ISSN 1826-3534

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

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

INFORMATION DISORDER E SISTEMA DEMOCRATICO
30 MAGGIO 2025

Problemi di coordinamento normativo nel contrasto alla disinformazione politica e commerciale

di Edoardo Alberto Rossi
Professore associato di Diritto internazionale
Università degli Studi di Urbino Carlo Bo

DAFNE

Questo Fascicolo speciale rappresenta il primo risultato di ricerca del Progetto PRIN 2022 *DAFNE* (*Democratic governance of Automated system for Fake News*), è finanziato dall'Unione europea - Next Generation EU, Missione 4 Componente 1, CUP H53D23010930001, Codice MUR P2022R7RS9 e raccoglie alcune delle relazioni e degli interventi presentati al Convegno "*Information disorder* e sistema democratico. Principi, regole e tecniche contro la disinformazione", Sapienza Università di Roma, 9 dicembre 2024.

Problemi di coordinamento normativo nel contrasto alla disinformazione politica e commerciale*

di Edoardo Alberto Rossi
Professore associato di Diritto internazionale
Università degli Studi di Urbino Carlo Bo

Abstract [It]: Negli ultimi anni si è assistito alla proliferazione delle fonti dell'Unione nel settore della transizione digitale e del mercato unico digitale, fino al recente AI act. Alla moltiplicazione del numero di interventi legislativi ha fatto seguito la moltiplicazione dei rischi di interferenze. I settori della comunicazione politica e commerciale si prestano facilmente ad essere terreno fertile per potenziali conflitti tra le disposizioni delle fonti UE, con conseguenze non secondarie sulla certezza del diritto, sull'effettività dell'esercizio dei diritti fondamentali e sull'efficacia dei rimedi in caso di violazioni.

Title: Regulatory coordination problems in countering political and commercial disinformation
Abstract [En]: Recent years have seen a proliferation of EU legal instruments in the area of digital transition and digital single market, up to the recent AI Act. The growing number of legal sources has been followed by growing risks of interferences. The areas of political and commercial communication are susceptible of potential conflicts between the provisions of EU legal sources, with not minor consequences for legal certainty, the exercise of fundamental rights and effectiveness of administrative and judicial remedies.

Parole chiave: Disinformazione, servizi digitali, intelligenza artificiale, comunicazione politica, comunicazione commerciale
Keywords: Disinformation, digital services, artificial intelligence, political communication, commercial communication

* Articolo sottoposto a referaggio. Il presente lavoro è stato elaborato nell'ambito delle attività del PRIN PNRR 2022, dal titolo DAFNE (Democratic governance of Automated systems for Fake News)

1. Introduzione. La proliferazione delle fonti dell'Unione europea nel settore del mercato unico digitale

Negli ultimi dieci anni si è assistito alla proliferazione delle fonti dell'Unione nel settore della transizione digitale e del mercato unico digitale[1], a partire dal GDPR[2] fino al recente regolamento sull'intelligenza artificiale (*AI act*)[3]. Alla moltiplicazione del numero di interventi legislativi ha fatto seguito la moltiplicazione dei rischi di interferenze fra gli stessi, con possibili sovrapposizioni, divergenze e incompatibilità applicative e interpretative.

Evidentemente il fenomeno della disinformazione[4] – in particolare nei due settori strategici di nostro interesse (comunicazione politica e comunicazione commerciale) – si presta facilmente ad essere terreno fertile per potenziali conflitti tra le disposizioni delle fonti UE.

---

[1] In tema v. F. MARCHETTI, *La strategia della Commissione europea per il mercato unico digitale nelle prossime iniziative legislative*, in *Riv. dir. int. priv. proc.*, 2016 fasc. 1, p. 326 ss.; C. SCHMIDT, R. KRIMMER, *How to implement the European digital single market:*
identifying the catalyst for digital transformation, in *Journal of European integration*, n. 1, 2022, p. 59 ss.; Ł.D. DĄBROWSKI, M. SUSKA (eds.), *The European Union Digital Single Market. Europe's Digital Transformation*, Routledge, London, 2023; B. BERTARINI, *European Union Digital Single Market*, FrancoAngeli, Milano, 2023, p. 15 ss.; nonché F. FERRI, *Il bilanciamento dei diritti fondamentali nel mercato unico digitale*, Giappichelli, Torino, 2022, p. 25 ss. e G. ZACCARONI, *Facing the Golem: Disruptive Technologies vs Democracy in the EU Digital Single Market*, in I. SAMMUT, I. MIFSUD (eds.), *The EU Internal Market in the Next Decade – Quo Vadis?*, Brill, Leiden, 2024, p. 186 ss.

[2] 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 (GDPR).

[3] La Commissione europea non ha reso disponibile un elenco completo degli atti legislativi nel settore delle tecnologie digitali. Affidandoci ad un diligente lavoro, possiamo richiamare la terza edizione del *Digital factsheet: A dataset on EU legislation for the digital world*, pubblicata il 6 giugno 2024 dal *think tank* specializzato in politiche economiche Bruegel (autori: J. Scott Marcus, Kamil Sekut, Kai Zenner). Questo documento contiene una precisa *Overview of EU Legislations in the Digital Sector*, aggiornata al mese di Maggio 2024, in cui viene evidenziato come oltre cento atti legislativi nel settore digitale siano stati adottati o siano in corso di adozione (circa novanta già adottati come atti legislativi, circa venti in corso di negoziazione e circa dieci già pianificati per il prossimo futuro) e oltre ottanta sono i meccanismi di *governance* per attuare e far rispettare la legislazione digitale (v. anche l'annuncio sul blog kaizenner.eu).

[4] Senza poterci soffermare diffusamente sugli aspetti definitori, basti qui ricordare che, nonostante la tendenza a distinguere tra misinformazione (che esclude la volontà di diffondere informazioni false "nella convinzione di essere nel giusto": v. G.M. RUOTOLO, *Nell'anno delle elezioni hanno tutti ragione. Alcune considerazioni sul ruolo di diritto internazionale ed UE nel contrasto alla disinformazione*, in *SIDIBlog*, 5 aprile 2024) e disinformazione in senso stretto, che invece presuppone la deliberata diffusione di notizie false o fuorvianti allo scopo di provocare conseguenze dannose (v. O. POLLICINO, P. DUNN, *Disinformazione e intelligenza artificiale nell'anno delle* global elections: *rischi (ed opportunità)*, in *federalismi.it*, n.12, 2024, p. v; M. CASTELLANETA, *La disinformazione nel conflitto in Ucraina: tra* ius in bello *e diritto alla libertà di espressione*, in O. PORCHIA, M. VELLANO, *Il diritto internazionale per la pace e nella guerra. Sviluppi recenti e prospettive future.* Liber amicorum *in onore di Edoardo Greppi*, Edizioni Scientifiche Italiane, Torino-Napoli, 2023, p. 327 ss.), in realtà con il termine "disinformazione" si possono identificare varie ed eterogenee forme di disordini informativi (v. i contributi di M. CAVINO, R. BRACCIALE-F. GRISOLIA, G. RUFFO-M. TAMBUSCIO, all'interno del fascicolo speciale dal titolo *La disinformazione* online *e il ruolo degli esperti nell'agorà digitale*, in questa *Rivista*, n. 11, 2020, oltre a B. BAADE, *Fake News and International Law*, in *The European Journal of International Law*, n. 4, 2018, p. 1358 ss., nonché, con particolare riferimento al DSA di cui diremo *infra*, M. BARBIERI, V. OTTONE, *La politica di prevenzione e contrasto alla disinformazione* online *nel* Digital Services Act. *Le sfide emergenti per la* multi-level governance *europea*, in *Comunicazione politica*, n. 2, 2023, p. 299). In argomento v. altresì l'ampia e approfondita disamina di G. VASINO, *Lotta alla disinformazione, garanzie costituzionali e tutela dei diritti fondamentali nel panorama normativo euro-unitario*, in questo numero speciale.

Le conseguenze che ne derivano non sono secondarie, perché impattano negativamente sulla certezza del diritto, sull'effettività dell'esercizio dei diritti fondamentali e sull'efficacia dei rimedi a disposizione dei cittadini[5].

Molteplici sono gli esempi che possono essere portati al riguardo, sia in riferimento alla comunicazione politica, sia alla comunicazione commerciale, con la consapevolezza che il numero è destinato ad aumentare.

In questo contributo esamineremo, senza pretese di esaustività, alcune interferenze che si possono manifestare nel settore della comunicazione "politica" (par. 2 ss.) e, più succintamente, in quello della comunicazione "commerciale" (par. 3 ss.), da cui ricaveremo alcune considerazioni di carattere generale sul contributo della politica legislativa, specialmente del diritto dell'Unione europea e del diritto internazionale, nel contrasto alla disinformazione (par. 4).

2. Interferenze normative nel settore della "comunicazione politica" *online*

Il settore della comunicazione "politica" non ha confini ben definiti. Molte forme di comunicazione attraverso mezzi digitali riguardano aspetti di natura politica, ma non per questo possono essere considerate "comunicazioni politiche". Inoltre, anche la qualifica dell'autore della comunicazione contribuisce ad accrescere l'incertezza sulla riconducibilità all'alveo della "comunicazione politica", posto che non tutte le forme di "comunicazione politica" provengono da esponenti del mondo politico o partitico a livello locale, nazionale o internazionale[6]. Anche i canali che vengono utilizzati non sono

[5] Trattasi di valori basilari del diritto dell'Unione europea, componenti irrinunciabili nel processo di "costituzionalizzazione" dello spazio digitale, sul quale v. F. FERRI, *Transizione digitale e valori fondanti dell'Unione: riflessioni sulla costituzionalizzazione dello spazio digitale europeo*, in *Il diritto dell'Unione europea*, n. 2, 2022, p. 277 ss., nonché E. CELESTE; *Digital Constitutionalism. The Role of Internet Bills of Rights*; Routledge, London, 2022, p. 81 ss.; E. CELESTE, N. PALLADINO, D. REDEKER, K. YILMA, *The Content Governance Dilemma. Digital Constitutionalism, Social Media and the Search for a Global Standard*, Palgrave MacMillan, 2023, p. 61 ss.; F. CASOLARI, *Il Digital Services Act e la costituzionalizzazione dello spazio digitale europeo*, in *Giurisprudenza italiana*, 2024, pp. 464-465; G. DE GREGORIO, *The rise of digital constitutionalism in the European Union*, in *International Journal of Constitutional Law*, n. 1, 2021, p. 41 ss. (e dello stesso Autore, più recentemente, G. DE GREGORIO, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, Cambridge, 2022).

