

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

Rossella Sabia

Abstract

Il contributo offre una panoramica sui caratteri di fondo del regolamento (UE) 2022/2065 (*Digital Services Act* – DSA) con riguardo all'architettura dei poteri di *enforcement* sul versante pubblico e del riparto di competenze tra livello nazionale ed europeo (Capo IV, dedicato all'attuazione, alla cooperazione, alle sanzioni e all'esecuzione del DSA). Si tratta di un ambito di sicuro interesse per il penalista, intercettando la questione dello spazio riservato – nella tutela sia dei diritti degli utenti di servizi digitali, sia delle funzioni delle autorità coinvolte – alla risposta sanzionatoria che – pur non ricorrendosi qui al diritto criminale – presenta non trascurabili connotati di afflittività. Il lavoro muove dal contesto nazionale, con riferimento alla figura del coordinatore dei servizi digitali; esamina il ruolo da protagonista della Commissione europea nei rapporti con le piattaforme di dimensioni molto grandi; discute il 'livello intermedio' costituito dal Comitato europeo per i servizi digitali, restituendo chiara la dimensione collaborativa e la struttura 'a rete' della *governance* tratteggiata dal Regolamento.

This article aims at outlining the main features of the Regulation (EU) 2022/2065 (*Digital Services Act* – DSA) with regard to the architecture of the public enforcement and the distribution of competences between national and EU levels (Chapter IV, dedicated to the implementation, cooperation, penalties and enforcement of the DSA).

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

This is an interesting area for criminal law scholars, as it involves the question of the role of penalties in the DSA – for the protection of both the rights of users of digital services and the functions of the authorities involved –; although not criminal in nature, they show a certain degree of severity. The contribution starts from the national context, with reference to digital services coordinators; it examines the leading role of the European Commission in relation with very large online platforms; it discusses the “intermediate level” represented by the European board for Digital Services, thus highlighting the collaborative dimension and the “network” structure of the governance outlined by the Regulation.

Sommario

1. L'*enforcement* pubblico del DSA: un inquadramento generale. – 2. La distribuzione dei poteri di *enforcement* tra la Commissione europea e gli Stati membri. – 3. Il livello nazionale. I coordinatori dei servizi digitali degli Stati membri: uno sguardo d'insieme. – 3.1. (*Segue*). I poteri sanzionatori degli Stati membri e gli strumenti di tutela dei destinatari del servizio. – 4. La disciplina in tema di assistenza reciproca con la Commissione europea e cooperazione transfrontaliera dei coordinatori nazionali. – 5. Il raccordo istituzionale tra Stati membri e Commissione europea: il Comitato europeo per i servizi digitali. – 6. I poteri di *enforcement* della Commissione europea: un “interlocutore privilegiato” dei più grandi *player* del mercato digitale. – 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*». – 7. Rilievi conclusivi.

Keywords

Digital Services Act – *Public enforcement* – Coordinatori dei servizi digitali – Commissione europea – Sanzioni

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: appron-

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. Nel contesto italiano, v. i diversi contributi pubblicati nel fascicolo n. 1/2023 di *Diritto di internet*, oltre alla circolare Assonime n. 17/2023 “Mercato Unico dei servizi digitali: il Digital Services Act” del 12 giugno 2023.

Sezione monografica - Il *Digital Services Act* e il contrasto alla disinformazione: responsabilità dei *provider*, obblighi di *compliance* e modelli di *enforcement*

tare 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 scala².

Tale intervento si iscrive nell'ambito della strategia dell'Unione europea³ 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 interno⁴.

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*⁵ – 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 utenti⁶. Sul punto, occorre ricordare che si tratta di doveri asimmetrici⁷, 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 platform*» – ossia quelle aventi un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a quarantacinque milioni e designate come tali dalla Commissione europea⁸ – a stabilire regole *ad hoc* nel Capo III, sezione 5 del DSA, su cui vigila in via esclusiva, come si vedrà, la Commissione europea⁹.

Questa opzione di *policy* muove dalla presa d'atto dell'insufficienza delle sole misure

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*, 4(1), 2022, 53, i quali definiscono appunto il DSA «*the biggest shake up to the rules for online intermediary liability in twenty years*». Per una analisi del regolamento con un focus sul suo impatto etico-sociale, si rinvia a A. Turillazzi - M. Taddeo - L. Floridi - F. Casolari, *The Digital Services Act: An Analysis of its Ethical, Legal, and Social Implications*, in *Law, Innovation and Technology*, 15, 2023, 83 ss.

