation* è andata assumendo. In proposito, si parla di «sovranità digitale» in capo a tali soggetti, che hanno finito per accentrare su di sé la definizione di regole generali, il controllo sul loro rispetto, la costruzione di apparati in linea di massima indipendenti per la risoluzione di eventuali controversie, così mimando «il potere pubblico [...] anche se tutte le funzioni [...] sono strutturate e rimangono all'interno della piattaforma», che presenta, in qualche misura, «i tratti tipici di un ordinamento giuridico, autonomo dall'ordinamento generale»[8].

Il DSA segna dunque una significativa volontà di riaffermazione del ruolo della eteroregolazione nel campo dei servizi digitali, delineando per la prima volta in modo strutturato una cornice di regole di fonte pubblicistica entro cui incasellare le pratiche di *private enforcement* degli operatori – attuate mediante la moderazione dei contenuti immessi *online* degli utenti, con un rilevante impatto sull'esercizio di diritti fondamentali, *freedom of speech in primis* – e fissando i criteri di riferimento delle scelte di *self-policing* e dei poteri *lato sensu* 'sanzionatori' delle piattaforme[9].

Il risultato è un apparato di regole alla ricerca di un equilibrio nella composizione di tale dualismo pubblico-privato, nel segno, anzitutto, di un ruolo attivo dei destinatari della disciplina – ic.d. servizi di intermediazione[10] – cui il DSA impone una serie di obblighi (si è parlato di «layer cake»)[11] stratificati dal basso verso l'altro, *id est* regole variabili in base alle caratteristiche del *provider* e via via più complesse, per cui il soggetto che si trovi al vertice è tenuto osservare sia le disposizioni specifiche per la propria attività, sia quelle dettate per i soggetti collocati ai livelli inferiori[12]. Come anticipato, si arriva ad affidare ai *player* di dimensioni molto grandi doveri *aggiuntivi*, quali la mappatura e gestione dei rischi sistemici, il sottoporsi a *audit* indipendenti e la costituzione di una funzione di *compliance* dedicata[13], con lo scopo

[6] Cfr. F. G'sell, *The Digital Services Act: a General Assessment*, in A. Von Ungern-Sternberg (a cura di), *Content Moderation in the EU*, cit., 88 ss.

[7] Infra, par. 6 e 6.1

[8] Così L. Torchia, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in *Riv. trim. dir. pubbl.*, 2022, 4, 1103 s. Rispetto ai riflessi di tali poteri sul versante sanzionatorio v. già E. Birritteri, *Punire la disinformazione: il ruolo del diritto penale e delle misure di moderazione dei contenuti delle piattaforme tra pubblico e privato,* in *Dir. pen. cont. – Riv. trim.*, 2021, 4, 304 ss.

[9] V. sul punto *supra* (cap. 2).

[10] Per la definizione, cfr. art. 3, par. 1, lett. g DSA, a norma del quale vi rientrano servizi della società dell'informazione quali il semplice trasporto (*mere conduit*), consistente nella trasmissione di informazioni su una rete di comunicazione o nella fornitura di accesso a una rete di comunicazione (*i*), la memorizzazione temporanea (*caching*) (*ii*) e la memorizzazione di informazioni fornite dagli utenti (*hosting*) (*iii*). A queste categorie, già presenti nella Direttiva sul commercio elettronico, si aggiungono quelle del medesimo articolo, *lett. i)* e *lett. j)*, riguardanti rispettivamente le piattaforme *online* (servizi di *hosting* che memorizzano e diffondono informazioni al pubblico) e i motori di ricerca *online* (servizi intermediari che consentono agli utenti di formulare domande per effettuare ricerche sulla base di un'interrogazione su qualsiasi tema).

[11] F. G'sell, *The Digital Services Act*, cit., 89.

[12] Cfr. *supra* (cap. 1, par. 1 e cap. 2., par. 1).

[13] Su cui, in dettaglio, v. *supra* (cap. 2, par. 4).

di colpire la propagazione di contenuti illegali e contrastare – per quanto qui d'interesse – anche la disinformazione *online*.

Del pari, il DSA tratteggia una complessa '*governance* pubblica' per l'efficace supervisione e attuazione della disciplina: l'articolazione dei poteri nel Regolamento segue uno schema tendenzialmente decentrato che è stato definito come «rete regolatoria condivisa», in cui le diverse autorità coinvolte in ambito nazionale e la Commissione europea – senza dimenticare il livello 'intermedio' rappresentato dal Comitato europeo per i servizi digitali – operano in collaborazione, riservandosi comunque agli Stati membri un ruolo di primo piano, pur nel contesto di un *framework* normativo armonizzato[14].

È evidente che un assetto di regole di tale portata sarebbe tuttavia destinato a rimanere ineffettivo ove non accompagnato da un puntuale e credibile meccanismo di implementazione che, nel caso di specie, è tratteggiato nel denso Capo IV del Regolamento, dedicato appunto all'attuazione, alla cooperazione, alle sanzioni e all'esecuzione del DSA, oggetto della presente sezione del *report* di ricerca.

È questo uno degli ambiti di intervento del Regolamento di sicuro interesse per il penalista, intercettando tra l'altro la questione dello spazio riservato – nella tutela sia dei diritti degli utenti di servizi digitali, sia delle funzioni delle autorità di *enforcement* coinvolte – alla risposta sanzionatoria, la quale – pur non ricorrendosi qui al diritto criminale – presenta non trascurabili connotati di afflittività.

Con l'obiettivo di offrire una panoramica dell'architettura dei poteri tratteggiata nel DSA avuto riguardo al versante pubblico e del riparto tra livello nazionale ed europeo (par. 2), il contributo ripercorre la progressione dell'articolato – ispirato a una logica, per così dire, 'ascendente' –, come segue: si muove dalle competenze attribuite alle autorità dei singoli Stati Membri e particolarmente ai coordinatori dei servizi digitali in relazione alla supervisione ed esecuzione del Regolamento (par. 3); si passa a esaminare la disciplina in tema di assistenza reciproca e cooperazione transfrontaliera (par. 4) e le funzioni del Comitato europeo per i servizi digitali (par. 5); si analizza, a seguire, il ruolo da protagonista della Commissione europea nei rapporti con le piattaforme *online* e i motori di ricerca *online* di dimensioni molto grandi (par. 6); si conclude con alcune considerazioni sui caratteri di fondo delle scelte regolatorie del legislatore europeo in punto di *enforcement* del DSA (par. 7).



## 2 La distribuzione dei poteri di *enforcement* tra la Commissione europea e gli Stati membri

Dalla lettura delle previsioni del Capo IV emerge come dell'*enforcement* pubblico del DSA siano titolari sia gli Stati membri – in particolare, attraverso la designazione di un'autorità nazionale di regolamentazione competente, il coordinatore dei servizi digitali[15] –, sia la Commissione europea. Nel quadro di una di «stretta cooperazione» tra livello nazionale ed europeo, l'art. 56 del Regolamento traccia una *summa divisio* tra quanto è di esclusiva pertinenza degli Stati membri – ossia, in termini generali, l'esercizio dei poteri di vigilanza e applicazione del DSA, sulla base del criterio del luogo di stabilimento principale del *provider* di servizi intermediari, fatto salvo quanto subito si dirà[16] – e gli ambiti di intervento

[14] L. Torchia, *I poteri di vigilanza*, cit., 1111.

[15] *Infra* par. 3.

[16] Il riparto di competenze tra Stati membri e Commissione è infatti ulteriormente precisato ai paragrafi 2, 3 e 4 dell'art. 56 DSA.

riservati alla sola Commissione – nello specifico, la supervisione sul rispetto degli obblighi più stringenti di cui si è fatta menzione (Capo III, sezione 5, artt. 33-43 DSA)[17] imposti ai fornitori di piattaforme *online* di dimensioni molto grandi (c.d. *Very Large Online Platforms – VLOPs*) e ai motori di ricerca *online* di dimensioni molto grandi (c.d. *Very Large Online Search Engines – VLOSEs*)[18]. Per tutte le altre norme applicabili alle «large companies» diverse da quelle appena citate si stabilisce, invece, una 'competenza concorrente' tra Commissione e Stati membri (art. 56, par. 3, DSA), ma va sottolineato che l'attivarsi delle autorità nazionali del luogo di stabilimento è subordinato al fatto che la Commissione non abbia avviato procedimenti per la stessa infrazione (così il par. 4 del medesimo articolo). Ben si comprende, quindi, come il legislatore europeo abbia voluto comunque attribuire alla Commissione il primato per la trattazione e gestione delle vicende in cui sono coinvolti gli operatori di più grande dimensione/importanza: ciò risponderebbe alla logica di evitare quei problemi di *enforcement* sperimentati nel contesto del GDPR[19] – ove, in ragione del *country-of-origin principle*, la competenza è di fatto nelle mani dell'autorità irlandese, avendo molte grandi aziende sede in tale Paese[20] –, sul presupposto di una maggior 'resilienza' della Commissione alle dinamiche di *regulatory capture*[21].
La suddivisione di cui si è detto è valevole anche per l'ipotesi in cui un fornitore di servizi intermediari non abbia uno stabilimento nell'Unione: esso ricadrà dunque nella competenza dello Stato membro in cui risiede o è stabilito il suo rappresentante legale – che i *provider* in questione, se offrono servizi nell'Unione, possono nominare a norma dell'art. 13 DSA[22] – o in quella della Commissione, sulla base delle regole appena delineate. In mancanza della nomina di un rappresentante legale da parte del fornitore, tutti gli Stati membri, e la Commissione per i *provider* di *VLOPs* e *VLOSEs*, dispongono dei poteri di vigilanza e applicazione del DSA, come chiarito dall'art. 56, par. 7 DSA. Per evitare sovrapposizioni e il rischio di duplicazioni procedimentali e sanzionatorie, tale previsione stabilisce che in queste circostanze, ove un coordinatore dei servizi digitali intenda procedere, sarà tenuto a informare tutti gli altri coordinatori nazionali e la Commissione, e lo stesso dovrà fare quest'ultima nell'ipotesi inversa. Un meccanismo così congegnato appare in grado, in principio, di inibire l'avvio di plurimi *proceeding* per la medesima violazione, ciò che – unitamente agli obblighi di comunicazione e notifica incombenti, a seconda dei casi, sulle autorità nazionali e sulla Commissione per i procedimenti rispettivamente avviati[23] – parrebbe scongiurare potenziali casi di *bis in idem*[24].



[17] Per una analisi di tali disposizioni, v. V. Colarocco, M. Cogode, *Gli obblighi applicabili a piattaforme* online *di dimensioni molto grandi (Artt. 33-43 – Capo III, Sezione 5)*, in *Dir. internet*, 2023, 1, 27 ss.

[18] Per le relative definizioni, v. *supra*, nt. 10.

[19] GDPR – Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE. Sull'effettiva capacità di enforcement dell'autorità irlandese v. la ricostruzione di M. Murgia, J. Espinoza, *Ireland is 'Worst Bottleneck' for Enforcing EU Data Privacy Law*, in *Irish Times*, 13 settembre 2021, https://www.irishtimes.com/business/technology/ireland-is-%20worst-bottleneck-for-enforcing-eu-data-privacy- law-iccl-1.4672480.

[20] F. G'sell, *The Digital Services Act*, cit., 106.

[21] I. Buri, *A Regulator Caught Between Conflicting Policy Objectives. Reflections on the European Commission's Role as DSA Enforcer*, in J. Van Hoboken e altri (a cura di), *Putting the Digital Services Act into Practice*, cit., 79; per alcune considerazioni sul punto, v. anche *infra* par. 7.

[22] L'art. 13, par. 1 DSA prescrive che i prestatori di servizi intermediari che non sono stabiliti nell'Unione ma che ivi offrono servizi «possono designare per iscritto una persona fisica o giuridica che funga da loro rappresentante legale in uno degli Stati membri in cui offrono i propri servizi».

[23] V. in particolare *infra* nei paragrafi che seguono.