[6] Anche se non sarà oggetto di specifica trattazione, sembra opportuno richiamare la recente direttiva 2024/1069 dell'11 aprile 2024, che dovrà essere attuata dagli Stati membri entro il 2026, relativa alla protezione delle persone attive nella partecipazione pubblica da domande giudiziali manifestamente infondate o abusive (azioni legali strategiche tese a bloccare la partecipazione pubblica), ormai già nota come direttiva anti-*slapps*. Questa direttiva, pur non occupandosi specificamente di comunicazione politica, tantomeno *online*, appare comunque idonea ad assumere rilevanza nella lotta alla disinformazione. Essa, infatti, è volta a proteggere la libertà di espressione di giornalisti, editori, media, ong, sindacati, ricercatori, accademici, attivisti e altri soggetti coinvolti nella "partecipazione pubblica". Pur trovando base giuridica nell'art. 81 TFUE (cooperazione giudiziaria in materia civile) e vertendo dunque prevalentemente su aspetti processuali, essa include nel proprio campo di applicazione "questioni di interesse pubblico", riconducendovi espressamente "le attività volte a proteggere i valori sanciti dall'articolo 2 del trattato sull'Unione europea, compresa la protezione dei processi democratici da indebite ingerenze, in particolare *combattendo la disinformazione*" (art. 4, n. 2, lett. *e*; cors. agg.). A tale scopo, ancorché limitatamente ad azioni giudiziarie con implicazioni transfrontaliere (cioè in cui i soggetti coinvolti sono domiciliati in Stati diversi), essa impone agli Stati membri di introdurre negli ordinamenti statali specifiche garanzie

sempre propriamente "politici", come potrebbero essere testate giornalistiche specialistiche, comunicati ufficiali o bollettini di informazione, dato che molto di frequente le comunicazioni politiche sono effettuate attraverso canali utilizzati anche per qualsiasi altra forma di comunicazione. Infine, l'incertezza è ulteriormente accresciuta dal fatto che all'interno della generale nozione di "comunicazione politica" è possibile distinguere tra varie forme di comunicazione, come la propaganda, la comunicazione elettorale e ulteriori diverse forme di comunicazione su questioni di natura "politica".

Alla luce di queste generali incertezze definitorie, che incidono notevolmente sull'accertamento dell'applicabilità di alcune fonti del diritto dell'Unione[7], si rendono necessarie valutazioni caso per caso, basate sull'approccio di qualificazione autonoma, tipico del diritto dell'Unione: per poter determinare se una data fonte è applicabile occorrerà preliminarmente accertare che la comunicazione in questione rientri nel suo campo di applicazione.

Questa considerazione, valida per alcune fonti con campo di applicazione circoscritto a specifiche forme di comunicazione, come il Regolamento sulla pubblicità politica (RPA)[8], non assume la medesima centralità per quelle fonti a più ampio raggio di azione che si propongono di dettare una disciplina di carattere generale, come, ad esempio, il *Digital Services Act* (DSA)[9] e l'*AI Act*[10]. Come vedremo nei seguenti paragrafi, al fine di determinare l'applicabilità e il conseguente coordinamento delle fonti vigenti sono richieste approfondite conoscenze dell'intero articolato quadro normativo di riferimento.

2.1. Coordinamento tra *DSA* e *AI Act*. Gli obblighi previsti per l'utilizzo di sistemi di IA in grado di influenzare esiti elettorali e comportamenti di voto

A partire dal 17 febbraio 2024 è diventato integralmente applicabile il Regolamento (UE) 2022/2065, comunemente conosciuto come *Digital Services Act* (DSA). A questo Regolamento è stato riconosciuto il merito di aver tentato di predisporre una cornice normativa idonea a rafforzare la protezione dei diritti

procedurali (art. 6 ss.: cauzioni, rigetto anticipato, trattazione accelerata e prioritaria, sanzioni e condanne), negando il riconoscimento delle sentenze emesse in Paesi terzi all'esito di procedimenti infondati o abusivi nei confronti di soggetti impegnati nella "partecipazione pubblica" (art. 16) e concedendo a questi ultimi il diritto di rivolgersi ai giudici degli Stati membri in cui sono domiciliati, al fine di ottenere risarcimenti per i danni derivanti dai procedimenti giudiziari subiti in uno Stato terzo (art. 17).

[7] V. *infra*, par. 2.1 ss.

[8] Regolamento (UE) 2024/900 del Parlamento europeo e del Consiglio del 13 marzo 2024 relativo alla trasparenza e al targeting della pubblicità politica (regolamento sulla pubblicità politica - RPA).

[9] 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 - DSA).

[10] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale – *AI Act*).

fondamentali degli utenti *online*[11], anche grazie all'introduzione di obblighi differenziati per i prestatori di servizi di intermediazione digitale[12] finalizzati all'incremento della chiarezza e della trasparenza dell'ambiente digitale[13].

Un basilare principio del DSA è costituito dall'esonero di responsabilità dei prestatori di servizi intermediari di memorizzazione di informazioni per i contenuti caricati dagli utenti e dall'assenza di generali obblighi di sorveglianza e accertamento attivo delle informazioni trasmesse o memorizzate[14].

L'art. 6 del DSA esclude infatti la responsabilità del prestatore per le informazioni memorizzate su richiesta di un utente, ad eccezione dei casi di effettiva conoscenza dell'illegalità dei contenuti oppure di mancata rimozione immediata dopo aver avuto conoscenza dell'illegalità degli stessi[15]. Coerentemente,

[11] A. TURILLAZZI, M. TADDEO, L. FLORIDI, F. CASOLARI, *The Digital Services Act: an Analysis of its Ethical, Legal, and Social Implications*, in *Law, Innovation and Technology*, 2023, p. 83 ss.; M.I. TORRES CAZORLA, *Ensuring a Safe and Accountable Online Environment. The Need for the Digital Services Act and its Historical Basis,* in *Revue des Affaires Européennes*, 2023, p. 617 ss.; A. MANTELERO, *Fundamental Rights Impact Assessment in the DSA,* in J. VAN HOBOKEN, J.P. QUINTAIS, N. APPELMAN, R. FAHY, I. BURI, M. STRAUB, *Putting the DSA into Practice. Enforcement, Access to Justice and Global Implications*, Verfassungsbooks, Berlin, 2023, p. 109 ss.

[12] Il DSA, all'art. 3, fornisce le seguenti definizioni dei c.d. servizi intermediari della società dell'informazione: "[U]n servizio di semplice trasporto (cosiddetto «mere conduit»), consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio o nel fornire accesso a una rete di comunicazione; un servizio di memorizzazione temporanea (cosiddetto «caching»), consistente nel trasmettere, su una rete di comunicazione, informazioni fornite dal destinatario del servizio, che comporta la memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficiente il successivo inoltro delle informazioni ad altri destinatari su loro richiesta; un servizio di memorizzazione di informazioni (cosiddetto «hosting»), consistente nel memorizzare informazioni fornite da un destinatario del servizio su richiesta dello stesso".

[13] Per una ricostruzione critica degli obblighi previsti dal DSA, il ruolo della c.d. co-regolamentazione e i rischi che ne possono derivare per la libertà di espressione v. A. PALUMBO, J. PIEMONTE, *Delega di funzioni regolamentari e lotta ai rischi sistemici causati della disinformazione nel* Digital Services Act*: quali rischi per la libertà di espressione?*, in *MediaLaws*, n. 3, 2023, p. 116 ss.

[14] Nonostante il DSA, all'art. 89, abbia abrogato gli articoli da 12 a 15 della direttiva sul commercio elettronico (direttiva n. 2000/31/CE), sostituendo i relativi riferimenti rispettivamente agli articoli 4, 5, 6 e 8 del DSA, in realtà la generale esenzione da responsabilità dei prestatori di servizi di *hosting* per i contenuti memorizzati provenienti da terzi, già prevista dall'art. 14, par. 1, della direttiva, è stata mantenuta a condizioni pressoché identiche (v. G.M. RUOTOLO, *Mercati e servizi digitali in Europa: valori fondanti e 'regimi' in competizione*, in *Diritti umani e diritto internazionale*, n. 1, 2023, pp. 72-73; M.A. ASTONE, Digital Services Act *e nuovo quadro di esenzione della responsabilità dei prestatori di servizi intermediari: quali prospettive?*, in *Contratto e impresa*, n. 4, 2022, p. 1060). Analoghe considerazioni valgono anche per l'assenza di generali obblighi di sorveglianza e ricerca di contenuti illeciti già previsti dall'art. 15 della direttiva sul commercio elettronico e confermata nel DSA (v. F. WILMAN, *Between Preservation and Clarification: The Evolution of the DSA's Liability Rules in Light of the CJEU's Case Law*, in J. VAN HOBOKEN, J.P. QUINTAIS, N. APPELMAN, R. FAHY, I. BURI, M. STRAUB, *Putting the DSA into Practice*, *cit.*, p. 37 ss.; G.M. RUOTOLO, Digital Services Act *e* Digital Markets Act *tra responsabilità dei fornitori e rischi di* bis in idem, in *Quaderni di SIDIBlog*, 2021, p. 223 ss.; nonché *infra*).

[15] L'art. 6, esclude l'esenzione di responsabilità, al par. 2, se l'utente che ha caricato i contenuti "agisce sotto l'autorità o il controllo del prestatore", nonché, al par. 3, qualora si tratti di "responsabilità prevista dalla normativa in materia di protezione dei consumatori per le piattaforme online che consentono ai consumatori di concludere contratti a distanza con operatori commerciali, qualora tali piattaforme online presentino informazioni specifiche o rendano altrimenti possibile l'operazione specifica in questione in modo tale da indurre un consumatore medio a ritenere che le informazioni, o il prodotto o il servizio oggetto dell'operazione, siano forniti dalla piattaforma stessa o da un destinatario del servizio che agisce sotto la sua autorità o il suo controllo". In tema v. M. NINO, *Il rapporto tra libertà di espressione e diritto d'autore: considerazioni critiche alla luce della prassi nazionale ed internazionale*, in *Diritti umani e diritto internazionale*, 2016, p. 549 ss.

l'art. 8 esclude in capo ai prestatori obblighi generali di sorveglianza sulle informazioni trasmesse o memorizzate e di accertamento attivo di fatti o circostanze indicative di attività illegali.

In questo quadro si inserisce l'art. 7 del DSA, che reputa irrilevante sull'esenzione di responsabilità (che continua pertanto a trovare applicazione) l'eventuale svolgimento di indagini volontarie, volte ad individuare e rimuovere contenuti illegali[16].

Questa disposizione innova il quadro giuridico normativo rispetto al precedente regime della direttiva sul commercio elettronico e si innesta nella consolidata giurisprudenza della Corte di Giustizia[17] relativa alla distinzione tra "*hosting providers* passivi", esenti da responsabilità in quanto ignari e sprovvisti del potere di controllo preventivo delle informazioni, e "*hosting providers* attivi", ai quali non è applicabile l'esenzione di responsabilità in ragione della "compartecipazione" nella gestione dei contenuti illeciti[18].

A questo riguardo, il considerando n. 18 del DSA ribadisce l'inapplicabilità delle esenzioni di responsabilità allorché il "prestatore di servizi intermediari svolga un ruolo attivo atto a conferirgli la conoscenza o il controllo di tali informazioni". Tuttavia, l'art. 7 precisa che l'adozione di sistemi di monitoraggio e controllo dei contenuti di iniziativa dei prestatori non rileva ai fini dell'esclusione dell'esenzione di responsabilità: se adottano tali forme di controllo – peraltro incentivate espressamente dal diritto dell'Unione – i prestatori non possono essere ritenuti attivamente coinvolti nell'immissione dei contenuti illegali. La *ratio* della norma è evidente: evitare di disincentivare l'utilizzo di sistemi volontari di controllo per non incorrere nella responsabilità correlata alla diffusione di contenuti illeciti.