³ Per un ampio inquadramento del ruolo dell'Unione europea nello scenario globale sul versante digitale, v. E. Fahey, *The EU as a Global Digital Actor. Institutionalising Global Data Protection, Trade, and Cybersecurity*, Oxford, 2022; A. Manganelli - A. Nicita, *Regulating Digital Markets. The European Approach*, Cham, 2022. Nella prospettiva di un raffronto tra il DSA e l'esperienza statunitense v. D. C. Nunziato, *The Digital Services Act and the Brussels Effect on Platform Content Moderation*, in *Chicago Journal of International Law*, 24(1), 2023, 115 ss.

⁴ G. Buttarelli, *La regolazione delle piattaforme digitali: il ruolo delle istituzioni pubbliche*, in *Giornale di diritto amministrativo*, 1, 2023, 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.

⁵ 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.

⁶ 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*, in questa medesima sezione monografica, in questa *Rivista*, 2, 2023.

⁷ 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.

⁸ V. 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*, cit., par. 4.

⁹ *Infra*, par. 6 e 6.1.

di autoregolazione da parte delle piattaforme per limitare la diffusione di *illegal 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 «i tratti tipici di un ordinamento giuridico, autonomo dall'ordinamento generale»¹⁰.

Il DSA denota 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 – come detto, *freedom of speech in primis*¹¹ – e fissando i criteri di riferimento delle scelte di *self-policing* e dei poteri *lato sensu* “sanzionatori” delle piattaforme¹².

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 – i c.d. servizi di intermediazione¹³ – cui il DSA impone una serie di obblighi (si è parlato di «*layer cake*»)¹⁴ stratificati dal basso verso l'alto, *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 inferiori¹⁵. 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

¹⁰ L. Torchia, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in *Rivista trimestrale di diritto pubblico*, 4, 2022, 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 *Diritto penale contemporaneo – Rivista Trimestrale*, 4, 2021, 304 ss.

¹¹ Per alcune notazioni critiche sull'approccio europeo al tema, v. V. Zeno-Zencovich, *The EU Regulation of Speech. A Critical View*, in questa *Rivista*, 1, 2023, 11 ss.

¹² V. sul punto 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*, cit.

¹³ 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).

¹⁴ F. G'sell, *The Digital Services Act*, cit., 89.

¹⁵ Cfr. L. D'Agostino, *Disinformazione e obblighi di compliance degli operatori del mercato digitale alla luce del nuovo Digital Services Act*, cit., par. 1 ed 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*, cit., par. 1.

Sezione monografica - Il *Digital Services Act* e il contrasto alla disinformazione: responsabilità dei *provider*, obblighi di *compliance* e modelli di *enforcement*

funzione di *compliance* dedicata¹⁶, con lo scopo 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 armonizzato¹⁷.

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 della 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 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, poi, 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 di-

¹⁶ Su cui, in dettaglio, v. 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*, cit., par. 4.

¹⁷ L. Torchia, *I poteri di vigilanza*, cit., 1111.

gitali¹⁸ –, sia la Commissione europea.

Nel quadro di una «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 dirà¹⁹ – e gli ambiti di intervento 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)²⁰ 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*)²¹.

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, ad esempio, nel contesto del GDPR²² – 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 Paese²³ –, sul presupposto di una maggior “resilienza” della Commissione alle dinamiche di *regulatory capture*²⁴.

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 DSA²⁵ – o in quella della Commissione, sulla base delle regole

¹⁸ *Infra* par. 3.

¹⁹ Il riparto di competenze tra Stati membri e Commissione è infatti ulteriormente precisato ai par. 2, 3 e 4 dell'art. 56 DSA.

²⁰ 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 *Diritto di internet*, 1, 2023, 27 ss.

²¹ Per le relative definizioni, v. *supra*, nt. 13.

²² 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 *irishtimes.com*, 13 settembre 2021.

²³ F. G'sell, *The Digital Services Act*, cit., 106.

²⁴ 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.

²⁵ 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».

Sezione monografica - Il *Digital Services Act* e il contrasto alla disinformazione: responsabilità dei *provider*, obblighi di *compliance* e modelli di *enforcement*

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 regolamento, come chiarito dall'art. 56, par. 7, DSA. Per evitare sovrapposizioni e il rischio di duplicazioni procedurali 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 avviati²⁶ – parrebbe scongiurare potenziali casi di *bis in idem*²⁷.

