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

Antonio Gullo

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

* Il presente report costituisce la sezione giuridica del terzo ciclo della ricerca dal titolo "Come individuare e contrastare operazioni coordinate di disinformazione in Italia. Casi di studio e indicazioni di policy per istituzioni pubbliche e private", condotta nell'A.A. 2022/2023 da ricercatori dell'Università Luiss Guido Carli, della Harvard Kennedy School e della School of Information dell'Università del Michigan. La ricerca è stata realizzata con un contributo dell'Unità di Analisi, Programmazione e Documentazione Storica del Ministero italiano degli Affari Esteri e della Cooperazione Internazionale (MAECI), ai sensi dell'art. 23-*bis* del d.p.r. n. 18 del 5 gennaio 1967. Le riflessioni contenute in questa ricerca riflettono esclusivamente la visione degli autori e non sono necessariamente rappresentative dell'opinione del MAECI e delle altre istituzioni coinvolte. Si ringraziano l'Unità di Analisi, Programmazione e Documentazione Storica del MAECI e gli altri Direttori della ricerca (Irene Pasquetto, Gianni Riotta e Costanza Sciubba Caniglia) per avere consentito la pubblicazione degli scritti in questa sede.

[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 *Diritto penale contemporaneo – Rivista trimestrale*, 4, 2021, 248 ss. Il report del secondo ciclo di studi è invece reperibile online in *esteri.it*.

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.

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 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 arene 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 adempimen-

[2] L. D'Agostino, *Disinformazione e obblighi di* compliance *degli operatori del mercato digitale alla luce del nuovo* Digital Services Act*,* in questa medesima sezione monografica, in *questa Rivista,* 2, 2023.

[3] 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,* in questa medesima sezione monografica, in *questa Rivista,* 2, 2023.

ti a strati progressivi, in cui 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.

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,* in questa medesima sezione monografica, in *questa Rivista,* 2, 2023.