Se così stanno le cose, resta aperto il problema dell'individuazione delle circostanze che generano la responsabilità del prestatore[19]. In altri termini, c'è da chiedersi se l'utilizzo di sistemi automatizzati che sfruttano algoritmi valga quale forma di "conoscenza" o "controllo" delle informazioni oppure se si tratti di una fattispecie rientrante nell'art. 7 del DSA.

In proposito, ci sembra di poter affermare che fintantoché il controllo ha esclusivo carattere automatizzato – cioè viene compiuto da un software che può soltanto accettare o rifiutare la memorizzazione richiedendo un'eventuale revisione manuale umana in via sussidiaria, senza manipolare

[16] M.A. ASTONE, Digital Services Act *e nuovo quadro di esenzione della responsabilità*, *cit.*, p. 1062.

[17] F. WILMAN, *Between Preservation and Clarification*, *cit*, p. 37 ss.

[18] Ad esempio, si veda nel vasto panorama giurisprudenziale la sentenza Corte di giustizia, C-682/18 e C-683/18, *Peterson c. Google e altri*, 22 giugno 2021, par. 106 ss.. Sull'evoluzione della responsabilità degli *hosting providers* in materia v. altresì, G.M. RUOTOLO, *Scritti di diritto internazionale ed europeo dei dati*, Cacucci, Bari, 2021, p. 251 ss.; M.A. ASTONE, Digital Services Act *e nuovo quadro di esenzione della responsabilità*, *cit.*, p. 1052 ss.; G. MONGA, *Responsabilità degli intermediari. Il Digital Services Act*, in M. MAGGIORE (a cura di), *Il commercio elettronico. Digital Markets Act, Digital Services Act e altre dimensioni giuridiche*, Giappichelli, Torino, 2024, p. 92 ss.

[19] Sul quale v. anche il contributo di L. CALIFANO, *La libertà di manifestazione del pensiero... in rete; nuove frontiere di esercizio di un diritto antico.* Fake news, hate speech *e profili di responsabilità dei* social network, in *federalismi.it*, n. 26, 2021, p. 16 ss. La problematica è ben inquadrata in termini ampi e sistematici anche da S. MARTINELLI, *I contratti della* platform economy, Giappichelli, Torino, 2023, p. 93 ss.

i contenuti o le informazioni – si possa ricadere nella fattispecie dell'art. 7 del DSA, escludendo dunque la responsabilità del prestatore del servizio[20]. Diversa è l'ipotesi in cui la verifica sia sottoposta – prima, dopo o contestualmente al controllo automatizzato – ad intervento umano. In questo caso appare ardua la dimostrazione della mancata conoscenza dei contenuti e, conseguentemente, la possibilità di invocare l'esenzione di responsabilità[21].

Alla luce di tali considerazioni, sembra ora opportuno formulare qualche riflessione sulle condizioni alle quali questi principi possono trovare applicazione in relazione a due dei sistemi automatizzati più frequentemente utilizzati dai prestatori di servizi di intermediazione digitale: i sistemi di moderazione e i sistemi di raccomandazione.

Quando i prestatori utilizzano sistemi automatizzati di moderazione sono sottoposti ad alcuni obblighi previsti dal DSA[22]. Le attività di "moderazione" sono definite dal DSA come "le attività, automatizzate o meno, svolte dai prestatori di servizi intermediari con il fine, in particolare, di individuare, identificare e contrastare contenuti illegali e informazioni incompatibili con le condizioni generali, forniti dai destinatari del servizio, comprese le misure adottate che incidono sulla disponibilità, sulla visibilità e sull'accessibilità di tali contenuti illegali o informazioni, quali la loro retrocessione, demonetizzazione o rimozione o la disabilitazione dell'accesso agli stessi, o che incidono sulla capacità dei destinatari del servizio di fornire tali informazioni, quali la cessazione o la sospensione dell'account di un destinatario del servizio".

In relazione a questo genere di sistemi e alla loro potenziale incidenza sulla "conoscenza" dei contenuti da parte dei prestatori digitali, è utile sottolineare che anche quando sono concepiti in maniera automatizzata, l'art. 16, par. 1, prevede che i prestatori di servizi di memorizzazione predispongano meccanismi di segnalazione per consentire agli utenti di notificare la presenza di contenuti asseritamente illegali, da valutare adottando decisioni "in modo tempestivo, diligente, non arbitrario e obiettivo",

[20] Vedi TAR Lazio, sentenza del 17 gennaio 2024, *Meta Platforms Ireland Ltd. v. AGCOM*, riguardante l'illecita sponsorizzazione del gioco d'azzardo su un *social network*.

[21] A questo riguardo v. le considerazioni di S. TOMMASI, Digital Services Act *e* Artificial Intelligence Act*: tentativi di futuro da armonizzare*, in *Persona e Mercato*, n. 2, 2023, p. 290 ss., che esprime forti perplessità sulla possibilità di individuare un ruolo meramente passivo dei prestatori di servizi digitali, anche alla luce dei caratteri tecnici tipici dell'attuale architettura dell'ecosistema digitale. In tema cfr. anche G. MONGA, *Responsabilità degli intermediari, cit.*, pp. 212-213.

[22] Ad esempio, secondo l'articolo 15, riguardante gli obblighi in materia di trasparenza, i prestatori sono tenuti a rendere accessibile almeno annualmente una relazione sull'attività di moderazione dei contenuti contenente, tra le altre cose, informazioni sulla formazione dei moderatori (lett. *c*) e sull'utilizzo di strumenti automatizzati ai fini di moderazione dei contenuti (lett. *c* ed *e*), "compresi la descrizione qualitativa, la descrizione delle finalità precise, gli indicatori di accuratezza e il possibile tasso di errore degli strumenti automatizzati utilizzati nel perseguimento di tali scopi e le eventuali garanzie applicate" (lett. *e*). In tema 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*, in *MediaLaws*, n. 2, 2023, p. 59 ss.

includendo informazioni sull'eventuale utilizzo di "strumenti automatizzati per tali processi di trattamento o decisione" (art. 16, par. 6)[23].

Queste segnalazioni hanno sicuramente l'effetto di escludere l'esenzione di responsabilità di cui all'art. 6 del DSA, come previsto dall'art. 16, par. 3, secondo cui "[s]i considera che le segnalazioni di cui al presente articolo permettono di acquisire una conoscenza o consapevolezza effettiva ai fini dell'articolo 6 in relazione alle specifiche informazioni in questione qualora consentano a un prestatore diligente di servizi di memorizzazione di informazioni di individuare l'illegalità della pertinente attività o informazione senza un esame giuridico dettagliato"[24]. Peraltro, le decisioni sugli eventuali reclami, ai sensi del par. 6 dell'art. 20, devono essere espressamente "prese con la supervisione di personale adeguatamente qualificato e *non avvalendosi esclusivamente di strumenti automatizzati*"[25] (cors. agg.).

Riflessioni di diverso tenore devono essere effettuate in ordine a strumenti automatizzati utilizzati dai prestatori con funzioni diverse dalla moderazione, come ad esempio i sistemi di raccomandazione. Questi sistemi sono definiti dal DSA, all'art. 3, lett. *s*, come ogni "sistema interamente o parzialmente automatizzato che una piattaforma *online* utilizza per suggerire informazioni specifiche, tramite la propria interfaccia *online*, ai destinatari del servizio o mettere in ordine di priorità dette informazioni anche quale risultato di una ricerca avviata dal destinatario del servizio o determinando in altro modo l'ordine relativo o l'importanza delle informazioni visualizzate"[26].

Posto che i sistemi di raccomandazione non ricadono nell'art. 7 del DSA, non trattandosi di indagini volontarie o attività similari, c'è tuttavia da chiedersi se tali sistemi, specialmente quando attuati in forma esclusivamente automatizzata, possano implicare una forma di "conoscenza o controllo" e, di conseguenza, realizzare una condotta di compartecipazione dei prestatori, che consentirebbe di escludere l'applicazione dell'esenzione di responsabilità prevista dall'art. 6. La risposta a questa questione non è di

[23] Sul punto v. S. TOMMASI, Digital Services Act *e* Artificial Intelligence Act, *cit.*, p. 282; E. BIRRITTERI, *Contrasto alla disinformazione,* Digital Services Act *e attività di* private enforcement, *cit.*, p. 60 ss.; L. D'AGOSTINO, *Disinformazione e obblighi di* compliance *degli operatori del mercato digitale alla luce del nuovo* Digital Services Act, in *MediaLaws*, n. 2, 2023, p. 235 ss.

[24] Qualora vengano adottate restrizioni sui contenuti illegali, devono essere fornite agli utenti informazioni sull'uso di strumenti automatizzati utilizzati per adottare decisioni "ivi compresa l'informazione che indichi se la decisione sia stata adottata in merito a contenuti individuati o identificati per mezzo di strumenti automatizzati" (art. 17, par 3, lett. *c*).

[25] V. ancora S. TOMMASI, Digital Services Act *e* Artificial Intelligence Act, *cit.*, pp. 282-283, la quale evidenzia la carenza di adeguata attenzione in merito agli obblighi di formazione, assistenza e trasparenza delle figure dei moderatori.

[26] V. anche il considerando 70, che ne evidenzia il possibile "impatto significativo sulla capacità dei destinatari di recuperare e interagire con le informazioni online" e il "ruolo importante nell'amplificazione di determinati messaggi, nella diffusione virale delle informazioni e nella sollecitazione del comportamento online". Valga inoltre la pena di evidenziare come tali sistemi siano soggetti agli obblighi di trasparenza previsti dall'art. 27 del DSA, il quale impone la menzione dell'utilizzo di sistemi di raccomandazione nelle condizioni generali di contratto relative ai servizi delle piattaforme digitali e i relativi parametri di utilizzo, chiarendo "il motivo per cui talune informazioni sono suggerite al destinatario del servizio" e le funzionalità che consentono "di selezionare e modificare in qualsiasi momento l'opzione preferita". Sugli obblighi di trasparenza del DSA v. diffusamente S. TOMMASI, Digital Services Act *e* Artificial Intelligence Act, *cit.*, pp. 287-288.

pronta reperibilità, ma d'altro canto è di assoluta centralità. Infatti, a seconda della risposta, sarebbe possibile (o meno) imputare ai prestatori di servizi di intermediazione la responsabilità per eventuali contenuti illeciti da essi raccomandati, ancorché in maniera totalmente automatizzata.