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 ambiti²⁸.

Per evitare il rischio di una frammentazione dei compiti²⁹, si prevede in ogni caso che sia il coordinatore dei servizi digitali ad assicurare l'efficace e coerente applicazione del DSA e a occuparsi, appunto, del coordinamento tra le eventuali autorità domestiche competenti. È dunque plausibile (e anzi, secondo alcuni commentatori, preferibile)³⁰ 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

²⁶ V. in particolare *infra* nei paragrafi che seguono.

²⁷ In senso analogo I. Castellucci - F. Coppola, *Il sistema sanzionatorio decentrato del DSA: dinamica dell'apparato istituzionale*, in *Diritto di internet*, 1, 2023, 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 *Diritto penale e processo*, 3, 2023, 377.

²⁸ Sottolineano questo aspetto M. Husovec - I. Roche Laguna, *Digital Services Act: A Short Primer*, in *ssrn.com*, 2. Il contributo è in corso di pubblicazione in M. Husovec - I. Roche Laguna, *Principles of the Digital Services Act*, Oxford, 2023.

²⁹ Come osservato da L. Torchia, *I poteri di vigilanza*, cit., 1109.

³⁰ E. M. Tripodi, *Le Autorità competenti, i Coordinatori nazionali dei servizi digitali e il Comitato europeo per i servizi digitali. Brevi note*, in *Diritto di internet*, 1, 2023, 62.

protezione dei dati personali –, dando luogo a una sorta di «competizione» per l’attribuzione del ruolo di coordinatore³¹.

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 membro³².

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)³³. Si richiede che tutte le predette misure adottate dai coordinatori nell’esercizio di tali poteri siano – secondo la consueta formula – effettive, dissuasive e proporzionate³⁴, 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 poteri d’indagine *sub* lett. *a*) e lett. *b*) possono, peraltro, attingere anche *altre perso-*

³¹ Così G. Buttarelli, *La regolazione delle piattaforme digitali*, cit., 123. Per l’Italia la scelta è infine ricaduta sull’Autorità per le garanzie nelle comunicazioni (AGCOM), che è stata di recente designata quale coordinatore dei servizi digitali ai sensi dell’art. 15, d.l. 15 settembre 2023, n. 123. Si prevede, peraltro, che l’Autorità garante della concorrenza e del mercato, il Garante per la protezione dei dati personali e «ogni altra Autorità nazionale competente» assicurino la propria collaborazione, i cui aspetti applicativi e procedurali potranno essere disciplinati mediante protocolli di intesa.

³² Con le precisazioni di cui subito si dirà rispetto anche ad altri soggetti che possono essere attinti dall’esercizio dei poteri in discorso.

³³ Si prevede che poteri di cui ai par. 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).

³⁴ Sulle tecniche di recepimento di tale clausola nel diritto interno v., per tutti, A. Gullo, *Deflazione e obblighi di penalizzazione di fonte UE*, in *Diritto penale contemporaneo*, 10 febbraio 2016.

Sezione monografica - Il *Digital Services Act* e il contrasto alla disinformazione: responsabilità dei *provider*, obblighi di *compliance* e modelli di *enforcement*

ne 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.* 37³⁵ e 75, par. 2 (nell'ambito della vigilanza rafforzata)³⁶ 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 vincolanti³⁷ (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 giudiziaria 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 piuttosto, attraverso l'impiego della tecnica ingiunzionale³⁸, 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

³⁵ V. al riguardo 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*, cit., par. 4.4.

³⁶ *Infra* par. 6.1.

³⁷ Sul medesimo tema nel contesto dell'attività della Commissione v. *infra*, par. 6.1.

³⁸ Su tale tecnica sanzionatoria v. già C. Pedrazzi, *Odierna esigenza economiche e nuove fattispecie penali*, in *Rivista italiana di diritto e procedura penale*, 4, 1975, 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.

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.

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 al giudice la possibilità 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

Sezione monografica - Il *Digital Services Act* e il contrasto alla disinformazione: responsabilità dei *provider*, obblighi di *compliance* e modelli di *enforcement*

numero massimo di rinnovi, che spetterà alla stessa autorità giudiziaria stabilire³⁹.

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 sulla *natura* delle sanzioni – dovendosi in ogni caso ritenere che si tratti di sanzioni amministrative⁴⁰ – 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

³⁹ V. le argomentazioni di I. Castellucci - F. Coppola, *Il sistema sanzionatorio decentrato del DSA*, cit., 54.