[24] In senso analogo I. Castellucci, F. Coppola, *Il sistema sanzionatorio decentrato del DSA: dinamica dell'apparato istituzionale*, in *Dir. internet*, 2023, 1, 51 e 53. Manifesta invece qualche perplessità in relazione al fatto che il sistema delineato dal legislatore europeo sia in grado di «assicurare il rispetto del divieto di bis in idem sovranazionale» S. Braschi, *Il nuovo Regolamento sui servizi digitali: quale futuro per la responsabilità degli* Internet Service Provider?, in *Dir. pen. proc.*, 2023, 3, 377.

# 3 Il livello nazionale. I coordinatori dei servizi digitali degli Stati membri: uno sguardo d'insieme

Come si accennava, il DSA prevede, all'art. 49, che gli Stati membri designino al loro interno una o più autorità incaricate della vigilanza dei fornitori di servizi intermediari e dell'esecuzione del Regolamento («autorità competenti»). Ciascuno Stato individua, altresì, una delle suddette autorità quale *coordinatore dei servizi digitali*, che risulterà responsabile, a livello nazionale, «di tutte le questioni relative alla vigilanza e all'applicazione» del DSA, salvo che determinati compiti o settori non risultino attribuiti ad altre autorità competenti – cosa assai probabile essendo il DSA un Regolamento orizzontale, che interessa diversi ambiti[25].

Per evitare il rischio di una frammentazione dei compiti[26], si prevede in ogni caso che sia il coordinatore dei servizi digitali ad assicurare l'efficace e coerente applicazione del Regolamento e a occuparsi, appunto, del coordinamento tra le eventuali autorità domestiche competenti. È dunque plausibile (e anzi, secondo alcuni commentatori, preferibile)[27] che gli Stati membri si muovano nella direzione di designare tali soggetti tra autorità esistenti e con esperienza nei settori vigilati – in Italia, ad esempio, candidature sono state avanzate dall'Autorità per le garanzie nelle comunicazioni e dal Garante per la protezione dei dati personali –, dando luogo a una sorta di «competizione» per l'attribuzione del ruolo di coordinatore[28].

I coordinatori sono tenuti ad agire in modo imparziale, trasparente e tempestivo, rendendosi a tal fine necessario che ciascuno Stato metta a disposizione adeguate risorse tecniche, finanziarie e umane e assicuri, del pari, sufficiente autonomia gestionale in relazione al bilancio – elemento questo indispensabile a preservare la piena indipendenza di tali soggetti, chiamati a operare al riparo da influenze esterne e senza richiedere o comunque ricevere istruzioni da parte di altre autorità pubbliche o da privati (art. 50 DSA).



Tra i profili più interessanti della disciplina in analisi si annoverano quelli riguardanti l'articolazione dei poteri d'indagine, esecuzione e sanzione previsti in capo ai coordinatori dei servizi digitali nei confronti dei *provider* che ricadono nella competenza del loro Stato membro[29].

Più precisamente, l'art. 51 DSA distingue e dettaglia le attività rientranti nel campo dei poteri d'indagine (par. 1) e quelle afferenti ai poteri d'esecuzione e sanzione (par. 2), prevedendo infine la possibilità, in via residuale e solo ove l'espletamento degli altri poteri non abbia sortito effetti, di ricorrere a misure ulteriori a carattere 'ingiunzionale/inibitorio' (ivi inclusa quella delle restrizioni all'accesso) (par. 3)[30]. Si richiede che tutte le predette misure adottate dai coordinatori nell'esercizio di tali poteri siano – secondo la

[25] Sottolineano questo aspetto M. Husovec, I. Roche Laguna, *Digital Services Act: A Short Primer*, p. 2 del testo accessibile all'indirizzo https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4153796. Il contributo è in corso di pubblicazione in M. Husovec, I. Roche Laguna, *Principles of the Digital Services Act*, Oxford, 2023.

[26] Come osservato da L. Torchia, *I poteri di vigilanza*, cit., 1109.

[27] E.M. Tripodi, *Le Autorità competenti, i Coordinatori nazionali dei servizi digitali e il Comitato europeo per i servizi digitali. Brevi note*, in *Dir. internet*, 2023, 1, 62.

[28] Così G. Buttarelli, *La regolazione delle piattaforme digitali*, cit., 123.

[29] Con le precisazioni di cui subito si dirà rispetto anche ad altri soggetti che possono essere attinti dall'esercizio dei poteri in discorso.

[30] Si prevede che poteri di cui ai paragrafi 1, 2 e 3 lascino impregiudicata la sezione 3, relativa alla disciplina del Comitato europeo per i servizi digitali (cfr. art. 51, par. 4, DSA).

consueta formula – *effettive, dissuasive e proporzionate*[31], avuto riguardo alla natura, gravità, reiterazione e durata della violazione cui si riferiscono, e altresì, ove opportuno, alla capacità economica, tecnica e operativa del fornitore di servizi intermediari interessato (par. 5).

Osservando più da vicino il contenuto dei poteri dei coordinatori nazionali, in sede di *indagine* (art. 51, par. 1) questi possono imporre ai *provider* di fornire, senza indebito ritardo, informazioni relative a una presunta violazione del Regolamento (*lett. a*); essi possono, altresì, effettuare ispezioni presso i locali utilizzati da tali fornitori «al fine di esaminare, sequestrare, prendere o ottenere copie di informazioni relative a una presunta violazione in qualsiasi forma», nonché chiedere a un'autorità giudiziaria nazionale di ordinare ispezioni, o a altre autorità pubbliche di procedervi (*lett. b*); da ultimo, i coordinatori dei servizi digitali possono domandare spiegazioni a qualsiasi membro del personale o rappresentante dei suddetti fornitori in merito a presunte violazioni e registrarne le risposte (*lett. c*).

I delineati poteri d'indagine *sub lett. a* e *lett. b*) possono, peraltro, attingere anche *altre persone* che agiscano «per fini connessi alla propria attività commerciale, imprenditoriale, artigianale o professionale» e che possano «ragionevolmente essere a conoscenza di informazioni» in merito a una presunta violazione del DSA, ivi incluse le organizzazioni che effettuano le revisioni indipendenti *ex* artt. 37[32] e 75, par. 2 (nell'ambito della vigilanza rafforzata)[33] per i *provider* di piattaforme *online* e i motori di ricerca *online* di dimensioni molto grandi.

Rispetto ai poteri di *esecuzione* di cui all'art. 51, par. 2 DSA, occorre invece distinguere, dal momento che taluni si indirizzano unicamente alle piattaforme, mentre altri – legati all'*enforcement* delle sanzioni imposte dai coordinatori nazionali, di cui si dirà tra un momento – possono riguardare anche le altre persone menzionate nel par. 1.



Sul primo versante, vengono in rilievo il potere dei coordinatori di accettare gli impegni offerti dai *provider* in relazione alla loro conformità al Regolamento e di rendere detti impegni vincolanti[34] (*lett. a*), nonché quelli – esercitabili direttamente o facendo richiesta a un'autorità giudiziaria statale – di ordinare la cessazione delle violazioni e, se opportuno, imporre misure correttive proporzionate e necessarie a tal fine (*lett. b*), e di adottare misure provvisorie per evitare il rischio di un danno grave (*lett. e*).

Quanto al secondo caso, le lett. *c*) e *d*) del par. 2 in discorso delineano, rispettivamente, il potere dei coordinatori dei servizi digitali – anche per il tramite di un'autorità giudiziari nazionale – di imporre *sanzioni pecuniarie* per l'inosservanza del Regolamento (dunque, anche con riferimento all'emissione degli ordini di indagine di cui al par. 1), nonché *penalità di mora* volte a garantire il rispetto di un ordine di cessazione delle violazioni di cui alla *lett. b*) o di uno dei, già ricordati, ordini di indagine. Trattasi di poteri che possono essere esercitati nei confronti non solo del *provider*, ma, come si è detto, anche di altre persone «in caso di mancato rispetto di uno qualsiasi degli ordini emessi nei loro confronti», previa informativa «in tempo utile» in relazione agli ordini in parola (compresi termine applicabile, sanzioni per l'inottemperanza, possibilità di ricorso). Le sanzioni, pertanto, non attengono qui *stricto sensu* a violazioni degli obblighi del DSA – i quali ricadono, in effetti, sui fornitori di servizi intermediari – ma presidiano

[31] Sulle tecniche di recepimento di tale clausola nel diritto interno v., per tutti, A. Gullo, *Deflazione e obblighi di penalizzazione di fonte UE*, in *Dir. pen. cont.*, 10 febbraio 2016.

[32] V. al riguardo *supra* (cap. 2, par. 4.4).

[33] *Infra* par. 6.1.

[34] Sul tema nel contesto dell'attività della Commissione v. *infra*, par. 6.1.

piuttosto, attraverso l'impiego della tecnica ingiunzionale[35], l'inosservanza da parte di altri soggetti degli ordini impartiti dal coordinatore nazionale – ad esempio, quello di consentire un'ispezione o di fornire informazioni.

Il par. 3 dell'art. 51 DSA prevede, infine, il potere dei coordinatori dei servizi digitali di adottare misure ulteriori nei riguardi dei *provider* a condizioni molto stringenti – sostanzialmente quale *ultima ratio* – laddove tutti gli altri poteri *ex* art. 51 siano stati esauriti e la violazione non sia cessata, non vi sia stato posto rimedio o prosegua e causi un danno grave, non evitabile neppure attraverso l'esercizio di altri poteri a livello unionale o nazionale.

Nell'alveo di queste misure rientrano: l'imposizione all'organo di gestione di tali fornitori di esaminare la situazione senza ritardo, di adottare e presentare un piano di azione che definisca le misure necessarie alla cessazione della violazione, di provvedere affinché il *provider* le adotti e di riferire su di esse (*lett. a*); la richiesta all'autorità giudiziaria competente dello Stato membro di ordinare la restrizione temporanea dell'accesso al servizio interessato dalla violazione da parte dei destinatari o, solo se ciò non sia fattibile tecnicamente, la restrizione dell'accesso all'interfaccia *online* interessata dalla violazione (*lett. b*).

Come si è anticipato, la richiesta di restrizione all'accesso, quale misura invasiva e incidente su diritti fondamentali, è attivabile solo a fronte di violazioni di rilevante gravità e la relativa procedura è accompagnata da particolari garanzie. Il coordinatore dei servizi digitali può, invero, procedere rivolgendosi all'autorità giudiziaria nazionale solo ove ritenga che un fornitore di servizi intermediari non si sia conformato in modo sufficiente agli obblighi appena descritti *sub* art. 51, par. 3, *lett. a*) DSA, e che alla violazione non si sia rimediato e che essa causi un danno grave e integri un reato grave che minacci la vita o la sicurezza delle persone.



Prima di inoltrare tale richiesta il coordinatore è tenuto a invitare le parti interessate a presentare osservazioni scritte, illustrando le misure individuate e identificando i destinatari delle stesse. La norma ribadisce che, quanto alla scelta, le misure debbono risultare «proporzionate alla natura, alla gravità, alla reiterazione e alla durata della violazione», senza limitare indebitamente l'accesso alle informazioni lecite da parte dei destinatari del servizio. Si prevede, poi, nell'ambito del procedimento giudiziario dinanzi all'autorità competente, la possibilità di partecipazione del *provider*, dei destinatari previsti e dei terzi che abbiano un interesse legittimo.

Le suddette restrizioni all'accesso sono disposte per un periodo di quattro settimane, passibili di proroga, entro il numero massimo stabilito, per ulteriori periodi della stessa durata, su ordine dell'autorità giudiziaria competente. L'art. 51, par. 3 DSA chiarisce inoltre un aspetto di rilievo, legato alla circostanza che il coordinatore dei servizi digitali può prorogare il periodo di restrizione unicamente se – considerati i diritti dei soggetti a vario titolo coinvolti – ricorrono, congiuntamente, due condizioni: ossia, che il fornitore di servizi intermediari non abbia adottato le misure necessarie alla cessazione della violazione e che la restrizione temporanea non limiti indebitamente l'accesso dei destinatari del servizio alle informazioni lecite (avuto riguardo al numero di destinatari interessati e all'esistenza di alternative adeguate e facilmente accessibili). Se tali condizioni persistono ma non è più possibile prorogare, il coordinatore potrà presentare una nuova richiesta di restrizione all'accesso all'autorità giudiziaria.