Peraltro, il quadro normativo sui sistemi automatizzati di moderazione e raccomandazione è ulteriormente complicato dall'*AI Act*[27]. Infatti, entrambi questi sistemi – così come molti altri – devono rispettare anche alla disciplina dell'*AI Act* nella misura in cui essi rientrano nella definizione fornita dal suo art. 3, n. 1[28]. Secondo questa disposizione, la capacità di generare da un *input* ricevuto "decisioni" (ad esempio sui criteri per filtrare i contenuti moderati) e "raccomandazioni" rientra tra le caratteristiche di un "sistema di intelligenza artificiale", definito, appunto, come "un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'*input* che riceve come generare *output* quali previsioni, contenuti, *raccomandazioni* o *decisioni* che possono influenzare ambienti fisici o virtuali" (cors. agg.)[29].

Questo implica che i prestatori, quando usano sistemi automatizzati di moderazione o raccomandazione, oltre a dover sottostare agli obblighi del DSA, devono rispettare anche gli obblighi che l'*AI Act* impone ai c.d "*deployers*", ovvero quei soggetti, pubblici e privati, che fanno uso di sistemi di intelligenza artificiale[30].

Sul campo della comunicazione politica ed elettorale, in particolare, occorre tenere conto della classificazione fornita dall'allegato III dell'*AI Act*, il quale, al n. 8, lett. *b*, include tra i sistemi di intelligenza artificiale ad alto rischio anche quelli "destinati a essere utilizzati per influenzare l'esito di un'elezione o

[27] Per una interessante disamina filosofica si rimanda a L. FLORIDI, *The European Legislation on AI: a Brief Analysis of its Philosophical Approach*, in *Philosophy & Technology*, 2021, p. 215 ss.

[28] Si veda O. POLLICINO, P. DUNN, *Disinformazione e intelligenza artificiale*, *cit.*, p. xii ss.; S. TOMMASI, Digital Services Act *e* Artificial Intelligence Act, *cit.*, p. 281 ss.

[29] Il considerando n. 12 dell'*AI Act* chiarisce, in termini generali, l'importanza di una definizione chiara dei sistemi di intelligenza artificiale, in modo da assicurare certezza del diritto, mantenendo tuttavia un certo grado di flessibilità e adattabilità agli sviluppi tecnologici. Le caratteristiche basilari dei sistemi di intelligenza artificiale, che li distinguono dai *software* "tradizionali" vengono identificate nella "capacità inferenziale" (ossia la capacità di governare "un processo di ottenimento degli output, quali previsioni, contenuti, raccomandazioni o decisioni, che possono influenzare gli ambienti fisici e virtuali e alla capacità dei sistemi di IA di ricavare modelli o algoritmi, o entrambi, da input o dati"), nelle capacità di adattabilità e apprendimento automatico ("che imparano dai dati come conseguire determinati obiettivi e approcci basati sulla logica e sulla conoscenza"), nella variabilità dei livelli di autonomia di azione rispetto all'intervento umano, nell'eterogeneità delle funzioni svolte (che si ripercuote sugli output generati dal sistema, come "previsioni, contenuti, raccomandazioni o decisioni" e sui suoi obiettivi, che possono essere espliciti o impliciti).

[30] L'art. 3, n. 4 dell'*AI Act* definisce il "*deployer*", come "l'utilizzatore professionale" del sistema di IA, ossia "una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale. Diversamente il "*provider*" è il "fornitore" del sistema, cioè il soggetto che "che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio (…)" (art. 3, n. 3). Peraltro, come ricorda il considerando n. 13 dell'*AI Act*, non solo *deployers* e fornitori, ma anche altre persone possono essere interessate dal funzionamento di un dato sistema di intelligenza artificiale "a seconda del tipo di sistema di IA".

di un referendum o il comportamento di voto delle persone fisiche nell'esercizio del loro voto alle elezioni o ai referendum"[31].

Ne deriva l'applicabilità della regole che l'*AI Act* prevede per questo genere di sistemi, che includono sia il rispetto dei numerosi requisiti della sezione 2 del capo III[32], sia gli stringenti obblighi per i fornitori[33] e per i *deployers* (cioè, nello specifico, i prestatori di servizi digitali, come i gestori delle piattaforme, che utilizzano sistemi di IA)[34]. A questi obblighi si sommano inoltre i rigorosi doveri di trasparenza per fornitori e *deployers* di determinati sistemi di IA previsti dall'art. 50[35].

---

[31] Si tenga presente che l'*AI Act* calibra gli obblighi dei fornitori e degli utilizzatori dei sistemi di IA sulla base della classificazione del rischio: per i sistemi a rischio contenuto sono previsti obblighi meno stringenti rispetto ai sistemi ad alto rischio (art. 6); ove il rischio risulti intollerabile le pratiche di IA sono vietate (v. art. 5). La capacità di incidere sui processi democratici, come sottolinea G. ZACCARONI, *Intelligenza artificiale e principio democratico: riflessioni a margine dell'emersione di un quadro normativo europeo*, in *Quaderni AISDUE*, n. 2, 2024, p. 222 ss., giustifica l'inclusione di taluni sistemi di IA tra quelli ad alto rischio. V. inoltre G. FINOCCHIARO, *La proposta di Regolamento sull'Intelligenza Artificiale: il modello Europeo basato sulla gestione del rischio*, in *Il diritto dell'informazione e dell'informatica,* n. 2, 2022, p. 303 ss.; G. DE GREGORIO, P. DUNN, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *Common Market Law Review,* n. 2, 2022, p. 473 ss.

[32] L'*AI Act* prevede per i sistemi di IA ad alto rischio il rispetto di requisiti ampi e stringenti. Deve infatti essere garantita, a cura dei fornitori, la conformità ai requisiti normativi (art. 8.2), il rispetto di requisiti di qualità dei set di dati di addestramento dei sistemi nella loro governance e gestione con modalità adeguate alle finalità (art. 10), la redazione prima dell'immissione sul mercato di specifica documentazione tecnica e il relativo aggiornamento (art. 11), nonché, per l'intero ciclo di vita, il mantenimento e l'aggiornamento di un sistema di gestione dei rischi (art. 9), la registrazione automatica e la conservazione degli eventi riguardanti l'utilizzo, detti *log* (art. 12). Inoltre, durante l'utilizzo dei sistemi di IA ad alto rischio deve essere garantita la sorveglianza umana (art. 14) e il rispetto di requisiti di accuratezza, robustezza e cybersicurezza (art. 15), e di trasparenza e informazione nei confronti dei *deployers*, ai quali devono essere fornite adeguate istruzioni d'uso (art. 13).

[33] Gli articoli da 16 a 21 impongono obblighi ai fornitori dei servizi di IA che comprendono la predisposizione di un sistema di gestione della qualità "documentato in modo sistematico e ordinato" (art. 17), la conservazione della documentazione di cui all'art. 18 per dieci anni dopo l'immissione sul mercato a disposizione delle autorità competenti (oltre ai *log* – ove possibile – di cui all'art. 19), l'adozione delle misure correttive dell'art. 20 nel caso in cui un sistema di IA ad alto rischio immesso sul mercato non sia conforme, indagando le cause e informando le autorità competenti (con le quali sono comunque tenuti a collaborare nei termini previsti dall'art. 21). Inoltre, i fornitori di sistemi di IA ad alto rischio devono applicare una delle procedure illustrate all'art. 43 per dimostrarne la conformità di cui all'art. 47, rispettando altresì gli obblighi di marcatura CE (art. 48) e di registrazione (art. 49).

[34] Gli obblighi gravanti sui *deployers* dei sistemi ad alto rischio sono indicati all'art. 26 e all'art. 27. L'art. 26 prevede che essi debbano utilizzare i sistemi di IA ad alto rischio conformemente alle istruzioni dei fornitori, adottando idonee misure tecniche e organizzative, affidando l'obbligatoria sorveglianza umana a persone adeguatamente formate, monitorandone il funzionamento, conservando i relativi dati automaticamente generati e – per alcuni sistemi – presentando alle competenti autorità relazioni annuali. Si badi bene che il par. 10 dell'art. 26 cerca di sciogliere un nodo conflittuale di sovrapposizione con la normativa sui dati personali, prevedendo la prevalenza dell'art. 9 del GDPR e dell'art. 10 della direttiva 2016/680 quando sono trattate speciali categorie di dati come i dati biometrici. L'art. 27 dispone, in alcuni casi e solo per alcune categorie di *deployers* e/o di sistemi di IA ad alto rischio, l'obbligo di effettuare una dettagliata valutazione di impatto sui diritti fondamentali prima dell'utilizzo, i cui risultati devono essere notificati alle competenti autorità.

[35] La recente prassi, peraltro, evidenzia la possibile insorgenza di gravi problematiche in campo elettorale nell'ambito del rapporto tra DSA e *AI Act*, come emerge dall'indagine che la Commissione europea ha avviato nei confronti della società che gestisce la piattaforma di social network *TikTok*, a seguito dell'annullamento delle elezioni presidenziali rumene (v. al riguardo i comunicati stampa ufficiali della Commissione europea del 17 dicembre 2024 "*Commission opens formal proceedings against TikTok on election risks under the Digital Services Act*", disponibile all'indirizzo https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487 e il più recente del 15 maggio 2025 "*Commission preliminarily finds TikTok's ad repository in breach of the Digital Services Act*", disponibile all'indirizzo https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1223.

La frammentazione delle regole applicabili – che, come vedremo, per i settori di nostro interesse non si limita ai soli DSA e *AI Act*[36]– non agevola la composizione di un quadro normativo chiaro e, al contrario, diventa foriera di incertezze nella definizione degli obblighi e delle responsabilità dei prestatori di servizi digitali, soprattutto in ragione della grande eterogeneità di algoritmi che possono essere sfruttati dai sistemi di intelligenza artificiale per scopi molto diversificati.

2.2. Il Regolamento 2024/900 relativo alla trasparenza e al *targeting* della pubblicità politica (RPA): coordinamento con il DSA e con l'*AI Act*

La pubblicità politica è stata recentemente oggetto di un intervento legislativo dell'Unione attraverso il Regolamento 2024/900 relativo alla trasparenza e al *targeting* della pubblicità politica (d'ora innanzi *Regulation on Political Advertising* o *RPA*), che sarà applicabile a partire dal 10 ottobre 2025. Questo Regolamento si propone di disciplinare la pubblicità politica – e quindi anche i relativi aspetti di comunicazione – sia quando le attività sono svolte *offline*, con canali tradizionali, sia quando sono utilizzati strumenti digitali[37], riconoscendone la centralità per il corretto sviluppo dei processi democratici[38], anche nell'ottica di contrastare la disinformazione[39].

Proprio con riferimento alla comunicazione *online* si presentano problemi di coordinamento tra fonti. A questo riguardo occorre infatti tenere presente che l'utilizzo e il trattamento di dati personali in questo settore non è stato oggetto di specifiche disposizioni del GDPR[40] (che comunque continua a trovare applicazione nei limiti del relativo campo di applicazione e in assenza di prevalenti disposizioni speciali) e che il DSA, nel regolare all'art. 26 la pubblicità sulle piattaforme digitali, non tratta specificamente i contenuti di natura politica: il RPA si pone quindi come *lex specialis*.

In particolare, l'art. 26 DSA si limita ad introdurre genericamente l'obbligo di chiara ed inequivocabile identificazione del carattere pubblicitario di ogni comunicazione – di qualsiasi genere – presentata ad ogni

---

[36] V. ancora O. POLLICINO, P. DUNN, *Disinformazione e intelligenza artificiale*, *cit.*, p. xviii ss.