⁴⁰ Per rimanere nel campo dei regolamenti, cfr. art. 83 GDPR, dove si parla espressamente di sanzioni *amministrative* pecuniarie (corsivo aggiunto). Con riferimento all'ordinamento italiano, v. ora quanto previsto dall'art. 15, co. 4, lett. b), d.l. 123/2023, ove si chiarisce che l'Autorità, nell'esercizio dei poteri di cui al combinato disposto degli artt. 51 e 52 DSA, irroga «in base a principi di proporzionalità, adeguatezza e rispetto del contraddittorio, secondo le procedure stabilite con proprio regolamento, sanzioni amministrative pecuniarie», richiamandosi la l. 689/1981 per escludere l'applicabilità del beneficio del pagamento in misura ridotta ivi previsto all'art. 16.

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 rappresenta un criterio alternativo⁴¹.

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 indagine⁴² – 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»⁴³ 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)⁴⁴.

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*»⁴⁵, 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,

⁴¹ 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. Una puntuale analisi, in chiave critica, della tecnica adoperata dal legislatore europeo per la comminatoria delle sanzioni nel GDPR e delle correlate scelte operate, sul punto, in ambito domestico, è svolta da L. D'Agostino, *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101*, in *Archivio penale web*, 1, 2019, 21 s.

⁴² *Supra*, par. 3.

⁴³ V. in argomento A.M. Felicetti, *La risoluzione extragiudiziale delle dispute nei mercati digitali: alcune novità dall'Europa*, in *Rivista trimestrale di diritto e procedura civile*, 1, 2023, 197 ss.

⁴⁴ Su tali previsioni, si rinvia a 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*, cit. (parr. 3.1 e 3.2).

⁴⁵ 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.

Sezione monografica - Il *Digital Services Act* e il contrasto alla disinformazione: responsabilità dei *provider*, obblighi di *compliance* e modelli di *enforcement*

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.

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 è parlato⁴⁶ – 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, presen-

⁴⁶ *Supra*, par. 2.

tando, 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 nel 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)⁴⁷. 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, richiedendo al coordinatore dei servizi digitali del luogo di stabilimento di riesaminare il caso⁴⁸.

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

⁴⁷ 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.

⁴⁸ 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.

Sezione monografica - Il *Digital Services Act* e il contrasto alla disinformazione: responsabilità dei *provider*, obblighi di *compliance* e modelli di *enforcement*

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 Comitato⁴⁹.

A garanzia della certezza dei tempi procedurali 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.

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 digitali⁵⁰, soggetto in qualche misura “intermedio” tra il livello nazionale – rappresentato dalle autorità competenti con il ruolo chiave, come illustrato, assegnato ai 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*⁵¹.

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, 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

⁴⁹ 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 abbia omissis di avviare prontamente l'indagine congiunta a seguito di raccomandazione del Comitato.

⁵⁰ Sul tema v. E. M. Tripodi, *Le Autorità competenti*, cit., 63 ss.

⁵¹ Cfr. G. Buttarelli, *La regolazione delle piattaforme digitali*, cit., 123.

i coordinatori dei servizi digitali e la Commissione nella vigilanza sulle piattaforme online di dimensioni molto grandi (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 livello⁵². 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 attività⁵³. 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.

Se, secondo le prescrizioni del DSA, al Comitato è richiesto di adottare una raccomandazione⁵⁴, 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 mantenuto 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 DSA⁵⁵; dell'as-

⁵² 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».

⁵³ Il funzionamento del Comitato sarà disciplinato da un regolamento interno, adottato previo accordo con la Commissione (art. 62, par. 7, DSA).

⁵⁴ 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).

⁵⁵ V. *supra*, par. 4.

Sezione monografica - Il *Digital Services Act* e il contrasto alla disinformazione: responsabilità dei *provider*, obblighi di *compliance* e modelli di *enforcement*

sistenza alle autorità competenti nell'analisi delle relazioni e dei risultati delle revisioni di *VLOPs* e *VLOSEs*⁵⁶; 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)⁵⁷ 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 europea⁵⁸, soggetto che – come si è già posto in luce – assume importanza centrale 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, perpetrata da 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.

⁵⁶ Si possono ad esempio richiamare le revisioni indipendenti *ex artt.* 37 e 75, par. 2, DSA già menzionate *supra*, par. 3.

⁵⁷ Su cui v. *infra*, par. 6.