[35] Su tale tecnica sanzionatoria v. già C. Pedrazzi, *Odierne esigenze economiche e nuove fattispecie penali*, in *Riv. it. dir. proc. pen.*, 1975, 4, 1099 ss. L'utilizzo di tale tecnica è stato poi promosso in dottrina soprattutto nei contesti di incertezza scientifica: v. di recente, anche per ulteriori riferimenti bibliografici, E. Birritteri, *Salute pubblica, affidamento dei consumatori e diritto penale. Limiti e prospettive di tutela nel settore alimentare tra individuo ed ente collettivo*, Torino, 2022, 270 ss.

Va detto che sono stati avanzati dubbi in merito alla compatibilità di tale prescrizione con il principio di proporzionalità – ribadito, come visto, dallo stesso art. 51 DSA – nella parte in cui essa dispone una durata fissa, pari a quattro settimane, del periodo di restrizione e dei successivi periodi di proroga, senza dare la possibilità al giudice di una modulazione parametrata sulle effettive esigenze poste dal caso concreto; a ciò si aggiungono perplessità legate alla circostanza che il DSA non prenda posizione sul numero massimo di rinnovi, che spetterà alla stessa autorità giudiziaria stabilire[36].

Da ultimo, l'art. 51 del DSA si premura di affidare agli Stati la definizione delle condizioni e le procedure specifiche per l'esercizio dei poteri qui descritti, secondo le garanzie previste dal diritto nazionale, in conformità alla Carta di Nizza e al diritto dell'Unione, con particolare attenzione al rispetto della vita privata e al diritto di difesa.

## *3.1 (Segue).* I poteri sanzionatori degli Stati membri e gli strumenti di tutela dei destinatari del servizio

Venendo ora a esaminare l'apparato punitivo tratteggiato, nel DSA, all'art. 52, deve in primo luogo evidenziarsi come il legislatore europeo si sia orientato nel senso di demandare agli Stati Membri di stabilire norme relative alle sanzioni applicabili in caso di violazioni del Regolamento da parte dei *provider* rientranti nella loro competenza, nonché di adottare ogni misura necessaria a assicurare l'implementazione del DSA e di notificare poi tali norme e misure alla Commissione, anche in sede di eventuali successive modifiche.



Ancora, la norma chiarisce che gli Stati membri sono chiamati ad assicurare una risposta sanzionatoria che presenti i connotati dell'effettività, proporzionalità e dissuasività (par. 2). Nondimeno, mancano indicazioni espresse[37] sulla *natura* delle sanzioni – dovendosi in ogni caso ritenere che si tratti di sanzioni amministrative – mentre se ne definisce la tipologia – essenzialmente, di carattere pecuniario – e si prevede altresì un tetto massimo per gli importi di tali «penalties». L'art. 52 DSA, nella specie, attribuisce ai coordinatori nazionali la prerogativa di irrogare sanzioni pecuniarie (*fine*) e penalità di mora (*periodic penalty payment*).

In particolare, quanto alla prima categoria, ai sensi del par. 3, si dovrà assicurare che l'importo massimo di tali sanzioni per i casi di inosservanza di un obbligo stabilito dal DSA sia pari al 6% del fatturato annuo mondiale del fornitore di servizi intermediari interessato, considerando l'esercizio finanziario precedente.

Nel caso, invece, di sanzione pecuniaria per la comunicazione di informazioni inesatte, incomplete o fuorvianti, di mancata risposta o rettifica di tali informazioni e di inosservanza dell'obbligo di sottoporsi a un'ispezione, gli Stati membri dovranno provvedere affinché l'importo massimo sia pari all'1 % del reddito annuo o del fatturato mondiale del fornitore dei servizi intermediari o della persona interessati, sempre nell'esercizio finanziario precedente. Si utilizza, sul punto, una tecnica diversa da quella di cui all'art. 83 GDPR in materia di *privacy*, ove, a seconda del tipo di violazione, si fissa un massimo pari a 10 o 20 milioni di euro o, per le imprese, pari al 2% o 4% del fatturato mondiale annuo, solo però se superiore ai predetti importi; a differenza del DSA, quindi, il fatturato è qui un criterio alternativo[38].

[36] V. le argomentazioni di I. Castellucci, F. Coppola, *Il sistema sanzionatorio decentrato del DSA*, cit., 54.

[37] Per rimanere nel campo dei regolamenti, cfr. art. 83 GDPR, dove si parla espressamente di sanzioni *amministrative* pecuniarie.

[38] Per un commento alla norma v. S. Aterno, Sub *art. 83*, in G.M. Riccio, G. Scorza, E. Belisario (a cura di), *GDPR e normativa privacy. Commentario*, Milano, 2022, 734 ss.

Il tetto dell'altra *penalty* prevista dal par. 4 dell'art. 52 DSA, ossia la penalità di mora – che può essere imposta, come anticipato, per assicurare il rispetto di un ordine di cessazione delle violazioni o di uno degli ordini di indagine[39] – non può superare il 5% del fatturato – in questo caso – giornaliero medio mondiale o del reddito del fornitore di servizi intermediari interessato nel precedente esercizio finanziario, calcolato a decorrere dalla data specificata nella decisione.

Appare poi di interesse fare alcuni cenni ai mezzi di tutela dell'utente delineati specificamente nell'ambito della disciplina delle prerogative del coordinatore dei servizi digitali, subito a seguire le previsioni in materia di poteri e sanzioni sin qui esaminate.

Preliminarmente, è bene ricordare che il DSA prevede, in termini generali, diversi possibili rimedi, sia di tipo *interno* alle piattaforme – si fa riferimento in particolare ai sistemi di gestione dei reclami che gli stessi operatori sono tenuti a implementare, *ex* art. 20 DSA –, sia di tipo *esterno*, compresa la possibilità di «scegliere qualunque organismo di risoluzione extragiudiziale delle controversie»[40] certificato dal coordinatore nazionale, anche per definire i *complaint* «che non è stato possibile risolvere mediante il sistema interno di gestione dei reclami» (art. 21, par. 1 DSA)[41].

Rispetto a tale opzione, poiché l'art. 21, par. 2 DSA stabilisce che l'organismo in questione non ha comunque il potere di imporre alle parti una risoluzione vincolante della controversia, in caso di perdurante disaccordo rimane impregiudicato il diritto degli utenti di adire un organo giurisdizionale conformemente al diritto applicabile, ad esempio per ottenere la rimozione di contenuti *online*. Qui viene in rilievo anche la disposizione – inserita nella sezione 1 del Capo IV in commento, dedicata ai coordinatori nazionali – secondo cui i destinatari del servizio possono chiedere un risarcimento ai fornitori di servizi intermediari, conformemente al diritto dell'Unione e a quello nazionale, in relazione a danni o perdite subiti a seguito di una violazione degli obblighi stabiliti dal Regolamento (art. 54 DSA).



Tra i rimedi relativi all'«access to justice outside of platforms»[42], il DSA introduce la possibilità, per i destinatari del servizio – oltre che per i soggetti incaricati di esercitare, per conto di costoro, i diritti conferiti dal DSA (ad esempio organismi, organizzazioni, associazioni) – di proporre al coordinatore dei servizi digitali dello Stato in cui essi sono situati o stabiliti dei reclami (*complaint*) vertenti su violazioni del Regolamento nei confronti dei fornitori di servizi intermediari (art. 53 DSA).

La procedura prevede che il coordinatore ricevente debba provvedere a valutare il reclamo e, se del caso, trasmetterlo al coordinatore dei servizi digitali del luogo di stabilimento, eventualmente corredato da un parere; inoltre, nell'ambito del suo ruolo di coordinamento, se reputa che il reclamo rientri nella responsabilità di un'altra autorità competente nel suo stesso Stato, il coordinatore ricevente lo trasmette a quest'ultima. Entrambi le parti conservano, in tali circostanze, il diritto di essere ascoltati e di ricevere informazioni sullo stato del reclamo.

---

[39] *Supra*, par. 3

[40] V. in argomento A.M. Felicetti, *La risoluzione extragiudiziale delle dispute nei mercati digitali: alcune novità dall'Europa*, in *Riv. trim. dir. proc. civ.*, 2023, 1, 197 ss.

[41] Su tali previsioni, si rinvia al cap. 2 (parr. 3.1 e 3.2).

[42] Su cui v. P. Ortolani, *If You Build it, They Will Come. The DSA "Procedure Before Substance" Approach*, in J. Van Hoboken e altri (a cura di), *Putting the Digital Services Act into Practice*, cit., 158 ss.

# 4 La disciplina in tema di assistenza reciproca con la Commissione europea e cooperazione transfrontaliera dei coordinatori nazionali

La sezione 2 del Capo IV delinea una puntuale disciplina – nel quadro del riparto di competenze tra livello nazionale e europeo di cui si parlato[43] – in materia di assistenza reciproca (art. 57 DSA), cooperazione transfrontaliera tra coordinatori di servizi digitali e deferimento alla Commissione (artt. 58-59 DSA), nonché indagini comuni (art. 60 DSA).

Emerge qui con particolare nitore il complesso di tipo 'reticolare' di cui si è detto: l'operato dei diversi attori, nell'ottica di mutua collaborazione, è scandito da tempistiche predeterminate e alquanto serrate; appare inoltre chiaro come uno degli obiettivi di fondo di tali previsioni sia quello di evitare l'inerzia delle autorità coinvolte, disponendo che in caso di mancato rispetto dei termini fissati, soccorrano meccanismi certi per il superamento della stasi decisionale in merito a una presunta violazione.

La prima norma rilevante attiene all'assistenza reciproca tra i coordinatori dei servizi digitali e la Commissione, in cui rientrano – nell'ottica di una coerente ed efficiente applicazione del DSA – lo scambio di informazioni e il dovere, in capo al coordinatore del luogo di stabilimento, di informare tutti i coordinatori dei servizi digitali del luogo di destinazione, il Comitato europeo per i servizi digitali e la Commissione in caso di avvio di un'indagine e rispetto all'intenzione di adottare una decisione definitiva nei confronti di uno specifico *provider* di servizi intermediari (art. 57, par. 1, DSA).

La collaborazione si estrinseca anche attraverso la possibilità che il coordinatore del luogo di stabilimento richieda informazioni – o richieda di esercitare i poteri di indagine ai sensi dell'art. 51, par. 1, DSA – ad altri coordinatori dei servizi digitali, i quali sono tenuti a soddisfare la richiesta «senza indebito ritardo» e comunque entro due mesi dal suo ricevimento. Se non è possibile dare a essa seguito – e le ragioni normativamente ammesse sono limitate ai casi di richiesta non sia sufficientemente specificata, motivata o proporzionata alla luce delle finalità dell'indagine, di mancato possesso delle informazioni e di impossibilità di soddisfare detta richiesta senza violare il diritto dell'Unione o nazionale –, il coordinatore ricevente dovrà giustificare il rifiuto, presentando, entro il medesimo termine, una risposta motivata.



Proseguendo, la previsione in tema di cooperazione transfrontaliera tra i coordinatori dei servizi digitali, *ex* art. 58 DSA, si apre con una clausola di salvaguardia che impedisce ai coordinatori nazionali di attivarsi per il caso in cui la Commissione abbia avviato un'indagine per la stessa presunta violazione.

Ove così non sia, il coordinatore dei servizi digitali del luogo di destinazione che sospetti una violazione del Regolamento con possibili ripercussioni negative sui destinatari del servizio nel proprio Stato membro, perpetrata da un fornitore di servizi intermediari, può chiedere al coordinatore del luogo di stabilimento di valutare la questione e adottare le misure di indagine ed *enforcement* necessarie (par. 1). La medesima procedura può essere messa in moto dal Comitato su richiesta di almeno tre coordinatori dei servizi digitali del luogo di destinazione nelle medesime circostanze (par. 2)[44].

[43] *Supra*, par. 2.

[44] Ai sensi dell'art. 58, par. 3, DSA, le richieste in questione debbono essere motivate e specifiche almeno rispetto al punto di contatto del fornitore di servizi intermediari interessato ai sensi dell'art. 11 DSA, alla descrizione dei fatti rilevanti, delle disposizioni del DSA interessate, dei motivi di sospetto e della descrizione degli effetti negativi della presunta violazione, nonché a qualsiasi altra informazione che il coordinatore richiedente o il Comitato ritenga pertinenti, compresi suggerimenti per l'adozione di specifiche misure di indagine o di esecuzione.