[37] Si pensi, ad esempio, a contenuti multimediali come fotografie, immagini e video con cui personaggi politici in prima persona o "*influencers*" di vario genere sponsorizzano attività e posizioni politiche o candidature su piattaforme digitali come i *social networks*.

[38] In questo senso v. L. CIANCI, *Il diritto ad essere informati alla prova delle strategie di* microtargeting *per la comunicazione politica*, in *Nomos*, n. 1, 2023, p. 1 ss.; G. STEGHER, *Da cittadini elettori a cittadini consumatori: osservazioni sull'importanza di regolare le campagne elettorali sui social media*, in *Nomos*, n. 1, 2023, p. 24.

[39] V. E. CATERINA, *Verso il nuovo regolamento Ue in materia di pubblicità politica: mercato delle idee o della propaganda?*, in *Quad. cost.*, n. 1, 2024, p. 209; C. MASSA, *Proposta di regolamento sulla pubblicità politica nell'UE: più trasparenza e meno* targeting, in *Quad. AISDUE*, n. 1, 2022, p. 363 ss.; E. STELLA, *La disciplina in materia di pubblicità politica del regolamento (Ue) 2024/900*, in *Eurojus.it*, 2024. Emblematico è il caso del recente annullamento delle elezioni presidenziali rumene, sul quale v., per tutti, D. VAIRA, Trick or t(h)reat*: disinformazione* online *e minacce ibride nel panorama europeo. Alcune considerazioni alla luce dell'annullamento delle elezioni in Romania*, in *SIDIBlog*, 29 dicembre 2024, nonché le puntuali riflessioni di F. ROSA, *L'annullamento delle elezioni presidenziali in Romania e la difficile difesa della democrazia*, in questo numero speciale.

[40] V. P. VILLASCHI, *The Regulation of Political Targeting in the Italian and European Union Legal Framework*, in *Riv. dir. int. priv. proc.*, n. 1, 2024, p. 137, il quale ricava la sostanziale inadeguatezza del GDPR a regolare l'utilizzo dei dati nella comunicazione politica in ragione del fatto che esso non è stato specificamente pensato per tale scopo.

singolo utente delle piattaforme, oltre al soggetto per conto del quale la pubblicità viene presentata (e, se differente, il soggetto che la finanzia), nonché le informazioni relative ai parametri utilizzati per determinare il destinatario e la loro modalità di modifica[41]. Gli utenti che diffondono "comunicazioni commerciali" sulla piattaforma devono altresì fornire un'apposita dichiarazione, della quale il gestore della piattaforma deve tener conto per segnalare a tutti gli altri utenti la natura commerciale dei contenuti.

La pubblicità di natura politica trova invece specifica disciplina nel RPA, che introduce mirati e più articolati obblighi al suo art. 6 (e seguenti)[42].

Quanto agli obblighi di trasparenza, ad esempio, gli artt. 9 e 10 del RPA, che si applicano anche alla pubblicità politica *offline*, prevedono la conservazione delle informazioni in appositi registri[43] e la loro trasmissione agli editori di pubblicità politica, ai fini dell'adempimento degli obblighi posti in capo ad essi. Inoltre, l'art. 11 impone obblighi di "etichettatura" dei messaggi di pubblicità politica, *online* e *offline*, più specifici e aderenti alla natura dei messaggi. In particolare, a norma dell'art. 11, si richiede la chiara ed inequivoca indicazione della natura di pubblicità politica del messaggio, del finanziatore, dell'elezione o del referendum cui si riferisce il messaggio, l'eventuale utilizzo di tecniche di *targeting* , nonché lo specifico avviso di trasparenza contenente le minuziose e dettagliate informazioni previste dall'art. 12. Ulteriori obblighi di trasparenza comprendono l'obbligo di predisporre relazioni periodiche sui servizi di pubblicità politica che indichino gli importi fatturati e l'uso di tecniche di *targeting* (art. 14) e meccanismi per segnalare la mancata conformità dei messaggi di pubblicità politica al Regolamento (art. 15), oltre all'obbligo di trasmissione delle informazioni rilevanti alle autorità competenti (art. 16) e ad altri soggetti interessati (art. 17).

Un aspetto di primaria importanza ai fini del coordinamento tra fonti riguarda altresì la disciplina del *targeting online* mediante l'utilizzo di strumenti automatizzati[44], che nel campo della comunicazione politica

[41] Strumento tipicamente utilizzato sulle piattaforme per ottemperare a quest'obbligo è l'indicazione del contenuto precedentemente visualizzato dall'utente dal quale è stato ricavato il suo interesse per un dato genere di prodotti o servizi. Si badi bene, tuttavia, che l'art. 26, par. 3, del DSA vieta espressamente le attività di profilazione (definite dall'art. 4.4 del GDPR come "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica", incluse "preferenze personali" e "interessi") aventi ad oggetto le categorie speciali di dati di cui all'art. 9, par. 1 del GDPR (come ad esempio l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose, l'orientamento sessuale, dati biometrici e relativi alla salute). Il divieto di profilazione viene ribadito anche nel PRA, all'art. 18, di cui diremo *infra*.

[42] Fatta salva la facoltà per la Commissione europea di elaborare "orientamenti comuni" chiarificatori, a norma dell'art. 8 del PRA, ai fini della determinazione della natura di pubblicità politica di un messaggio occorre tener conto del suo contenuto, del soggetto che lo finanzia, della lingua utilizzata, del contesto e del periodo di trasmissione, dei mezzi utilizzati per predisporlo e diffonderlo, dei suoi destinatari e del suo obiettivo.

[43] Con specifico riguardo per la pubblicità *online*, si veda anche l'art. 13 relativo al "registro europeo dei messaggi di pubblicità politica online" istituito dalla Commissione europea, contenente "tutti i messaggi di pubblicità politica online pubblicati nell'Unione o diretti a cittadini o residenti dell'Unione".

[44] Sul tema, con riferimento alla comunicazione politica, v. L. CIANCI, *Il diritto ad essere informati*, *cit.*, p. 15 ss.

ha già dato luogo ad una casistica significativa di cui si è interessata la Commissione europea[45]. Infatti, alla disciplina introdotta dal DSA (specialmente in relazione agli strumenti automatizzati di raccomandazione), che già deve affrontare il problema del coordinamento con le disposizioni dell'*AI Act*[46], si sovrappongono, per la pubblicità politica, le disposizione degli articoli 18 e 19 del RPA.

L'art. 18 ammette l'utilizzo di tecniche di *targeting* in ambito di pubblicità politica *online* solo a condizione che il titolare del trattamento dei dati abbia raccolto i dati personali presso l'interessato, il quale deve aver prestato il proprio consenso esplicito al trattamento a fini di pubblicità politica[47]. Inoltre, analogamente a quanto previsto dal DSA, anche secondo il RPA è vietata la "profilazione" sulla base delle categorie particolari di dati di cui all'art. 9.1 del GDPR e all'art. 10.1 del Regolamento (UE) 2018/1725[48].

L'art. 19 introduce obblighi addizionali di trasparenza per i titolari del trattamento dei dati che si avvalgano di tecniche di *targeting* politico *online* riguardanti, anzitutto, l'adozione, l'applicazione e la divulgazione pubblica di un documento di strategia interna sulle tecniche utilizzate alle quali devono vincolarsi per almeno sette anni; è inoltre richiesta la conservazione di appositi registri, la trasmissione di informazioni sul funzionamento delle tecniche di *targeting* ai soggetti interessati specificando l'eventuale utilizzo di sistemi di intelligenza artificiale, la preparazione annuale di una procedura di valutazione interna dei rischi (da rendere pubblica), nonché l'indicazione dei riferimenti sui mezzi effettivi a disposizione dell'interessato per l'esercizio dei propri diritti previsti dal GDPR e dal Regolamento (UE) 2018/1725.

L'intreccio normativo che ne deriva, anche in questo settore, è foriero di un alto grado di complessità che rende difficoltosa la delimitazione dell'estensione degli obblighi dei prestatori e dei diritti degli utenti, sempre più inclini al rischio di violazioni[49]. Come vedremo, tuttavia, non solo nel campo della comunicazione politica, ma anche in quello della comunicazione commerciale, le cui tecniche sono sempre più spesso utilizzate anche in settori non propriamente economici, il quadro normativo è ricco di problemi di sovrapposizioni normative di primaria rilevanza.

---

[45] Per una puntuale ricostruzione della recente casistica v. L. PIGNA, Microtargeting *politico nell'Unione europea: alcune riflessioni alla luce della prassi istituzionale e della regolamentazione più recenti*, in *Ordine internazionale e diritti umani*, 2025, p. 286 ss.

[46] V. *supra*, in questo paragrafo.

[47] Ai sensi del par. 4 dell'art. 18, all'interessato non può essere richiesto il consenso "se ha già indicato con mezzi automatizzati che non acconsente al trattamento dei dati a fini di pubblicità politica, a meno che la richiesta non sia giustificata da un mutamento sostanziale delle circostanze" (lett. *a*) e deve essergli offerta "un'alternativa equivalente per l'utilizzo del servizio online senza ricevere pubblicità politica" nell'ipotesi in cui non intenda prestare il proprio consenso. Va inoltre segnalato come le tecniche di *targeting* in ambito di pubblicità politica non siano ammesse, ai sensi del par. 2 dell'art. 18, nei confronti di soggetti che anagraficamente devono ancora attendere un anno per ottenere la capacità di esercizio del diritto di voto secondo le norme nazionali.

[48] Si consideri comunque che le disposizioni dell'art. 18 non si applicano per le comunicazioni effettuate da partiti e organizzazioni politiche senza scopo di lucro nei confronti dei propri membri o ex membri, connesse alle attività politiche, a condizione che vengano rispettate le prescrizioni dell'art. 18.4.

[49] Cfr. C. CARUSO, *Il tempo delle istituzioni di libertà. Piattaforme digitali, disinformazione e discorso pubblico europeo*, in *Quad. cost.*, 2023, p. 543 ss.

3. Interferenze normative nel settore della "comunicazione commerciale"

Il settore della "comunicazione commerciale" è di strategico interesse perché connotato dall'intrinseca ambivalenza tra la sua dimensione pubblica e quella interprivata. Infatti, se da un lato gli aspetti commerciali sono spesso legati ai rapporti tra soggetti privati, dall'altro lato la loro regolamentazione non può prescindere dal coinvolgimento delle autorità pubbliche, anche in ragione dell'incidenza sul generale assetto dei mercati e dei correlati interessi economici generali. Occorre inoltre considerare che in ambito commerciale possono emergere situazioni che interessano anche diritti fondamentali, come, ad esempio, la libertà di iniziativa economica, il diritto di proprietà, la tutela dei dati personali e la libertà di manifestazione del pensiero[50].

Per tutte queste ragioni prenderemo ora in esame alcune interferenze normative nel campo della comunicazione commerciale, che comprovano l'esistenza di un quadro normativo altamente complesso che non contribuisce a rendere districabili le gravi questioni problematiche che frequentemente si presentano, come quelle di cui diremo, a titolo esemplificativo, nei paragrafi seguenti.