⁵⁸ 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 *Diritto di internet*, 1, 2023, 73 ss.

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 membri⁵⁹: 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 *VLOPs* e *VLOSEs*.

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 nazionale⁶⁰, 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 DSA⁶¹, ferma restando la possibilità che la Commissione richieda il sostegno, singolo o congiunto, dei coordinatori dei servizi digitali interessati dalla presunta violazione⁶², i quali dovranno cooperare «dealmente e tempestivamente» (art. 66, par.

⁵⁹ *Supra*, par. 3.

⁶⁰ 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).

⁶¹ 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».

⁶² 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).

Sezione monografica - Il *Digital Services Act* e il contrasto alla disinformazione: responsabilità dei *provider*, obblighi di *compliance* e modelli di *enforcement*

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 parere⁶³.

Soffermando 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 DSA⁶⁴ 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.

Come osservato, 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

⁶³ Con riferimento alle constatazioni preliminari della Commissione v. anche *infra*, par. 6.1.

⁶⁴ *Supra*, par. 3.

interessata; nell'esame dei libri e 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 stato adottato il relativo *implementing regulation*⁶⁵.

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 violazione⁶⁶.

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 si offre di assumere *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)⁶⁷.

⁶⁵ Regolamento di esecuzione (UE) 2023/1201 della Commissione del 21 giugno 2023 relativo alle modalità dettagliate di attuazione da parte della Commissione di determinate procedure a norma del regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio («regolamento sui servizi digitali»).

⁶⁶ 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».

⁶⁷ Rileva una qualche similitudine tra la logica di tali «soluzioni negoziate» volte a definire il procedimento e quella dei *non prosecution agreement* nordamericani E. Birritteri, *Punire la disinformazione*, cit., 315.

Sezione monografica - Il *Digital Services Act* e il contrasto alla disinformazione: responsabilità dei *provider*, obblighi di *compliance* e modelli di *enforcement*

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, 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). A tal fine, 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. 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)⁶⁸.

Considerate le conseguenze di una simile decisione, la relativa adozione è corredata da talune garanzie procedurali: la Commissione deve infatti comunicare le proprie constatazioni preliminari al soggetto interessato prima di procedere, 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

⁶⁸ L'esito procedimentale può anche condurre a ritenere le condizioni di cui all'art. 73, par. 1, DSA 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.

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. *d*).

La sanzione in oggetto a carico di *VLOPs* e *VLOSEs* sarà invece non superiore 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 – se, in modo intenzionale o per negligenza, si verifichi uno dei seguenti casi: 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 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 interessati⁶⁹ 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 diverso⁷⁰ – *sub* art. 74, par. 1, lett. *a*), sostanzialmente, qualsiasi violazione del regolamento – che, forse, più opportunamente si sarebbe potuto differenziare mediante cornici sanzionatorie autonome; ciò avrebbe contribuito, altresì, 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 dei suddetti 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

⁶⁹ 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).

⁷⁰ V. già, per considerazioni di simile tenore nel contesto del GDPR, L. D'Agostino, *La tutela penale dei dati personali nel riformato quadro normativo*, cit., 21.

Sezione monografica - Il *Digital Services Act* e il contrasto alla disinformazione: responsabilità dei *provider*, obblighi di *compliance* e modelli di *enforcement*

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 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 respingerlo, 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 servizi 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).

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)⁷¹.

Il regolamento si premura di prevedere anche una disciplina degli atti interruttivi – elencati in via esemplificativa al par. 3 della disposizione⁷² 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 prescrizione massimo⁷³.

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)⁷⁴.

⁷¹ 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).

⁷² 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.

⁷³ *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.

⁷⁴ L'art. 78, par. 3, DSA stabilisce che il termine di prescrizione per l'esecuzione delle sanzioni è

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 strutturata 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 pacchetto⁷⁵ 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 decentramento⁷⁶.

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.⁷⁷

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

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.

⁷⁵ In argomento v. M. Eifert - A. Metzger - H. Schweitzer - G. Wagner, *Taming the giants: The DMA/DSA package*, in *Common Market Law Review*, 2021, 987 ss. Per una chiave di lettura focalizzata sull'impatto socio-economico dei due regolamenti in discorso, v. il recente studio di F. Decarolis - M. Li, *Regulating Online Search in the EU: From the Android Case to the Digital Markets Act and Digital Services Act*, in *International Journal of Industrial Organization*, 90, 2023, 1 ss.