Si prescrive che il coordinatore dei servizi digitali del luogo di stabilimento debba tenere «nella massima considerazione tali richieste, anche domandando informazioni supplementari al coordinatore richiedente o al Comitato, secondo la procedura dell'art. 57 DSA o, in alternativa, avviando un'indagine congiunta ai sensi dell'art. 60, par. 1, DSA; in ogni caso, è tenuto a comunicare la sua valutazione sulla presunta violazione, unitamente a una spiegazione delle eventuali misure di indagine o di esecuzione adottate o previste, entro due mesi dal ricevimento della richiesta.

Per i casi, sostanzialmente, di mancata valutazione o di disaccordo sul merito delle scelte proposte, la normativa introduce anche una procedura di *referral* da parte del Comitato europeo per i servizi digitali alla Commissione (art. 59 DSA), volta a evitare il rischio di inazione o l'adozione di misure insoddisfacenti da parte delle autorità nazionali. La Commissione è a sua volta chiamata a valutare la questione entro due mesi dal deferimento, ma se ritiene che le misure già adottate siano insufficienti o incompatibili con il DSA, può fornire un parere in merito richiedendo al coordinatore dei servizi digitali del luogo di stabilimento di riesaminare il caso[45].

Merita un cenno anche la disciplina delle indagini comuni che possono essere avviate e dirette dal coordinatore dei servizi digitali del luogo di stabilimento – di propria iniziativa o dietro raccomandazione del Comitato, su richiesta di almeno tre coordinatori – con la partecipazione di altri coordinatori interessati, laddove venga in rilievo una violazione del DSA con impatto in più Stati membri.

I coordinatori dei servizi digitali partecipanti cooperano in buona fede e, peraltro, qualsiasi coordinatore che dimostri di avere un interesse legittimo alla partecipazione può fare richiesta; ai coordinatori dei servizi digitali del luogo di destinazione si riconosce il diritto di esercitare i loro poteri di indagine nei confronti dei fornitori di servizi intermediari interessati per ciò che concerne le informazioni e i locali situati nel loro territorio.



Anche in sede di indagini congiunte, è poi fatta salva, a specifiche condizioni, la possibilità di deferimento alla Commissione a cura del Comitato[46].

A garanzia della certezza dei tempi procedimentali è stabilito un termine di tre mesi per la conclusione dell'indagine – decorrenti, salvo diverso accordo tra i partecipanti, dall'avvio della stessa – e, non oltre un mese da tale scadenza, il coordinatore dei servizi digitali che ha promosso l'indagine dovrà comunicare a tutti i coordinatori dei servizi digitali, alla Commissione e al Comitato la sua posizione preliminare sulla presunta violazione, con la quale si potranno disporre anche misure di esecuzione.

[45] L'art. 59, par. 3, DSA precisa che «il coordinatore dei servizi digitali del luogo di stabilimento adotta le misure di indagine o di esecuzione necessarie [...] tenendo nella massima considerazione il parere e la richiesta di riesame della Commissione», dovendo poi fornire informazioni in merito alle misure adottate entro due mesi dalla richiesta di riesame.[45] L'art. 59, par. 3, DSA precisa che «il coordinatore dei servizi digitali del luogo di stabilimento adotta le misure di indagine o di esecuzione necessarie [...] tenendo nella massima considerazione il parere e la richiesta di riesame della Commissione», dovendo poi fornire informazioni in merito alle misure adottate entro due mesi dalla richiesta di riesame.

[46] Ai sensi dell'art. 60, par. 3, DSA il Comitato può deferire la questione alla Commissione se: il coordinatore dei servizi digitali del luogo di stabilimento non abbia comunicato la sua posizione preliminare entro il termine previsto; se si trovi in sostanziale disaccordo con la posizione preliminare comunicata dal predetto coordinatore; se quest'ultimo abbi amesso di avviare prontamente l'indagine congiunta a seguito di raccomandazione del Comitato.

# 5 Il raccordo istituzionale tra Stati membri e Commissione europea: il Comitato europeo per i servizi digitali

L'architettura del DSA prevede l'istituzione del – più volte menzionato – Comitato europeo per i servizi digitali[47], soggetto in qualche misura 'intermedio' tra il livello nazionale – rappresentato dalle autorità competenti con il ruolo chiave, come illustrato, dei coordinatori dei servizi digitali – e il livello europeo, che vede protagonista delle attività di *enforcement* destinate ai grandi *player* del mercato digitale la Commissione.

È possibile considerare il Comitato una realtà 'a metà strada' nel riparto di competenze tra Stati membri e Commissione dal momento che esso è composto, come subito si dirà, da coordinatori dei servizi digitali nazionali, ma è presieduto dalla Commissione: si tratta, quindi, del meccanismo istituzionalmente previsto per il raccordo, in tema di vigilanza sull'applicazione del Regolamento, tra ambito nazionale ed europeo. Come si è osservato, simili organismi non costituiscono una novità nel panorama regolatorio dell'Unione: si pensi, nel contesto della protezione dei dati, allo *European Data Protection Board*[48].

I caratteri essenziali del Comitato, avuto riguardo agli obiettivi perseguiti, alla struttura e ai compiti, sono descritti nella sezione 3 del Capo IV del DSA (artt. 62-64 DSA). Più in particolare, Il Comitato è un gruppo consultivo indipendente di coordinatori dei servizi digitali per la vigilanza sui *provider* di servizi intermediari, la cui *mission* è di contribuire all'applicazione coerente del Regolamento e alla cooperazione efficace dei coordinatori nazionali e della Commissione, di coordinare e contribuire agli orientamenti e alle analisi della Commissione, dei coordinatori nazionali e di altre autorità competenti sulle questioni emergenti nel mercato interno nelle materie disciplinate dal DSA, nonché di assistere i coordinatori dei servizi digitali e la Commissione nella vigilanza sulle piattaforme online di dimensioni molto grandi (così l'art. 61, par. 2, DSA).



Quanto alla sua composizione, si prevede la partecipazione di tutti i coordinatori dei servizi digitali degli Stati membri rappresentati da funzionari di alto livello[49]. Se tuttavia in ambito nazionale vi sono altre autorità competenti «investite di specifiche responsabilità operative per l'applicazione e l'esecuzione» del DSA insieme al coordinatore dei servizi digitali, esse possono partecipare al Comitato; è altresì ammessa la possibilità che altre, diverse autorità nazionali possano essere invitate alle riunioni, ove siano oggetto di discussione questioni per loro di rilievo. Per evitare che il Comitato non possa attivarsi in ragione dell'inerzia degli Stati membri, è stabilito che la mancata designazione di uno o più coordinatori dei servizi digitali nazionali non impedisce a esso di svolgere i propri compiti (art. 62, par. 1, DSA). Come si anticipava, è la Commissione a presiedere il Comitato e a convocarne le riunioni, fornendo anche il necessario sostegno amministrativo e analitico per lo svolgimento delle attività[50]. Alle riunioni del Comitato possono essere invitati esperti e osservatori e si prevede la possibilità di cooperazione con altre istituzioni e altri organi dell'Unione nonché con esperti esterni, e di consultazione delle parti interessate, assicurando che i risultati di dette attività siano resi disponibili per il pubblico.

[47] Sul tema v. E.M. Tripodi, *Le Autorità competenti*, cit., 63 ss.

[48] Cfr. G. Buttarelli, *La regolazione delle piattaforme digitali*, cit., 123.

[49] Osserva E.M. Tripodi, *Le Autorità competenti*, cit., 64 che «[d]el «gruppo» fanno parte funzionari di alto livello (uno per ogni coordinatore nazionale con «diritto di voto» mentre possono essere presenti anche altri rappresentanti per le autorità competenti, ovvero altre autorità nazionali), ma non il Presidente o il rappresentante del Coordinatore nazionale. Si tratta, pertanto di un consesso "tecnico" e non politico».

[50] Il funzionamento del Comitato sarà disciplinato da un regolamento interno, adottato previo accordo con la Commissione (art. 62, par. 7, DSA).

Se, secondo le prescrizioni del DSA, al Comitato è richiesto di adottare una raccomandazione[51], esso deve mettere tale richiesta a disposizione degli altri coordinatori dei servizi digitali nazionali «immediatamente», avvalendosi del sistema di condivisione delle informazioni appositamente previsto dall'art. 85 DSA: si tratta, nella specie, di un sistema affidabile e sicuro che dovrà essere istituito e manutenuto dalla Commissione europea e che rappresenterà il canale ordinario per lo scambio di informazioni tra i coordinatori dei servizi digitali, la Commissione e il Comitato, i quali ne dovranno fare uso per tutte le comunicazioni sancite dal Regolamento. Con riferimento ai meccanismi di funzionamento del Comitato, ogni Stato membro dispone di un voto mentre la Commissione non ha diritto di voto, e gli atti del Comitato sono adottati a maggioranza semplice (art. 62, par. 3, DSA).

I compiti del Comitato sono delineati all'art. 63 DSA e ad alcuni di questi – data la natura 'trasversale' di tale organismo – si è già fatto o si farà ancora riferimento: si tratta del supporto al coordinamento delle indagini congiunte di cui all'art 60 DSA[52]; dell'assistenza alle autorità competenti nell'analisi delle relazioni e dei risultati delle revisioni di piattaforme *online* o motori di ricerca di dimensioni molto grandi[53]; della predisposizione di pareri, raccomandazioni o consulenze ai coordinatori dei servizi digitali nazionali; della consulenza alla Commissione in riferimento all'avvio di un procedimento a carico di *provider* di piattaforme *online* o motori di ricerca *online* di dimensioni molto grandi (art. 66 DSA)[54] e di adozione di pareri in relazione ai medesimi soggetti; della promozione dell'elaborazione e attuazione di norme, orientamenti, relazioni, modelli e codici di condotta europei in cooperazione con i pertinenti portatori di interessi, come previsto dal DSA, anche fornendo pareri o raccomandazioni su questioni connesse all'art. 44 DSA (in tema di sviluppo e attuazione di *voluntary standards*), nonché dell'individuazione di questioni emergenti in relazione alle materie disciplinate dal Regolamento.

L'art. 63, par. 2, DSA chiarisce che per discostarsi da tali pareri, richieste o raccomandazioni del Comitato i coordinatori dei servizi digitali (e, se del caso, le altre autorità nazionali competenti) debbono giustificare la scelta, fornendo una spiegazione sulle indagini, le azioni e le misure che hanno attuato.



## 6 I poteri di *enforcement* della Commissione europea: un 'interlocutore privilegiato' dei più grandi *player* del mercato digitale

Nella struttura di tipo ascendente – dal livello nazionale a quello europeo – che l'articolato del DSA pare delineare nel Capo qui in commento, la relativa sezione 4 è dedicata in larga parte all'analisi dei poteri della Commissione europea[55], soggetto che – come si è già posto in luce – assume un ruolo centrale

[51] Tra le raccomandazioni che il Comitato può proporre, si segnala quella prevista nel contesto della particolare procedura di risposta alle crisi *ex* art. 36 DSA, nell'ambito della quale la Commissione può imporre a uno o più fornitori di piattaforme *online* o di motori di ricerca *online* di dimensioni molto grandi di intraprendere azioni preventive, di mitigazione dei rischi e di *reporting* «quando circostanze eccezionali» comportino una minaccia grave «per la sicurezza pubblica o la salute pubblica nell'Unione o in parti significative di essa» (questa la definizione di 'crisi' di cui all'art. 36, par. 2, DSA). In tali casi, il Comitato è tenuto a votare entro 48 ore dalla richiesta del suo presidente (art. 62, par. 3, DSA).

[52] V. *supra*, par. 4.

[53] Si possono ad esempio richiamare le revisioni indipendenti *ex* artt. 35 e 75, par. 2, DSA già menzionate *supra*,

[54] Su cui v. *infra*, par. 6.