3.1. DSA e direttiva sui diritti d'autore *online* (direttiva 2019/790)

In campo commerciale, la disinformazione può essere strumento di pratiche concorrenziali sleali, ad esempio attraverso la violazione di diritti d'autore e di proprietà intellettuale.

Questo genere di violazioni si verifica sempre più frequentemente attraverso piattaforme digitali, che in ragione della capacità di diffusione immediata e generalizzata dei contenuti e delle informazioni possono amplificare le conseguenze negative per i titolari dei relativi diritti.

Proprio per questa ragione il legislatore europeo ha adottato la direttiva 2019/790[51] sul diritto d'autore e sui diritti connessi nel mercato unico digitale (direttiva sui diritti d'autore *online*), con la quale si è tentato di tener conto della duplice natura dei diritti d'autore: da un lato, estensione materiale del diritto alla proprietà privata[52], la cui violazione può produrre indebiti vantaggi concorrenziali e falsare l'assetto del mercato; dall'altro, espressione morale di attività e creazioni intellettuali che rilevano anche sotto il profilo della libertà di espressione[53].

---

[50] V. oltre par. 3.1.

[51] Direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE.

[52] Vedi al riguardo anche il par. 2 dell'art. 17 della Carta dei diritti fondamentali dell'Unione europea, il quale dispone espressamente che "[l]a proprietà intellettuale è protetta", includendola nell'articolo dedicato al diritto di proprietà; nonché la giurisprudenza della Corte europea dei diritti dell'uomo sull'art. 1 del Protocollo addizionale n. 1 (v. la prima affermazione nel caso *Smith Kline e French Laboratories LTD c. Paesi Bassi*, ric. 12633/87, dec. 4 ottobre 1990, alla quale è seguito un ondivago orientamento giurisprudenziale fino alla definitiva conferma avuta con la sentenza *Anheuser-Busch Inc. c. Portogallo*, ric. 73049/01, sent. 11 gennaio 2007, par. 72).

[53] V. G.M. RICCIO, *Diritto d'autore,* Digital Services Act *e la fragilità teorica dietro i diritti fondamentali*, in *Diritti umani e diritto internazionale*, n. 1, 2023, p. 100 ss., nonché la giurisprudenza della Corte di Strasburgo, *Ashby Donald e altri c. Francia*, ric.

In questo contesto, quando vengono sfruttate piattaforme digitali, le disposizioni della direttiva vanno coordinate con quelle del *Digital Services Act*[54]. Ad esempio, l'articolo 17 della direttiva sui diritti d'autore *online* disciplina l'utilizzo di contenuti protetti ad opera di prestatori di servizi di condivisione, prevedendo l'obbligo di autorizzazione preventiva da parte dei titolari dei diritti di proprietà intellettuale. Lo stesso articolo precisa che la limitazione di responsabilità prevista dall'art. 14 della direttiva sul commercio elettronico non si applica ai prestatori di servizi digitali che mettono a disposizione *online* opere protette da diritti d'autore senza autorizzazione[55], a meno che non venga fornita prova della sussistenza delle circostanze di cui alle lett. *a*, *b* e *c* del par. 4 dell'art. 17[56]. Il riferimento alla direttiva sul commercio elettronico deve ora essere inteso all'art. 6 del DSA (come prevede il suo art. 89), che, come abbiamo visto[57], esclude la responsabilità dei prestatori di servizi di memorizzazione di informazioni per i contenuti caricati dagli utenti, salvo conoscenza dell'illegalità degli stessi o mancata rimozione immediata[58].

Tuttavia, chiarisce ulteriormente l'art. 17, par. 3, della direttiva, tale eccezione al principio di generale esenzione di responsabilità viene meno, rendendolo dunque applicabile, se le finalità delle attività dei

36769/08, sent. 10 gennaio 2013, par. 40 ss. e *Neij e Sunde Kolmisoppi c. Svezia*, ric. 40397/12, dec. 19 febbraio 2013). Sul tema v. anche G.M. RUOTOLO, *Scritti*, *cit.*, p. 186 ss.

[54] Anche se rappresenta un problema ancora aperto, non ci occuperemo in questa sede, per ragioni di spazio e pertinenza, della questione dei diritti d'autore sulle opere prodotte dai sistemi di IA generativa, comparsi più di recente e causa di emendamento dell'*AI Act* durante il suo *iter* di approvazione: in tema v. comunque gli spunti di riflessione di F. POSTERARO, *Il copyright al tempo dell'IA generativa*, in *MediaLaws*, n. 2, 2023, p. 11 ss.

[55] In tema v. G.M. RUOTOLO, *La responsabilità per la diffusione online di informazioni tra Artificial Intelligence Act e DSA*, in *Quaderni di SIDIBlog*, 2023, pp. 410-411, nonché Id., *Scritti*, *cit.*, p. 197 ss.; Id. *A Season in the Abyss. Il nuovo copyright UE tra libertà di informazione, diritti fondamentali e mercato unico digitale*, in *Il diritto dell'Unione europea*, n. 2, 2019, p. 369 ss.

[56] Al fine di poter invocare la limitazione di responsabilità il prestatore deve dimostrare di "*a)* aver compiuto i massimi sforzi per ottenere un'autorizzazione, e *b)* aver compiuto, secondo elevati standard di diligenza professionale di settore, i massimi sforzi per assicurare che non siano disponibili opere e altri materiali specifici per i quali abbiano ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti; e in ogni caso, *c)* aver agito tempestivamente, dopo aver ricevuto una segnalazione sufficientemente motivata dai titolari dei diritti, per disabilitare l'accesso o rimuovere dai loro siti *web* le opere o altri materiali oggetto di segnalazione e aver compiuto i massimi sforzi per impedirne il caricamento in futuro conformemente alla lettera *b)*".

[57] V, *supra* par. 2.1.

[58] La Corte di giustizia, attraverso la propria copiosa giurisprudenza in materia, ha tentato di chiarire alcune aspetti critici dei vigenti obblighi, in particolare in relazione ai criteri che i prestatori di servizi digitali devono seguire quando utilizzano sistemi di filtraggio preventivo dei contenuti lesivi di diritti d'autore. V. segnatamente la sentenza nel caso C-275/06, *Productores de Música de España (Promusicae) contro Telefónica de España SAU*, 29 gennaio 2008 e, soprattutto, le sentenze C-70/10, *Scarlet Extended SA contro Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 novembre 2011, par. 43 ss. e C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) contro Netlog NV*, 16 febbraio 2012, par. 43 ss., con le quali la Corte ha escluso che gli obblighi di sorveglianza implichino la predisposizione di un sistema di filtraggio, perché trattasi di sistemi informatici permanenti, tanto costosi e complessi da incidere negativamente sulla libertà di iniziativa economica (v. giurisprudenza citata poc'anzi), ma anche sulla libertà di espressione (v. C-160/15, *GS Media BV contro Sanoma Media Netherlands BV e a.*, 8 settembre 2016, par. 31 ss.). Di recente, peraltro, con la sentenza C-401/19, *Polonia c. Parlamento e Consiglio*, 26 aprile 2022, la Corte ha respinto il ricorso presentato dalla Polonia al fine di ottenere l'annullamento delle lett. *b* e *c* del par. 4 dell'art. 17 della direttiva sui diritti d'autore *online* per violazione del diritto alla libertà di espressione tutelato dall'art. 11 della Carta dei diritti fondamentali dell'Unione europea e dall'art. 10 della CEDU.

prestatori di servizi di condivisione di contenuti *online* "non rientrano nell'ambito di applicazione della [presente] direttiva".

Il rapporto tra le due fonti è molto contorto e sicuramente la formulazione delle disposizioni, tra responsabilità, esenzione di responsabilità, eccezioni all'esenzione e esclusione dell'eccezione dell'esenzione, non contribuisce a facilitarne l'applicazione, l'interpretazione e a rendere chiaro il quadro normativo[59].

A ciò si aggiunga, inoltre, la necessità di coordinamento di alcuni obblighi, come quelli di informazione, previsti sia dal DSA sia dalla direttiva sui diritti d'autore *online*: gli obblighi previsti dall'art. 14 del DSA, che trovano applicazione per tutti i diritti fondamentali – inclusi quelli correlati al *copyright*[60] – sono affiancati dagli obblighi previsti dall'art. 17, par. 9, della direttiva, che impone ai *providers* di informare i propri utenti, all'interno delle condizioni contrattuali, "della possibilità di utilizzare opere e altri materiali conformemente alle eccezioni o limitazioni al diritto d'autore e ai diritti connessi previste dal diritto dell'Unione"[61].

3.2. *Digital Markets Act*, diritto antitrust e GDPR

L'analisi delle possibili interferenze nell'ambito della disinformazione commerciale non può trascurare l'impatto che il *Digital Markets Act* (DMA)[62] ha avuto sulla normativa antitrust[63]. Questo Regolamento, approvato contestualmente al DSA[64], si caratterizza per aver introdotto più stringenti obblighi per i c.d. *gatekeepers*[65], imprese che, ai sensi dell'art. 3, "hanno un impatto significativo sul mercato interno",

[59] Sulla complessità del quadro normativo dell'Unione in materia di diritti d'autore v. anche C. ANGELOPOULOS, J.P. QUINTAIS, *Fixing Copyright reform: A better solution to online infringement*, in *Journal of Intellectual Property, Information Technology, and Electronic Commerce Law*, n. 2, 2019, p. 147 ss.

[60] V. in proposito G.M. RICCIO, *Diritto d'autore,* Digital Services Act *e la fragilità teorica dietro i diritti fondamentali*, *cit.*, pp. 113-114, il quale nota come l'art. 14 del DSA preveda l'obbligo di inserire nelle condizioni generali di servizio informazioni sulle restrizioni imposte dai prestatori agli utenti in relazione all'uso dei servizi (art. 14, par. 1, 2 e 3), applicandole nel rispetto dei diritti e degli interessi degli utenti, compresa la libertà di espressione e il pluralismo dei media (art. 14, par. 4).

[61] Sull'impatto che i nuovi obblighi del DSA potrebbero avere sulla tutela dei diritti di proprietà intellettuale v., con opinione critica sulla calibrazione degli obblighi sulla base della dimensione dei prestatori di servizi digitali, C. A. DE MICHELIS, *Il* Digital Services Act*: i nuovi obblighi volti a migliorare la lotta alla contraffazione e i temi aperti*, in. *Dir. ind.*, n. 2, 2022, p. 171 ss.

[62] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali - DMA).

[63] V. sin d'ora P. AKMAN, *Regulating Competition in Digital Platform Markets: a Critical Assessment of the Framework and Approach of the EU Digital Markets Act*, in *European Law Review,* n.1, 2022, p. 85 ss.; A. ANDREANGELI, *The Digital Markets Act and the Enforcement of EU Competition Law: Some Implications for the Application of Articles 101 and 102 TFEU in Digital Markets*, in *European Competition Law Review*, n. 11, 2022, p. 496 ss.