⁷⁶ Questa la lettura di L. Torchia, *I poteri di vigilanza*, cit., 1106 ss. e 1110 ss. Sulle potenziali interferenze applicative, in particolare, tra DSA e *AI Act*, v. S. Tommasi, *Digital Services Act e Artificial Intelligence Act: tentativi di futuro da armonizzare*, in *Persona e mercato*, 2, 2023, 279 ss.

⁷⁷ F. G'sell, *The Digital Services Act*, cit., 106.

Sezione monografica - Il *Digital Services Act* e il contrasto alla disinformazione: responsabilità dei *provider*, obblighi di *compliance* e modelli di *enforcement*

europea nei casi di stasi⁷⁸.

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 capacità di non subire, quale *enforcer* del DSA, condizionamenti legati alla propria agenda e ai propri obiettivi politici in ambiti correlati al regolamento⁷⁹.

Sul piano dei risvolti dei poteri di cui alla normativa, l'insieme delle previsioni prese in esame restituisce l'immagine di un sistema finalizzato in via principale alla tutela dell'utente che – contemperando l'affettività di alcune delle misure introdotte con la costruzione di un apparato di garanzie⁸⁰ – replica nel contesto dei servizi digitali l'approccio *risk based* adottato in altri settori: merita attenzione l'imposizione, 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 cybersicurezza⁸¹ e di sostenibilità⁸². Se tale scelta appare condivisibile in vista di una massimizzazione del grado di effettività del DSA, come già rilevato permangono, tuttavia, talune perplessità sulle relative modalità di attuazione: si pensi alla previsione, sostanzialmente, di una unica macro cornice edittale nell'ambito delle sanzioni pecuniarie applicabili da parte della Commissione, per violazioni di – anche notevole – diverso disvalore⁸³.

Concludendo, in definitiva resterà da vedere come gli attori pubblici – Stati membri e Commissione – si orienteranno nel dare esecuzione alle disposizioni del nuovo regolamento.

Certamente sarà particolarmente importante provvedere, tramite ogni opportuna modifica normativa o regolamentare di raccordo, a implementare procedure efficaci per adempiere agli obblighi di cooperazione reciproci tra i soggetti coinvolti e per il migliore esercizio dei poteri di *enforcement* attribuiti dal DSA. A livello nazionale, ove emergeranno *gap* di disciplina sul punto, ciò comporterà la necessità di introdurre, in particolare, sanzioni amministrative per le violazioni del regolamento, conformemente

⁷⁸ V. in questo senso le riflessioni di G. Buttarelli, *La regolazione delle piattaforme digitali*, cit., 123.

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

⁸⁰ Di una «riedizione» dell'effetto di Bruxelles di cui si è detto a proposito dell'esportazione del GDPR, ma questa volta fondato più su un *humus* procedurale che assiologico-sostanziale, e quindi meno suscettibile di crisi di rigetto» parla O. Pollicino, voce *Potere digitale*, in *Enciclopedia del diritto, I tematici*, V, Milano, 2023, 442.

⁸¹ Il riferimento è, ad esempio, agli obblighi di adozione di misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi per la sicurezza delle reti e dei sistemi informativi e di notifica degli incidenti da parte degli operatori di servizi essenziali e fornitori di servizi digitali di cui alla direttiva (UE) 2016/1148 (NIS), il cui impianto è sostanzialmente confermato – pur con alcune novità, ad esempio sul piano dei destinatari della normativa – dalla recente direttiva (UE) 2022/2555 (NIS 2).

⁸² 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 *Archivio penale web*, 2, 2022, 8 ss.

⁸³ V. *supra*, par. 6.1.

ai criteri ivi sanciti: ossia, dovrà trattarsi di «*penalties*» effettive, proporzionate e dissuasive e in linea con i limiti massimi edittali previsti. Dovrà, del pari, essere oggetto di regolamentazione il correlato procedimento di applicazione delle sanzioni, nel rispetto dei principi di garanzia richiamati dal DSA (tra l'altro, tutela del diritto di difesa, diritto di essere ascoltati e di accedere al fascicolo, diritto a un ricorso giurisdizionale effettivo, secondo quanto stabilito dall'art. 51, par. 6 del regolamento)⁸⁴.

⁸⁴ Cfr. sul punto la scelta operata, come si è detto, dal legislatore italiano, che ha demandato all'AGCOM, in qualità di coordinatore dei servizi digitali, di individuare le modalità di applicazione delle sanzioni secondo procedure stabilite con proprio regolamento.