[55] Per alcune considerazioni sul ruolo della Commissione nel contesto del DSA v. A. Contaldo, *Il DSA e le competenze della Commissione europea sulla stregua della procedura anticoncorrenziale e la scelta del* "ne bis in idem", in *Dir. internet*, 2023, 1, 73 ss.

nell'*enforcement* pubblico del DSA, con particolare riferimento alle piattaforme *online* e ai motori di ricerca *online* di dimensioni molto grandi.

L'analisi svolta ha già fatto emergere come l'operato della Commissione in tale contesto si orienti in una duplice direzione: in generale, come attività di *enforcement* concorrente rispetto a quella dei coordinatori nazionali in rapporto alle possibili violazioni del DSA da parte dei *player* di grandi dimensioni; e, particolarmente, come meccanismo esclusivo di risposta alla violazione, da parte di tali soggetti, degli obblighi specifici contenuti nella sezione 5 del Capo III. Invero, la norma di apertura della sezione ora in esame puntualizza, nella cornice di un generale ruolo di promozione e sviluppo delle competenze e capacità dell'Unione *in subiecta materia* da parte della Commissione, che a questa spetta il coordinamento della valutazione delle questioni sistemiche ed emergenti in tutta l'Unione in relazione alle piattaforme *online* e ai motori di ricerca *online* di dimensioni molto grandi (art. 64, par. 2, DSA). Ciò a ribadire – fatti salvi i predetti obblighi del Capo III, sezione 5 – che di tali categorie di destinatari possano, in principio, occuparsi anche i coordinatori nazionali, pur competendo il 'coordinamento generale' alla Commissione. Rispetto all'assetto dei poteri della Commissione nei confronti delle «large platforms», può osservarsi che essi ricalcano, per molti versi, quelli già visti rispetto ai coordinatori dei servizi digitali degli Stati membri[56]: anche qui vengono in considerazione poteri d'indagine, poteri di esecuzione e di imposizione di sanzioni ma – come si avrà modo di chiarire – da un lato, anche rispetto a tali poteri 'comuni', le norme della sezione dedicata all'*enforcement* da parte della Commissione sono, sul piano dei contenuti, maggiormente dettagliate; dall'altro, si aggiungono strumenti peculiari, di cui solo la Commissione dispone, rivolti unicamente a *VLOP*s e *VLOSE*s. All'art. 65 il Regolamento si premura anzitutto di precisare che la Commissione può esercitare i poteri di indagine sia di propria iniziativa, sia su richiesta di un coordinatore nazionale[57], anche prima di avviare un formale procedimento, secondo i dettami dell'art. 66, par. 2, DSA.



L'*iter* di accertamento di eventuali violazioni di disposizioni del DSA da parte di *provider* di piattaforme *online* e motori di ricerca *online* di dimensioni molto grandi segue infatti precisi *step* procedurali: la Commissione, ove sospetti che la condotta di uno di tali soggetti importi una violazione, può avviare un procedimento in vista dell'adozione di una decisione di non conformità (art. 73 DSA) e dell'irrogazione di sanzioni pecuniarie (art. 74 DSA). A tal fine, essa ne dà *notifica* all'interessato e altresì al Comitato e a tutti i coordinatori dei servizi digitali (art. 66, par. 1, DSA), essendo questi ultimi tenuti a trasmettere, senza indebito ritardo, ogni rilevante informazione di cui siano in possesso.

All'apertura di un procedimento da parte della Commissione consegue l'esonero, per qualsiasi autorità competente, dall'esercizio dei propri poteri di vigilanza ed esecuzione stabiliti nel DSA[58], ferma restando

[56] *Supra*, par. 3.

[57] Nella specie, ai sensi dell'art. 65, par. 2, DSA 2 ove un coordinatore dei servizi digitali abbia motivo di sospettare che un fornitore di una piattaforma *online* o di un motore di ricerca *online* di dimensioni molto grandi abbia violato le disposizioni del Capo III, sezione 5, o abbia violato sistematicamente una delle disposizioni del Regolamento con gravi ripercussioni per i destinatari del servizio nel suo Stato membro, può presentare – attraverso il sistema di condivisione delle informazioni *ex* art. 85 – una richiesta alla Commissione affinché valuti la questione. La richiesta è «debitamente motivata» e specifica almeno il punto di contatto della *VLOP* o del *VLOSE*, una descrizione dei fatti rilevanti, delle disposizioni del DSA pertinenti e dei motivi per cui il coordinatore richiedente sospetti violazioni del Regolamento, nonché qualsiasi altra informazione questi ritenga pertinente, comprese quelle raccolte di propria iniziativa (art. 65, par. 3, DSA).

[58] Il richiamo è all'art. 56, par. 4, DSA a mente del quale «[q]ualora la Commissione non abbia avviato procedimenti per la stessa infrazione, lo Stato membro in cui è situato lo stabilimento principale del fornitore di una piattaforma online di dimensioni molto grandi o di un motore di ricerca online di dimensioni molto grandi dispone di poteri di vigilanza e di applicazione degli obblighi di cui al presente regolamento diversi da quelli di cui al capo III, sezione 5, nei confronti di tali fornitori».

la possibilità che la Commissione richieda il sostegno, singolo o congiunto, dei coordinatori dei servizi digitali interessati dalla presunta violazione[59], i quali dovranno cooperare «lealmente e tempestivamente» (art. 66, par. 3, DSA).

Come si anticipava, i poteri attivabili in sede d'indagine, funzionali allo svolgimento dei compiti assegnati alla Commissione, sono sostanzialmente analoghi a quelli attribuiti alle autorità nazionali e attengono alla richiesta di informazioni (art. 67 DSA), alle audizioni e raccolta di dichiarazioni (art. 68 DSA), all'effettuazione di ispezioni (art. 69 DSA), all'adozione di misure provvisorie (art. 70), alla possibilità che la Commissione renda gli impegni assunti dal *provider* vincolanti e ponga in essere le relative azioni di monitoraggio (artt. 71 e 72 DSA).

Per assicurare un 'controllo incrociato' sull'operato della Commissione, si stabilisce in ogni caso che essa debba fornire al coordinatore dei servizi digitali del luogo di stabilimento e al Comitato europeo per i servizi digitali tutte le pertinenti informazioni sull'esercizio dei suddetti poteri, nonché le sue constatazioni preliminari, sulle quali il Comitato è chiamato a fornire un parere[60].

Soffermando qui l'attenzione sui profili caratterizzanti i poteri di cui la Commissione è titolare, anche nel raffronto con quelli delle autorità nazionali, possono essere sottolineati, in linea generale, alcuni aspetti.

Anzitutto, anche i poteri della Commissione si indirizzano tanto ai grandi *player* direttamente, quanto a «qualsiasi altra persona fisica o giuridica che agisca per fini connessi alla propria attività commerciale, imprenditoriale, artigianale o professionale e che possa ragionevolmente essere a conoscenza di informazioni relative alla presunta violazione, comprese le organizzazioni che effettuano le revisioni indipendenti *ex* artt. 37 e 75, par. 2», al riguardo ricalcandosi testualmente l'art. 51 DSA[61] con riferimento a quanto disposto per i coordinatori nazionali.



In secondo luogo, ove è previsto che tali poteri siano, o possano essere, esercitati mediante decisione (come per le richieste di informazioni o le ispezioni), la Commissione è tenuta a specificare, tra l'altro, lo scopo della richiesta, i tempi, le sanzioni pecuniarie e le penalità di mora irrogabili, indicando il diritto dei soggetti incisi di chiedere il riesame della decisione alla Corte di giustizia dell'Unione europea. Inoltre, le norme in tema di poteri d'indagine della Commissione paiono improntate ad assicurare – forse anche in modo ancora più puntuale rispetto alle omologhe disposizioni riguardanti i coordinatori nazionali – un costante flusso di comunicazione e scambio reciproco d'informazioni tra tutti i soggetti coinvolti, a voler garantire – particolarmente per le ipotesi che coinvolgono i *provider* di *VLOPS* e *VLOSEs* – non solo uno svolgimento ordinato delle attività, ma un assetto di *checks and balances* sull'esercizio dei penetranti poteri della Commissione.

Emerge poi come proprio detti poteri siano descritti in termini decisamente più dettagliati di quanto non avvenga per quelli dei coordinatori – per i quali il Regolamento rimette la scelta agli Stati membri, rinviando per la definizione delle condizioni e delle procedure specifiche al diritto nazionale. Si veda per raffronto, ad esempio, il grado di precisione della norma in tema di ispezioni della Commissione, che all'art. 69, par. 2 DSA, lett. da *a*) a *g*) puntualizza come queste possano consistere nell'accesso a tutti i locali, terreni e mezzi di trasporto del fornitore o dell'altra persona interessata; nell'esame dei libri e

[59] I quali potranno a quel punto, conformemente alla richiesta, esercitare i loro poteri di indagine (art. 51, par. 1, DSA) nei confronti del *provider* della piattaforma *online* o del motore di ricerca *online* di dimensioni molto grandi riguardo alle informazioni e ai locali ubicati nel loro Stato membro (art. 66, par. 3 DSA).

[60] Con riferimento alle constatazioni preliminari della Commissione v. anche *infra*, par. 6.1.

[61] *Supra*, par. 3.

qualsiasi altro documento relativo alla fornitura del servizio in questione e nell'ottenimento di copie o estratti; nella richiesta di fornire accesso e chiarimenti relativi all'organizzazione, al funzionamento, al sistema informatico, agli algoritmi, alla gestione dei dati e alle pratiche commerciali dell'impresa nonché di registrare o documentare i chiarimenti forniti; nel sigillare i locali; nel chiedere chiarimenti e rivolgere domande a qualsiasi rappresentante o membro del personale in relazione a fatti o documenti inerenti all'oggetto e allo scopo dell'accertamento. In coerenza con la previsione dell'art. 83 DSA che attribuisce alla Commissione il potere di adottare atti di esecuzione riguardanti le modalità pratiche per la conduzione di taluni procedimenti – tra cui ispezioni, audizioni e divulgazione negoziata di informazioni di cui all'art. 79 DSA – è attualmente in corso di adozione la relativa bozza di *implementing regulation*[62].

Nell'ambito di un procedimento che può portare all'adozione di una decisione di non conformità, la Commissione può con decisione ordinare misure provvisorie nei confronti del fornitore della piattaforma *online* o del motore di ricerca *online* di dimensioni molto grandi (art. 70 DSA), in caso di urgenza dovuta al rischio di danni gravi per i destinatari del servizio e sulla base di una constatazione *prima facie* della sussistenza di una violazione[63].

Da ultimo, è disposto che, qualora siano stati esauriti tutti i poteri della Commissione e la violazione persista, causando un danno grave non evitabile attraverso il ricorso a altri poteri previsti in ambito nazionale o dell'Unione, la Commissione europea possa sollecitare, a norma dell'art. 82 DSA, il coordinatore del luogo di stabilimento del fornitore della piattaforma *online* o del motore di ricerca *online* di dimensioni molto grandi interessato ad adire l'autorità giudiziaria per richiedere una restrizione all'accesso *ex* art. 51, par. 3 DSA.

## 6.1 (*Segue*). Le soluzioni "negoziate" per la definizione del procedimento tra Commissione e *very large online platform* e le sanzioni all'esito di «non-compliance decisions»



Se, nel corso di un procedimento avviato dalla Commissione, un *provider* della piattaforma *online* o del motore di ricerca *online* di dimensioni molto grandi offre di assumersi *impegni* (*commitment*) volti a garantire la conformità alle pertinenti disposizioni del DSA, si prevede che la Commissione possa, mediante decisione, rendere tali impegni vincolanti per quel fornitore, dichiarando che non vi sono ulteriori motivi per intervenire (art. 71, par. 1, DSA).

Ciò non mette, tuttavia, il fornitore in ogni caso al riparo dall'instaurazione di futuri procedimenti da parte della Commissione, che invero può – su richiesta o di propria iniziativa – riaprire il caso laddove, alternativamente: si verifichi un cambiamento determinante di uno dei fatti su cui si è fondata la decisione (*lett. a*); il fornitore in questione agisca in contrasto con i propri impegni (*lett. b*); la decisione sia stata fondata su informazioni incomplete, inesatte o fuorvianti trasmesse dal fornitore o da un'altra persona ai sensi dell'art. 67, par. 1, DSA.