[64] V. M. EIFERT, A. METZGER, H. SCHWEITZER, G. WAGNER, *Taming the giants: The DMA/DSA package*, in *Common Market Law Review*, n. 4, 2021, p. 987 ss.

[65] V. P. AKMAN, *Regulating Competition in Digital Platform Markets, cit.*, p. 85 ss.; M. MAGGIORE, *Il Digital Markets Act*, in M. MAGGIORE (a cura di), *Il commercio elettronico*, *cit.*, p. 180 ss.

forniscono un "servizio di piattaforma di base che costituisce un punto di accesso (*gateway*) importante affinché gli utenti commerciali raggiungano gli utenti finali" e detengono "una posizione consolidata e duratura, nell'ambito delle proprie attività (…)"[66], in modo da garantire mercati digitali equi e contendibili[67].

Infatti, l'adozione del DMA è avvenuta sulla base della consapevolezza che alcuni operatori commerciali del settore digitale sono in grado di influenzare le condizioni di accesso al mercato e la formazione di oligopoli, anche grazie al possesso o alla disponibilità di una enorme mole di dati[68].

Proprio per questo motivo, tra gli obblighi autonomamente applicabili ai *gatekeepers* figurano anche obblighi concernenti l'utilizzo di dati nei mercati digitali[69]: a questo proposito si possono profilare sovrapposizioni normative[70], ad esempio, nell'ambito di campagne o singole condotte di disinformazione e "diffamazione" commerciale *online*, che possono violare contestualmente una pluralità di normative, come il DMA, il GDPR e il generale diritto antitrust[71]. Si presenta così il rischio di violazione del *ne bis in idem*[72] e di difficoltà nell'individuazione delle autorità competenti ad irrogare sanzioni, a trattare i reclami o a pronunciarsi su ricorsi e risarcimenti.

---

66 Il par. 2 dell'art. 3 introduce delle soglie volte a determinare il soddisfacimento dei requisiti, che comprendono il fatturato annuo nell'Unione, il numero complessivo di utenti finali e il numero di utenti commerciali attivi stabiliti o situati nell'Unione. Attualmente, la Commissione europea ha individuato sette *gatekeepers*, cioè Amazon, Alphabet (Google), Apple, ByteDance (TikTok), Meta (Facebook, Instagram, WhatsApp), Microsoft e Booking (v. digital-markets-act.ec.europa.eu/gatekeepers_en). Sulla designazione dei *gatekeepers* v. M. MAGGIORE, *Il Digital Markets Act*, *cit.*, p. 174.

67 P. MANZINI, *Equità e contendibilità dei mercati digitali: il* Digital Markets Act, in G. CAGGIANO, G. CONTALDI, P. MANZINI (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Cacucci, Bari, 2021, p. 99 ss.; L.J. HOFFMAN, *Fairness in the Digital Markets Act*, in *European Papers*, n. 1, 23, p. 17 ss.; R. CAFARI PANICO, *Il DMA nel prisma della strategia digitale dell'UE: la scelta europea e la competizione fra sistemi*, in *Papers di diritto europeo*, n. 2, 2023, p. 159 ss.

68 R. CAFARI PANICO, *Il DMA nel prisma della strategia digitale dell'UE*, *cit.*, p. 164; M. MIDIRI, *Privacy e antitrust: una risposta ordinamentale ai Tech Giant*, in *federalismi.it*, n. 14, 2020, p. 217 ss.

69 Si vedano, ad esempio, gli obblighi riguardanti l'utilizzo dei dati previsti dall'art. 5.2 del DMA, il divieto di impedire agli utenti di offrire gli stessi prodotti o servizi attraverso differenti canali (art. 5.3) e il divieto di impedire comunicazioni. promozioni di offerte e la conclusione di contratti con gli utenti acquisiti attraverso i servizi del *gatekeeper* (art. 5.4). Inoltre, sono previsti numerosi obblighi in materia di trasparenza (art. 6) e altri riguardanti l'interoperabilità dei servizi di comunicazione interpersonale (art. 7). L'elenco è arricchito da molti altri obblighi, come quelli sulle relazioni (art. 11), obblighi antielusione (art. 13), obblighi di informazione (artt. 14-15) e di cooperazione (art. 37 ss.).

70 V. G.M. RUOTOLO, *Mercati e servizi digitali in Europa*, *cit.*, p. 72 ss.

71 Quanto alle sovrapposizioni tra diritto antitrust e *data protection* v. il tentativo di integrazione recentemente proposto dalla Corte di Giustizia con la sentenza nel caso C-252/12, *Meta Platforms Inc. e a. contro Bundeskartellamt*, 4 luglio 2023, sulla quale v. G. D'IPPOLITO, Data economy*: la Corte di giustizia precisa il rapporto tra concorrenza e protezione dei dati personali e le norme sulla pubblicità personalizzata*, in *MediaLaws*, n. 2, 2023, p. 324 ss. Cfr. altresì G.M. RUOTOLO, *Scritti*, *cit.*, p. 148 ss.

72 Tale rischio è espressamente contemplato dal considerando 86 del DMA, in accordo al quale è opportuno che ammende e penalità di mora per la violazione degli obblighi normativi siano di livello adeguato, soggette a ragionevoli termini di prescrizione, e la loro applicazione avvenga "conformemente ai principi di proporzionalità e *ne bis in idem*"; più nello specifico viene segnalato che "[è] opportuno che la Commissione e le pertinenti autorità nazionali coordinino i loro sforzi di applicazione al fine di garantire il rispetto di tali principi. In particolare, la Commissione dovrebbe tenere conto di eventuali ammende e penalità irrogate alla stessa persona giuridica per gli stessi fatti mediante una decisione definitiva nei procedimenti relativi a una violazione di altre norme dell'Unione o nazionali, in modo da garantire che l'importo complessivo delle ammende e delle penalità irrogate corrisponda alla gravità delle infrazioni commesse". Sul

Se, da un lato, l'introduzione di specifici obblighi in materia di concorrenza è senz'altro giustificata dal fatto che le regole sull'antitrust sono state pensate per far fronte ai problemi della *digital economy*[73], dall'altro lato è irrinunciabile prevedere adeguate forme di coordinamento con gli strumenti legislativi che si occupano specificamente del settore[74].

La risoluzione dei potenziali conflitti tra norme incontra vari ostacoli. Il primo riguarda la difficile coesistenza degli obblighi del DMA con la generale disciplina antitrust, nonché il rapporto tra DMA e GDPR[75]. A questo proposito il considerando 12 del DMA afferma che esso non intende pregiudicare l'applicazione del GDPR e coerentemente l'art. 8, par. 1, impone ai *gatekeepers* l'obbligo di assicurare la conformità, tra le altre, al GDPR.

Anche se gli obblighi del GDPR sembrerebbero quindi prioritari, in realtà alcune disposizioni del DMA rafforzano e integrano gli standard di tutela predisposti dal GDPR, ai quali non è pensabile rinunciare per non sminuire la portata generale del DMA[76].

Inoltre, occorre considerare che il DMA non pone una disciplina integralmente sovrapponibile alle normative antitrust o al GDPR, dovendo piuttosto integrare le loro disposizioni[77] nella complessa cornice normativa esistente. Ciò impone di procedere alla risoluzione delle potenziali antinomie con un approccio

punto v. N.M.F. FARAONE, *Della serie "a volte ritornano" (o non se ne sono mai veramente andati): il principio del* ne bis in idem *alla prova delle piattaforme digitali*, in *federalismi.it*, n. 6, 2023, p. 69 ss.. Quanto alle potenziali violazioni del principio nel rapporto tra DSA e DMA v. G.M. RUOTOLO, Digital Services Act *e* Digital Markets Act, *cit.*, p. 229.

[73] G. CONTALDI, *Il DMA (*Digital Markets Act*) può contribuire alla protezione dei dati degli utenti online?*, in *Diritti umani e diritto internazionale*, n. 1, 2023, pp. 81-82, il quale ne identifica gli elementi di peculiarità nel fatto che molto spesso si tratta di prestazioni a titolo gratuito, il cui mercato rilevante è difficilmente individuabile, così come l'accertamento dell'esistenza di pratiche concordate e posizioni dominanti, con la conseguenza che i "rimedi tradizionali" possono facilmente risultare inadeguati. Nello stesso senso v. anche R. CAFARI PANICO, *Il DMA nel prisma della strategia digitale dell'UE*, *cit.*, pp. 164-165; in tema si segnala altresì P. MANZINI, *Equità e contendibilità dei mercati digitali*, *cit.*, p. 100 ss.

[74] A. MANGANELLI, *Il regolamento EU per i mercati digitali: ratio, criticità e prospettive di evoluzione*, in *Mercato Concorrenza Regole*, n. 3, 2021, p. 486 ss.; M. LIBERTINI, *Il regolamento europeo sui mercati digitali e le norme generali in materia di concorrenza*, in *Rivista trimestrale di diritto pubblico*, n. 4, 2022, p. 1072 ss. Per una rilettura "costituzionalmente orientata" del diritto della concorrenza v. G. PITRUZZELLA, *Diritto costituzionale e diritto della concorrenza: c'è dell'altro oltre l'efficienza economica?*, in *Quad. cost.*, n. 3, 2019, p. 579 ss., nonché, con specifico riguardo per la dimensione "costituzionale" del DMA, A. IANNOTTI DELLA VALLE, *Il* Digital Markets Act *e il ruolo dell'Unione europea verso un costituzionalismo digitale*, in *Giur. cost.*, n. 3, 2022, p. 1867 ss.

[75] Si noti che, pur avendo chiara rilevanza anche nell'ambito della concorrenza, il DMA non trova la propria base giuridica nelle norme dei Trattati sulla concorrenza (artt. 101, 102, 103 TFUE), bensì sull'art. 114 TFUE, su cui è fondata la competenza concorrente dell'Unione nel ravvicinamento delle legislazioni degli Stati membri aventi ad oggetto "l'instaurazione ed il funzionamento del mercato interno". Sul punto v. G. COLANGELO, *The European Digital Markets Act and antitrust enforcement:* a liaison dangereuse, in *European Law Review*, n. 5, 2022, p. 597 ss. Cfr. altresì M. POLO, A. SASSANO, *DMA: Digital Markets Act o Digital Markets Armistice?*, in *Mercato Concorrenza Regole*, n. 3, 2021, p. 520 ss.

[76] V. G. CONTALDI, *Il DMA (*Digital Markets Act*)*, *cit.*, pp. 90-91, il quale deduce che "svariati obblighi imposti ai *gatekeepers* dal regolamento si configurano, in realtà, quali specificazione di determinate prerogative degli utenti già previste del GDPR", come, ad esempio, la portabilità dei dati (art. 6, par. 9, DMA).

[77] V. F. BUONOMENNA, *Verso la «cittadinanza digitale» dell'Unione europea*, in A. DI STASI, M.C. BARUFFI, L. PANELLA (a cura di), *Cittadinanza europea e cittadinanza nazionale. Sviluppi normativi e approdi giurisprudenziali*, Editoriale Scientifica, Napoli, 2023, pp. 612-613; R. CAFARI PANICO, *Il DMA nel prisma della strategia digitale dell'UE*, *cit.*, p. 164.

caso per caso: d esempio, gli obblighi previsti dagli art. 5 e 6 del DMA si pongono come obblighi supplementari, che mirano ad anticipare la tutela prevenendo possibili condotte anticoncorrenziali[78].