D'altronde, la Commissione non è neppure tenuta ad accettare, per così dire, 'a monte' tali impegni,

[62] Per il procedimento seguito, che prevede la pubblicazione di un *draft* da parte della Commissione e un periodo di raccolta di osservazioni da parte dei soggetti interessati, oltre che per la consultazione del testo proposto, si veda il seguente indirizzo: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13565-Digital-Services- Act-implementing-regulation_en.

[63] L'art. 70, par. 2, DSA precisa che le tali decisioni si applicano per un periodo determinato e possono essere rinnovate «se necessario e opportuno».

ben potendo – ove ritenga che questi non siano idonei a garantire l'effettivo rispetto delle pertinenti disposizioni del Regolamento – respingerli con decisione motivata al momento della conclusione del procedimento (art. 71, par., 3 DSA).

Lo svolgimento dei compiti della Commissione risulterebbe alquanto difficile da assicurare ove a essa non fosse consentito di intraprendere «le azioni necessarie per monitorare l'effettiva attuazione e osservanza» del DSA da parte di *VLOPs* e *VLOSEs* (art. 72 DSA). In questa ottica, la Commissione può ordinare a tali soggetti di fornire accesso alle banche dati e agli algoritmi nonché spiegazioni al riguardo, oltre a poter imporre loro l'obbligo di conservazione di tutti i documenti ritenuti necessari per la valutazione sull'osservanza e attuazione degli obblighi del Regolamento. Nell'ambito del monitoraggio, la Commissione può anche avvalersi della consulenza di esperti e revisori esterni indipendenti o delle autorità nazionali competenti.

La Commissione può invece determinarsi all'adozione di una decisione di non conformità (*non-compliance decision*) nei casi di mancato rispetto, da parte del fornitore della piattaforma *online* o del motore di ricerca online di dimensioni molto grandi, di uno o più dei seguenti requisiti: le pertinenti disposizioni del DSA (*lett. a*); le misure provvisorie ordinate *ex* art. 70 DSA (*lett. b*); gli impegni resi vincolanti secondo le prescrizioni dell'art. 71 DSA (*lett. c*) (art. 73, par. 1, DSA)[64].

Considerate le conseguenze di una simile decisione, la relativa adozione è corredata da talune garanzie procedurali: prima di procedere, infatti, la Commissione deve comunicare le proprie constatazioni preliminari al soggetto interessato, illustrando le misure che intende prendere, o che ritiene il fornitore in questione dovrebbe prendere in risposta alle constatazioni preliminari.



La decisione di non conformità contiene l'ordine al fornitore di adottare le misure necessarie a garantire il rispetto della medesima, specificando altresì un termine ragionevole per provvedere e richiedendo informazioni sulle misure che il destinatario preveda di adottare per rendersi *compliant*.

Con la decisione di non conformità *ex* art. 73 la Commissione può imporre al *provider* di *VLOPs* e *VLOSEs* sanzioni pecuniarie analoghe a quelle già esaminate con riferimento ai coordinatori dei servizi digitali nazionali, sebbene le casistiche non siano coincidenti.

In particolare, la Commissione può imporre a tali soggetti sanzioni pecuniarie non superiori al 6 % del fatturato totale realizzato a livello mondiale su base annua nell'esercizio precedente (art. 74, par. 1, DSA) laddove essi, intenzionalmente o per negligenza, violino le pertinenti disposizioni del Regolamento *(lett. a)*, non rispettino una decisione che dispone le misure provvisorie di cui all'art. 70 DSA *(lett. b)* o non si conformino a un impegno reso vincolante ai sensi dell'art. 71 DSA *(lett. c)*.

Alle medesime condizioni, la sanzione in oggetto a carico di *VLOPs* e *VLOSEs* sarà invece pari all'1 % del reddito annuo o del fatturato totale annuo a livello mondiale dell'esercizio precedente – e potrà attingere anche un'altra persona fisica o giuridica ai sensi dell'art. 67, par. 1, DSA – nei casi di: informazioni inesatte, incomplete o fuorvianti in risposta a una richiesta semplice o formulata mediante decisione; mancata risposta entro il termine stabilito alla richiesta di informazioni formulata mediante decisione; omessa rettifica entro i termini di informazioni inesatte, incomplete o fuorvianti, o omissione o rifiuto di fornire informazioni complete; rifiuto di sottoporsi a un'ispezione; mancato rispetto dei provvedimenti adottati

[64] L'esito procedimentale può anche condurre a ritenere le condizioni di cui all'art. 73, par. 1 non soddisfatte, e in tal caso il par. 5 della medesima disposizione precisa che la Commissione dovrà chiudere l'indagine per mezzo di una decisione che si applica con effetto immediato.

dalla Commissione a norma dell'art. 72 DSA; mancato rispetto delle condizioni di accesso al fascicolo della Commissione *ex* art. 79, par. 4, DSA (art. 74, par. 2, DSA). Anche l'adozione di una decisione a norma del par. 2 appena descritto deve essere preceduta dalla comunicazione ai soggetti interessati[65] da parte della Commissione delle proprie constatazioni preliminari.

Quanto ai criteri di determinazione dell'importo della sanzione pecuniaria, deve tenersi conto della natura, della gravità, della durata e della reiterazione della violazione e, per le menzionate sanzioni di cui al par. 2 dell'art. 74 DSA, del ritardo causato al procedimento.

In linea generale, rispetto all'impianto complessivo, non può però farsi a meno di osservare come la proporzionalità della comminatoria astratta risulti alquanto sacrificata, avendo il legislatore accomunato sotto un unico 'macro *range*' edittale fatti dal disvalore anche assai diverso – *sub lett. a*), sostanzialmente qualsiasi violazione del Regolamento – che, forse, più opportunamente si sarebbe potuto differenziare mediante cornici sanzionatorie autonome – ciò che avrebbe contribuito a rendere maggiormente prevedibile l'esito concreto dell'esercizio della potestà sanzionatoria da parte della Commissione.

Va poi segnalata la peculiare procedura di *vigilanza rafforzata* (*enhanced supervision*) da parte della Commissione sull'*enforcement* degli obblighi di cui al Capo III, sezione 5 (art. 75 DSA).

Nell'adottare una decisione di *non-compliance* che attenga, nella specie, alla violazione, da parte di una *VLOP* o di un *VLOSE*, di uno di tali obblighi, la Commissione chiede al soggetto in questione «di elaborare e comunicare, entro un termine ragionevole specificato nella decisione, ai coordinatori dei servizi digitali, alla Commissione e al comitato un piano d'azione che stabilisca le misure necessarie, sufficienti per porre fine alla violazione o porvi rimedio». La norma chiarisce che le misure possono consistere nell'impegno a effettuare una revisione indipendente secondo quanto previsto dall'art. 37 DSA – dovendosi specificare l'identità dei revisori, la metodologia, la tempistica e il seguito da dare alla revisione – e a partecipare a un codice di condotta pertinente, ai sensi dell'art. 45 DSA.



L'*action plan* viene sottoposto dapprima al vaglio del Comitato, che entro un mese dal ricevimento deve trasmettere il proprio parere alla Commissione, la quale successivamente, entro un termine analogo, decide se le misure stabilite nel piano siano sufficienti – in ciò tenendo in conto l'eventuale impegno della *large platform* ad aderire ai codici di condotta pertinenti – fissando un termine ragionevole per la relativa attuazione. La Commissione deve, a seguire, monitorare l'implementazione del piano e a questi fini il fornitore coinvolto deve trasmettere prontamente la relazione di revisione e fornire aggiornamenti in merito alle misure adottate, potendo la Commissione richiedere informazioni supplementari.

Anche nel contesto della vigilanza rafforzata, la Commissione – laddove non riceva il piano d'azione (o gli altri documenti o informazioni sopra indicati), o ritenga di respingere il piano d'azione o lo consideri insufficiente a porre fine o a rimediare alla violazione – può infliggere penalità di mora (art. 76 DSA) e, nei casi previsti, come detto, può rivolgersi al coordinatore dei sevizi digitali del luogo di stabilimento e sollecitare una richiesta di restrizione all'accesso (art. 82, par. 1, DSA).

Più in generale, le penalità di mora ricalcano quelle a disposizione delle autorità nazionali e presidiano altresì gli obblighi di *VLOPs* o *VLOSEs* di fornire informazioni corrette e complete in risposta a una decisione, di sottoporsi a un'ispezione, di conformarsi a una decisione che dispone misure provvisorie, di rispettare gli impegni resi giuridicamente vincolanti da una decisione (art. 76, par. 1, DSA).

[65] Oltre al fornitore della piattaforma *online* o del motore di ricerca *online* di dimensioni molto grandi si menziona anche «un'altra persona» ex art. 67, par. 1, DSA (art. 74, par. 3, DSA).

I poteri conferiti alla Commissione per l'irrogazione di sanzioni pecuniarie o penalità di mora (ex artt. 74 e 76 DSA) sono soggetti a un termine di prescrizione di cinque anni, decorrente dal giorno in cui è stata commessa la violazione (art. 77, par. 1 e par. 2, DSA)[66].

Il Regolamento si premura di prevedere anche una disciplina degli atti interruttivi – elencati in via esemplificativa al par. 3 della disposizione[67] e coincidenti con «[q]ualsiasi azione intrapresa dalla Commissione o dal coordinatore dei servizi digitali ai fini dell'indagine o del procedimento in relazione a una violazione» – nonché casi di sospensione del termine di prescrizione – fin tanto che la decisione della Commissione sia oggetto di un procedimento dinanzi alla Corte di giustizia dell'Unione europea. Sebbene ogni interruzione comporti un nuovo decorso dal principio del termine di prescrizione, è stabilito altresì un termine prescrizionale massimo[68].

Anche il potere della Commissione di procedere all'esecuzione delle sanzioni si prescrive in cinque anni dal giorno in cui la decisione diventa definitiva, prevedendosi pure in questo caso regole in tema di atti interruttivi (art. 78 DSA)[69]

## 7 Rilievi conclusivi

Al termine della disamina condotta sull'assetto di *enforcement* pubblico del DSA è possibile tracciare un primo, essenziale bilancio della disciplina introdotta dal nuovo Regolamento in questo campo.

Si è messo in evidenza come la cifra degli equilibri istituzionali risieda nel sistema 'reticolare' che prevede una vasta cooperazione tra le autorità coinvolte e tra l'ambito nazionale e quello europeo; in dottrina, non si è mancato di porre l'accento su questa caratteristica quale elemento distintivo rispetto ad altri, recenti modelli di regolazione della «trasformazione digitale», a cominciare dal Regolamento 'gemello' *Digital Markets Act* – come noto, parte dello stesso pacchetto con cui è stato introdotto il DSA e in cui si rinviene un più marcato accentramento di poteri in capo alla Commissione – e dall'*AI Act* in corso di approvazione – in cui parrebbe prevalere la dimensione del decentramento[70].



[66] Tuttavia, in caso di violazioni continuate o reiterate, tale termine decorre dal giorno in cui cessa la violazione (così ancora l'art. 77, par. 2, DSA).

[67] Rientrano nel novero degli atti interruttivi, in particolare, le richieste di informazioni da parte della Commissione o di un coordinatore dei servizi digitali, le ispezioni e l'avvio di un procedimento da parte della Commissione a norma dell'art. 66, par. 1, DSA.

[68] *Id est*, il decorso di un tempo pari al doppio del termine di prescrizione senza che la Commissione abbia irrogato una sanzione pecuniaria o una penalità di mora, eventualmente prolungato della durata della menzionata sospensione: cfr. art. 77, par. 4 e par. 5, DSA.

[69] L'art. 78, par. 3, DSA stabilisce che il termine di prescrizione per l'esecuzione delle sanzioni è interrotto: «a) dalla notifica di una decisione che modifica l'importo iniziale della sanzione pecuniaria o della penalità di mora, oppure respinge una domanda intesa ad ottenere una tale modifica; b) da qualsiasi azione della Commissione, o di uno Stato membro che agisca su richiesta della Commissione, volta a dare esecuzione al pagamento della sanzione pecuniaria o della penalità di mora». Ogni interruzione fa decorrere nuovamente il termine di prescrizione dal principio.

[70] Questa la lettura di L. Torchia, *I poteri di vigilanza*, cit., 1106 ss. e 1110 ss.

Questa dinamica di collaborazione e la scelta di fare assegnamento sul ruolo di vari attori si espone, secondo talune letture, a possibili criticità sia dalla prospettiva delle autorità nazionali, sia da quella della Commissione europea.

Con riguardo ai coordinatori dei servizi digitali, si è già anticipato come una delle questioni chiave dell'intera attività di implementazione del DSA dipenderà da come gli Stati membri interpreteranno la designazione di tali soggetti. Anzitutto sul piano domestico, inevitabilmente si richiederà la cooperazione tra il coordinatore e le altre autorità nazionali che potrebbero avere voce in capitolo su questioni specifiche, come in materia di protezione dei dati, concorrenza, telecomunicazioni etc.[71]

In ottica multilivello, poi, nelle dinamiche di pesi e contrappesi che, come visto, sostengono i 'rapporti di forza' tra Stati membri e Commissione, «i limiti intrinseci» alla strategia di individuazione dell'autorità nazionale competente basata sul luogo di stabilimento delle piattaforme – sulla scia dei problemi sperimentati con il GDPR, dato che la gran parte di queste ultime ha sede in pochissimi Stati membri – potranno comportare molteplici rischi: dalla erosione delle prerogative degli altri coordinatori statali, al «sovraccarico» per le amministrazioni nazionali interessate che potrebbero non essere in grado di svolgere in modo rapido ed efficace l'attività di vigilanza, sino al consequenziale esito di un rafforzamento del ruolo di 'supplenza' della Commissione europea nei casi di stasi[72].

Inoltre, la normativa sottolinea, tra i requisiti delle autorità nazionali, quello dell'indipendenza: la circostanza che siano previsti casi di competenza concorrente ed esclusiva della Commissione solleva, secondo alcuni – trattandosi di una istituzione che ha il monopolio dell'iniziativa legislativa –, esattamente la questione della sua indipendenza e capacità di non subire, quale *enforcer* del DSA, condizionamenti legati alla propria agenda e ai propri obiettivi politici in ambiti correlati al Regolamento[73].



Sul piano dei risvolti dei poteri di cui alla normativa, infine, l'insieme delle previsioni prese in esame restituisce l'immagine di un sistema finalizzato in via principale alla tutela dell'utente che – contemperando l'afflittività di alcune delle misure introdotte con la costruzione di un apparato di garanzie – replica nel contesto dei servizi digitali l'approccio adottato in altri settori: nell'ottica di una massimizzazione del grado di effettività del DSA, merita attenzione la previsione, specialmente in capo alle grandi *corporation*, di puntuali obblighi di *compliance* autonomamente sanzionati, sulla falsariga di quanto già accaduto, nel contesto regolatorio europeo, ancora una volta in tema di *privacy* – o, ad attestare che si tratta di un *trend* trasversale in diversi ambiti – in materia di sostenibilità[74].

[71] F. G'Sell, *The Digital Services Act*, cit., 106.

[72] V. in questo senso le riflessioni di G. Buttarelli, *La regolazione delle piattaforme digitali,* cit., 123.

[73] I. Buri, *A Regulator Caught Between Conflicting Policy Objectives*, cit., specie 79 s.

[74] Si veda la strada imboccata, in particolare, con la proposta di Direttiva del Parlamento europeo e del Consiglio relativa al dovere di diligenza delle imprese ai fini della sostenibilità e che modifica la direttiva (UE) 2019/1937. Sul tema degli obblighi di *compliance*, v. da ultimo A. Gullo, *Compliance*, in *Arch. pen. web*, 2022, 2, 8 ss.

# Aggiornamento delle indicazioni di *policy*

In linea con i precedenti due cicli della ricerca, sono qui pubblicate le indicazioni di *policy* finali che raccolgono i vari spunti e le diverse indicazioni delle sezioni della ricerca. Occorre evidenziare, come necessaria premessa metodologica, che in considerazione del significativo mutamento del quadro normativo e istituzionale di riferimento, segnato dalla definitiva approvazione del DSA, diverse indicazioni di *policy* – specie quelle rivolte, nei precedenti cicli di indagine, ai decisori pubblici – sono state eliminate o riformulate *ex novo* in quanto non più in linea con il rinnovato panorama regolamentare (per cui, ad es., è ormai da escludersi che i singoli Stati membri possano intervenire in materie dettagliatamente disciplinate dal regolamento europeo). In conformità agli scopi e all'ambito tematico di riferimento di questa ricerca, e in continuità con i primi due cicli dello studio, va infine chiarito che tali indicazioni di *policy* sono state formulate avuto specifico riguardo al contrasto alle operazioni di disinformazione, considerando, pertanto, i principali adempimenti in tal senso pertinenti imposti dal *Digital Services Act* e dalle altre norme applicabili.



**Indicazioni di *policy* per piattaforme e motori di ricerca online**

| n° | Descrizione |
|---|---|
| IP-01 | **Nomina di *compliance officer* (ove applicabile *ex* art. 41 DSA)** - Nominare uno o più responsabili di *compliance* per la gestione dei rischi legati alla disinformazione, attribuendo tra l'altro a tale funzione il potere di sovraintendere a tutti gli adempimenti connessi alla DSA *compliance*, nonché poteri di impulso e verifica con particolare riguardo alle correlate azioni di *risk-assessment* e *risk-management*. È opportuno valutare l'istituzione di tale figura anche nelle organizzazioni che non rientrano nel raggio applicativo dell'art. 41 DSA e in conformità ai criteri ivi rinvenibili. |

| | |
|---|---|
| **IP-02** | **Procedure di valutazione dei rischi (ove applicabile *ex* art. 34 DSA)** - Predisporre idonee procedure di valutazione dei rischi legati alla diffusione di informazioni false, analizzando su base almeno annuale gli ambiti tematici (es. categorie, *hashtag*, profili) più esposti e prevedendo in relazione ad essi adeguate misure di contenimento del rischio in base al livello di rischio misurato. Le procedure dovranno considerare in particolare i rischi legati alla diffusione di notizie false atte a turbare l'ordine pubblico, la sicurezza e la salute pubblica, il dibattito democratico su temi di preminente interesse pubblico. Le piattaforme online e i motori di ricerca di grandi dimensioni dovranno altresì valutare eventuali rischi sistemici derivanti dall'erogazione dei propri servizi e assicurare il rispetto dei principi sanciti dall'art. 34 del DSA. È opportuno che anche le organizzazioni non soggette all'applicazione obbligatoria di quest'ultima previsione svolgano simili attività e applichino anche su base volontaria, pur tenendo conto delle proprie specificità operative, i principi sanciti da tale previsione del regolamento. |
| **IP-03** | **Attuazione e monitoraggio di misure di attenuazione dei rischi** - Predisporre idonee misure per attenuare i rischi identificati ai sensi della procedura di valutazione di cui all'IP-02 e costruire e implementare procedure per verificare l'effettiva attuazione delle misure di contenimento dei rischi in parola, assicurandone il miglioramento continuo. Le piattaforme dovrebbero coordinare le *policies* di contrasto alla disinformazione con i sistemi di gestione interni e con le procedure di controllo della qualità dei servizi resi e della sicurezza delle informazioni. Le piattaforme online e i motori di ricerca di grandi dimensioni dovranno conformarsi agli obblighi sanciti dall'art. 35 del DSA. È opportuno che anche le organizzazioni non soggette all'applicazione obbligatoria di quest'ultima previsione svolgano simili attività e applichino anche su base volontaria, pur tenendo conto delle proprie specificità operative, i principi sanciti da tale previsione del regolamento. |
| **IP-04** | **Audit interni e revisioni esterne indipendenti (ove applicabile *ex* art. 37 DSA)** - Prevedere su base almeno annuale lo svolgimento di *audit* interni, sotto la supervisione dei responsabili indicati nella IP-01, volti a valutare la conformità delle procedure interne con le fonti di *soft law* (codici etici e di condotta, linee guida, indicazioni di *policies* etc.) e con le norme cogenti di legge con particolare riguardo al DSA.<br>Le piattaforme online e i motori di ricerca di grandi dimensioni dovranno conformarsi agli obblighi sanciti dall'art. 37 del DSA, richiedendo una revisione indipendente esterna. È opportuno, ad ogni modo, che anche le organizzazioni non soggette all'applicazione obbligatoria di quest'ultima disposizione valutino l'opportunità di sottoporsi periodicamente a *audit* esterni indipendenti. |
| **IP-05** | **Informativa agli utenti** - Includere nelle condizioni generali del servizio idonee previsioni contrattuali volte a vietare la diffusione di notizie false ove ciò costituisca reato o contenuto illegale ai sensi dell'art. 3, lett. h), del DSA.<br>Predisporre, sui propri applicativi, idonee interfacce affinché l'utente possa agevolmente reperire tali previsioni contrattuali. |

**IP-06** **Sistemi di segnalazione delle informazioni illecite o lesive delle condizioni d'uso del servizio. Provvedimenti conseguenti sui contenuti e denunce all'Autorità. Strumenti e procedure di cooperazione con le Autorità anche in caso di crisi** - Predisporre strumenti e interfacce per consentire agli utenti di segnalare la presenza nel servizio di informazioni illecite o lesive delle condizioni d'uso del servizio. Predisporre procedure interne di esame tempestivo della segnalazione, che assicurino l'immeditata attuazione dei correlati provvedimenti ai sensi del DSA. Prevedere che venga altresì data notizia all'autore del contenuto dei provvedimenti adottati e degli strumenti di reclamo disponibili. Le procedure di segnalazione e l'obbligo di fornire motivazioni sui connessi provvedimenti devono essere svolte dalle piattaforme in conformità a tutti gli obblighi di dettaglio definiti in particolare dagli artt. 16 e 17 del DSA. Predisporre procedure interne, tempestive ed efficaci, per rimuovere contenuti illegali ai sensi dell'art. 9 del DSA, in relazione alla ricezione di ordini delle autorità pubbliche, e per notificare sospetti reati nei limiti di quanto specificamente previsto dall'art. 18 del DSA. Prevedere procedure dettagliate ed efficaci per assicurare una pronta esecuzione degli obblighi connessi all'eventuale attivazione da parte della Commissione europea di un meccanismo di risposta alla crisi *ex* art. 36 del DSA. Valutare altresì la partecipazione ai correlati protocolli di crisi *ex* art. 48 DSA. Assicurare l'accesso ai propri dati ai sensi dell'art. 40 DSA.

**IP-07** **Definizione delle condizioni d'uso del servizio, delle sanzioni disciplinari e dei reclami** - Definire le regole d'utilizzo del servizio nel rispetto dei fondamentali principi di garanzia sanciti dalle Carte europee dei diritti (su tutti, il diritto alla libertà di espressione dell'utente) e in conformità agli obblighi definiti in dettaglio dagli artt. 14 e 15 del DSA. Non prevedere un generale divieto di condivisione di notizie false, ma introdurre, con un approccio caso per caso, divieti ben circoscritti e tassativi di diffondere certi contenuti, nonché relativi – anche a prescindere dal contenuto dell'informazione – a specifiche modalità fraudolente di utilizzo del servizio (ad. es. interazione artificiosa tra più *account*), con riferimento a singoli settori sensibili identificati tramite le attività di cui alla IP-02. Disciplinare le violazioni e le collegate misure di carattere sanzionatorio/interdittivo – dalla etichettatura o rimozione del contenuto, al blocco temporaneo al servizio, fino alla sospensione temporanea o permanente dell'*account* – nel rispetto, oltre che dei principi sanciti dal DSA e in particolare dall'art. 14, delle correlate minimali garanzie *sostanziali e procedurali,* tra cui, ad es.: 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, 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. Assicurare un elevato livello di trasparenza e dettaglio nel rendere pubbliche le modalità di funzionamento e le specifiche fasi delle procedure interne di applicazione delle misure sanzionatorie/inibitorie e per la gestione dei reclami da parte degli utenti, nel rispetto di minimali diritti procedurali, specie per ciò che concerne il diritto al contraddittorio preventivo e la garanzia di 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, etc. Per le piattaforme online e i motori di ricerca occorre altresì conformarsi agli obblighi sanciti dagli artt. 20, 21 e 22 del DSA. È opportuno che anche gli operatori non soggetti all'applicazione di queste ultime previsioni predispongano sistemi interni di reclamo e meccanismi di cooperazione con segnatori attendibili in conformità alle previsioni in parola e ai principi generali di cui alla presente indicazione di *policy*.

| | |
|---|---|
| **IP-07-*bis*** | **Misure specifiche a garanzia del pluralismo dell'informazione nella definizione delle condizioni d'uso del servizio** – Prevedere misure specifiche e puntuali, nella definizione delle condizioni d'uso del servizio, a tutela del pluralismo dell'informazione e della garanzia per tutti i media della possibilità di poter accedere e condividere i propri contenuti in piattaforma in condizioni di piena ed effettiva parità. Prevedere delle garanzie rafforzate per quanto attiene alle attività di moderazione dei contenuti immessi da tali operatori dell'informazione, nel rispetto della cornice generale delle misure a protezione dei diritti degli utenti definite ai sensi della IP-07. |
| **IP-08** | **Pubblicità online** – Istituire un registro di informazioni chiare, corrette e trasparenti in merito all'identità o a caratteristiche di terzi che sponsorizzano propri prodotti o servizi sulla piattaforma. Imporre ai professionisti (es. agenzie di *marketing*, intermediari etc.) che si avvalgono dei servizi di pubblicità intra-piattaforma di indicare il nominativo del cliente e/o il titolare effettivo dell'annuncio che sarà mostrato sulla piattaforma. Prevedere procedure di controllo, anche a campione, sulle pubblicità mostrate dalla piattaforma in ambiti ritenuti a rischio ai sensi della IP-02. Annotare nel registro anche il periodo durante il quale è stata presentata la pubblicità e il novero di soggetti a cui era rivolto, nonché i parametri utilizzati per individuare i destinatari. Assicurare, nel predisporre tali procedure, il rispetto delle previsioni di cui all'art. 39 del DSA. |
| **IP-09** | **Verifiche sugli operatori business** – Prevedere procedure di controllo, anche a campione, sui contenuti diffusi da operatori *business* (es. profili *social* di grandi imprese, istituzioni, ONG, profili di persone politicamente esposte) attivi in ambiti ritenuti a rischio ai sensi della IP-02. Assicurare che le segnalazioni relative a tali operatori siano trattate in via prioritaria rispetto alle altre segnalazioni. Sottoporre a tali operatori una informativa sulle procedure, le misure e gli strumenti applicabili alle condotte di disinformazione sulla piattaforma, in modo da ottenere una presa d'atto per accettazione. Prevedere procedure di tracciabilità degli operatori *business*. Qualora tali operatori intendano pubblicizzare o offrire prodotti o servizi, la piattaforma dovrà previamente acquisire (*ex* art. 30 DSA, ove applicabile) i dati identificativi dell'impresa (es. denominazione, estremi dell'iscrizione nel registro delle imprese, dettagli relativi al conto di pagamento), oltre a un'autocertificazione relativa alla conformità dei prodotti o servizi offerti alle norme dell'Unione. |
| **IP-10** | **Codici di condotta** – Adottare strumenti di regolazione flessibile e *best practices* per il contenimento dei rischi legati alla disinformazione, aderendo se del caso a codici di condotta già esistenti elaborati da enti o istituzioni qualificate. Prevedere, con riferimento a tali strumenti, procedure e controlli particolari in contesti e periodi temporali particolarmente esposti al rischio di disinformazione (es, periodi precedenti alle elezioni politiche, contesti emergenziali).<br>Verificare periodicamente l'avvenuta adozione *ex* art. 45 DSA di codici di condotta a cui la piattaforma possa aderire. |

| | |
|---|---|
| **IP-11** | **Algoritmi di raccomandazione** – Svolgere controlli periodici ed effettuare *algorithm auditing* sui parametri utilizzati dai sistemi di raccomandazione dei contenuti presenti sulla piattaforma, con particolare riguardo agli ambiti tematici a rischio di disinformazione ai sensi della IP-02. Prevedere misure atte a prevenire che un contenuto afferente a tali ambiti (specie contenente informazioni false costituenti contenuto illegale o la cui condivisione sia vietata dalle condizioni d'uso del servizio definite nel rispetto dei principi di cui alla IP-07) possa essere "consigliato" dagli algoritmi di raccomandazione, diventando così "virale" nel web, senza che detti algoritmi siano stati sottoposti a controllo o validazione, anche in osservanza degli standard internazionali applicabili. Specificare nelle condizioni generali *ex* art. 27 o 38 DSA (ove applicabili) i principali parametri utilizzati dagli algoritmi di raccomandazione, nonché qualunque opzione che consenta all'utente di modificare tali parametri. Assicurare almeno un'opzione non basata sulla profilazione. |
| **IP-12** | **Report periodici** – Pubblicare almeno una volta all'anno *ex* art. 15 DSA un report sulle attività di moderazione dei contenuti, che includa tutti i dettagli previsti da tale disposizione. Tale relazione dovrà essere altresì redatta in conformità all'art. 42 DSA per quanto riguarda piattaforme online e motori di ricerca di dimensioni molto grandi. |
| **IP-12-*bis*** | **Conservazione dei contenuti rimossi e della documentazione connessa a ogni misura di moderazione dei contenuti degli utenti che sia stata adottata** – Conservare, in appositi archivi online, i contenuti rimossi e la documentazione connessa a ogni misura adottata all'esito dell'attività di moderazione dei contenuti degli utenti svolta ai sensi e nel rispetto delle indicazioni della IP-07 e della IP-07-*bis* e prevedere la conservazione dei documenti relativi all'istruttoria svolta in modo da garantire la possibilità di ricostruire con chiarezza il percorso decisionale sfociato nella decisione di rimuovere il contenuto illecito o lesivo delle condizioni d'uso del servizio o di adottare qualsiasi altra misura in relazione allo stesso. |



### Indicazioni di *policy* per operatori e imprese non destinatari degli obblighi definiti dal DSA

| n° | Descrizione |
|---|---|
| **IP-13** | **Valutazione dei rischi** – Effettuare con cadenza almeno annuale la valutazione dei rischi legati alla diffusione di informazioni false sui canali *social* e sulle piattaforme utilizzate dall'impresa o dall'operatore. Analizzare in particolare gli ambiti di attività (es. linee di *business*, tipologie di prodotti etc.) particolarmente esposti al rischio di disinformazione e prevedere in relazione ad essi adeguate misure di contenimento del rischio in base alle risorse disponibili e al livello di rischio misurato. Le procedure dovranno considerare in particolare i rischi legati alla diffusione di notizie false atte a turbare l'ordine pubblico, la sicurezza pubblica, il dibattito democratico su temi di preminente interesse pubblico. |

| | |
|---|---|
| **IP-14** | **Gestione dei profili business** – Predisporre adeguate procedure organizzative e di controllo per l'utilizzo delle utenze e dei profili registrati su piattaforme online, prevedendo in particolare che i privilegi di amministratore della pagina e le credenziali di accesso siano attribuiti a soggetti all'uopo designati, sottoposti alla vigilanza di organi e funzioni di controllo. |
| **IP-15** | **Controllo sui contenuti** – Predisporre adeguate procedure di controllo da parte di responsabili aziendali prima della pubblicazione di notizie (es. *post*, messaggi, articoli) su piattaforme online. Prevedere la necessità di una autorizzazione preventiva per la pubblicazione di contenuti ritenuti particolarmente sensibili in base agli esiti della valutazione dei rischi. |
| **IP-16** | **Meccanismi di segnalazione degli *user-generated contents*** – Prevedere procedure di controllo sui contenuti diffusi da utenti privati e collegati alla pagina social dell'impresa (o dell'organizzazione) mediante il sistema dei *tag*. Segnalare senza indebito ritardo al gestore della piattaforma notizie non veritiere relative ad ambiti ritenuti a rischio, al fine di consentire l'applicazione dei provvedimenti conseguenti. Tale segnalazione dovrebbe essere effettuata anche nel caso in cui il contenuto diffuso dagli utenti non sia direttamente collegato alla pagina social dell'impresa (o dell'organizzazione), ma quest'ultima ne abbia comunque avuto conoscenza. |
| **IP-17** | **Doveri di diligenza per i professionisti dell'informazione** – Predisporre adeguate procedure di controllo sulla veridicità delle fonti e sul rispetto dei criteri di verità, pertinenza e continenza nell'attività giornalistica e di informazione su aree tematiche ritenute a rischio. Laddove il professionista dell'informazione (es. agenzie di stampa, operatori radio e televisivi, testate telematiche registrate, quotidiani *online*) disponga di una pagina su una piattaforma online, coordinare tali procedure di controllo con quelle previste dalla IP-15.<br>Predisporre adeguate procedure di controllo sul rispetto delle disposizioni contenute in codici etici e di condotta al quale il professionista dell'informazione abbia aderito. |
| **IP-18** | **Codici di condotta** – Adottare strumenti di regolazione flessibile e *best practices* per il contenimento dei rischi legati alla disinformazione, aderendo ove possibile a codici di condotta già esistenti elaborati da enti o istituzioni qualificate. Tale misura dovrebbe essere seguita in particolare dalle organizzazioni che operano come professionisti dell'informazione. |
| **IP-19** | **Controlli sull'attività dei fornitori** – Prevedere procedure di controllo, anche a campione, sulle attività affidate in *outsourcing* a terzi fornitori (es. gestione del profilo social da parte di agenzie di stampa o di *marketing*) in ambiti ritenuti a rischio o ad essi connessi o correlati. |

**Indicazioni di *policy* per istituzioni pubbliche nazionali**

| n° | Descrizione |
|---|---|
| IP-20 | **Costituzione di gruppi di lavoro e *partnership* con gli operatori privati** – In misura compatibile con gli obblighi del DSA, costituire – sotto la supervisione del coordinatore nazionale dei servizi digitali – tavoli di lavoro per la discussione sui temi della disinformazione e per incentivare il dibattito pubblico su questi temi. Diffondere la cultura della "buona informazione" nel rispetto del pluralismo democratico e della libertà di espressione, sensibilizzando i cittadini e gli operatori economici sui rischi legati alla manipolazione dell'informazione. |
| IP-21 | **Analisi nazionale dei rischi legati alla disinformazione** – In conformità al DSA, e sotto la supervisione e l'impulso del coordinatore nazionale dei servizi digitali, intraprendere iniziative, anche attraverso il coordinamento tra pubbliche amministrazioni, per elaborare, su base almeno annuale, un documento riassuntivo dei rischi e delle priorità nazionali per ciò che concerne la lotta alla disinformazione. Il documento contenente l'analisi nazionale dei rischi dovrebbe essere pubblicato e reso facilmente accessibile per tutti gli operatori pubblici e privati. |
| IP-22 | **Attuazione delle modifiche normative necessarie ad assicurare l'efficace applicazione del DSA** – Provvedere alla designazione del coordinatore nazionale dei servizi digitali in conformità al DSA, e assicurare, anche tramite ogni modifica normativa o regolamentare di necessario raccordo, l'implementazione di procedure efficaci per adempiere agli obblighi di cooperazione con la Commissione europea, e altre istituzioni, delineati dal nuovo regolamento europeo, nonché per assicurare il migliore esercizio dei poteri di *enforcement* nazionali ivi disciplinati. Sotto il profilo sanzionatorio, provvedere all'introduzione di sanzioni amministrative per la violazione del nuovo regolamento europeo in conformità ai criteri sanciti dagli artt. 51 e 52 del DSA, disciplinando altresì le regole connesse al correlato procedimento applicativo nel rispetto dei principi di garanzia stabiliti dall'art. 51, par. 6, del DSA (tra l'altro, tutela del diritto di difesa, diritto di essere ascoltati e di accedere al fascicolo, diritto a un ricorso giurisdizionale effettivo). Disciplinare sanzioni amministrative pecuniarie e penalità di mora, nonché eventuali connesse misure provvisorie ai sensi dell'art. 51 del DSA, che siano "effettive, proporzionate e dissuasive" nel senso richiesto dal già menzionato art. 52, par. 1, del DSA, e in linea con i limiti massimi edittali sanciti dai parr. 3 e 4 della stessa previsione. |