Tuttavia, non sempre il coordinamento e l'eventuale integrazione delle disposizioni tra le diverse fonti è di semplice esecuzione, soprattutto alla luce della costante evoluzione dei servizi erogati dai prestatori di servizi digitali, con la conseguenza che chiarezza, accessibilità e efficacia della disciplina applicabile ne risentono negativamente.

Inoltre, anche sotto il profilo sanzionatorio e su quello dei rimedi a disposizione degli utenti si presentano gravi problematicità, soprattutto in relazione alla determinazione delle autorità competenti ad irrogare sanzioni, ad adottare provvedimenti di contrasto e repressione di condotte illecite e a garantire la tutela dei diritti degli utenti. Si pensi, ad esempio, al riparto di competenza tra le autorità nazionali per la concorrenza e la Commissione europea, in caso di pratiche anticoncorrenziali derivanti da condotte diffamatorie o da campagne di disinformazione: nonostante la centralità del ruolo assunto in questo campo dalle autorità nazionali della concorrenza, con il DMA si è però consolidata la controtendenza all'accentramento di poteri in mano alla Commissione europea[79], complicando le attività di cooperazione e collaborazione.

Analogamente, i problemi di cooperazione e riparto di competenza – nonché il conseguente rischio di violazione del principio del *ne bis in idem* o di errori nell'individuazione delle autorità meglio posizionate per adottare le misure più efficaci – riguardano la potenziale concorrenza tra le autorità indipendenti istituite dal GDPR, a livello nazionale ed europeo[80].

Tutto ciò senza dimenticare che anche nello spazio digitale permangono problemi di localizzazione dei rapporti e applicazione dei criteri di competenza territoriale per individuare le autorità competenti a livello nazionale tra i vari Stati membri.

---

[78] Sulla complementarità dell'approccio "*ex ante regulation*" del DMA con la normativa antitrust e *data protection* v. A. LICASTRO, Meta Platforms Inc., già Facebook Inc. v. Bundeskartellamt*: la Corte di Giustizia dell'Unione Europea apre (finalmente) all'integrazione fra diritto antitrust e* data protection, in *Rivista della Regolazione dei Mercati*, n. 2, 2023, p. 503 ss., in commento alla citata sentenza nel caso C-252/12, *Meta Platforms Inc.*, *cit.*

[79] Ciò, secondo R. CAFARI PANICO, *Il DMA nel prisma della strategia digitale dell'UE*, *cit.*, pp. 166-168, è dovuto al fatto che la base giuridica risiede nell'art. 114 TFUE e non negli articoli sulla concorrenza. Su questo aspetto v., in particolare, I. MAHER, M. HOSSEINI, *Cooperation between National Competition Authorities: An overview of EU and national case law*, in *e-Competitions Concurrences*, 2024, p. 1 ss., anche per i dettagliati riferimenti casistici e giurisprudenziali. In tema v. altresì I. MAHER, *Regulatory design in the EU Digital Markets Act: no solo run for the European Commission*, in *Journal of Antitrust Enforcement*, n. 2, 2024, p. 273 ss.

[80] R. CAFARI PANICO, *Il DMA nel prisma della strategia digitale dell'UE*, *cit.*, p. 170; C. PERARO, *Quando la violazione della privacy costituisce un illecito antitrust: quali rimedi nell'ordinamento UE?*, in *Eurojus*, n. 3, 2023, p. 54.

4. Conclusioni

Gli illustrati spunti di riflessione sulla disinformazione in campo politico e commerciale, proposti a titolo esemplificativo per comprovare l'esistenza di alcuni potenziali conflitti tra norme dell'Unione, fanno parte di un elenco incompleto ed in continuo ampliamento[81].

La complessità del quadro normativo è idonea a produrre conseguenze negative sull'effettività della tutela dei diritti, in ragione dell'accrescimento della complessità nel coordinamento dei meccanismi di protezione e dei rimedi a disposizione dei cittadini[82], nonché nel riparto di competenza, per materia e per territorio, delle autorità amministrative e giurisdizionali competenti, peraltro con rischio di interpretazioni divergenti su principi cardine e di violazione del principio del *ne bis in idem*.

Dall'affermazione degli operatori commerciali nel settore digitale sono nati nuovi servizi e schemi commerciali basati sull'utilizzo di piattaforme digitali che hanno richiesto l'adozione di nuovi atti legislativi al fine di tenere conto delle innovazioni digitali nello scenario economico internazionale: le nuove esigenze che si sono profilate erano sconosciute alle tradizionali forme imprenditoriali a cui si riferivano gli strumenti legislativi europei.

Tuttavia, è inevitabile prendere consapevolezza che le fattispecie digitali si muovono troppo rapidamente e costringono all'analisi continuativa non solo della disciplina di uno specifico genere di rapporti, ma anche di tutti gli altri ambiti che possono essere indirettamente influenzati[83]. La sovrapposizione di discipline richiede un'attenta opera di applicazione e interpretazione di regimi giuridici tra loro in concorrenza e l'adattamento di istituti che si applicano in contesti diversi, con costante opera di coordinamento[84].

Peraltro, come autorevolmente osservato nel Rapporto richiesto dalla Commissione europea *The Future of European Competitiveness*[85], l'eccesso di regolazione nel settore dei mercati digitali ("legislative activity has

[81] Il quadro normativo è ulteriormente complicato dalla necessità di determinare gli spazi residui di applicazione per i diritti nazionali, applicabili secondo le norme di conflitto dell'Unione sia in materia contrattuale – attraverso i criteri del Regolamento n. 593/2008 sulla legge applicabile alle obbligazioni contrattuali (Regolamento Roma I) – ma soprattutto extracontrattuale (si pensi a violazioni di diritti della personalità o atti di concorrenza sleale, la cui disciplina nelle situazioni transfrontaliere viene designata attraverso i criteri del Regolamento n. 864/2007 sulla legge applicabile alle obbligazioni extracontrattuali (Regolamento Roma II). Al riguardo si consenta il rinvio al nostro E.A. ROSSI, *The Digital Services Act (DSA) and Conflict of Laws*, in *Revue des affaires européennes*, n. 3, 2023, p. 625 ss.

[82] V. A. PALUMBO, J. PIEMONTE, *Delega di funzioni regolamentari e lotta ai rischi sistemici causati della disinformazione nel* Digital Services Act, *cit.*, p. 129 ss.

[83] Così G.M. RUOTOLO, *Mercati e servizi digitali in Europa*, *cit.*, p. 71. In senso analogo v. anche F. POSTERARO, *Il copyright al tempo dell'IA generativa*, *cit.*, p. 11 ss.

[84] G.M. RUOTOLO, *Mercati e servizi digitali in Europa*, *cit.*, 75.

[85] M. DRAGHI, *The Future of European Competitiveness*, Rapporto del 9 settembre 2024, sul quale v. A. POGGI, F. FABRIZZI, *Il nuovo* Whatever it takes. *Il rapporto Draghi: ambizioni e difficoltà del futuro dell'Europa*, in *federalismi.it*, n. 22, 2024.

been growing excessively") incide negativamente sulla competitività europea nello scenario globale, denotando mancanza di visione organica e strategia complessiva[86].

In questo quadro è già stato sottolineato il ruolo che il diritto internazionale e il diritto dell'UE[87] possono avere nel contribuire al contrasto alla disinformazione[88], nell'ambito sia dell'*enforcement* pubblico[89], sia privato[90]. Ma per poter ottenere risultati concreti, non solo a beneficio dei mercati, degli investitori e degli operatori commerciali[91], ma anche sotto il profilo della protezione dei diritti minacciati dalla disinformazione[92], appare imprescindibile una massiccia operazione di miglioramento della qualità e della chiarezza del quadro legislativo vigente.

[86] M. DRAGHI, *The Future of European Competitiveness*, *cit.*, *Part A. A competitiveness strategy for Europe*, p. 8: *"First, Europe is lacking focus. We articulate common objectives, but we do not back them by setting clear priorities or following up with joined-up policy actions. For example, we claim to favour innovation, but we continue to add regulatory burdens onto European companies, which are especially costly for SMEs and self-defeating for those in the digital sectors (…)".*

[87] Si vedano, ad esempio, anche le carenze metodologiche dell'*AI Act* nella valutazione del livello di rischio dei sistemi di intelligenza artificiale evidenziate da C. NOVELLI, F. CASOLARI, A. ROTOLO, M. TADDEO, L. FLORIDI, *AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act*, in *Digital Society*, 2024, p. 2 ss.

[88] V. B. BAADE, *Fake News and International Law*, *cit.*, p. 1373 ss., il quale sembra rilevare l'esistenza di obblighi internazionali gravanti sugli Stati volti a soddisfare il bisogno di selezione delle informazioni, in via diretta, regolando la diffusione di notizie false e astenendosi dal contribuire alla loro fabbricazione e circolazione, nonché, in via indiretta, utilizzando strumenti legislativi per rafforzare la fiducia nei *media* liberi e trasparenti e per preservare il pluralismo degli stessi. V. inoltre, con riferimento alla necessità di conciliare la funzione regolatrice del diritto internazionale dei diritti umani con le politiche fondate sull'accumulo di dati e le regole che governano il cyberspazio, G. DELLA MORTE, Big Data *e protezione internazionale dei diritti umani. Regole e conflitti*, Editoriale Scientifica, Napoli, 2018. In tema v. altresì, E. CELESTE, N. PALLADINO, D. REDEKER, K. YILMA, *The Content Governance Dilemma, cit.*, p. 27 ss.

[89] V. R. SABIA, *L'*enforcement *pubblico nel* Digital Services Act *tra Stati membri e Commissione europea: implementazione, monitoraggio e sanzioni*, in *MediaLaws*, n. 2, 2023, p. 88 ss.

[90] Vedi G.M. RUOTOLO, *Nell'anno delle elezioni hanno tutti ragione*, *cit.*, che ricorda come, specialmente nell'ambito dei regolamenti dell'Unione sul digitale, entrambe le forme di *enforcement* siano contemplate (anche se non sempre in egual misura): infatti, dopo una prima fase di regolamentazione del fenomeno della disinformazione basata su norme "volontarie", è seguita una seconda fase a partire dal 2020 basata su misure "eteroimposte". Sull'applicazione di modelli di contrasto alla disinformazione basato sull'enforcement pubblico-privato cfr. anche D. BROMELL, *Regulating Free Speech in a Digital Age*, Springer, Cham, 2022, p. 218 ss., nonché O. POLLICINO, *I codici di condotta tra* self-regulation *e* hard law*: esiste davvero una terza via per la regolazione digitale? Il caso della strategia europea contro la disinformazione* online, in *Riv. trim. dir. pubbl.*, n. 4, 2022, p. 1051 ss.

[91] V. ancora M. DRAGHI, *The Future of European Competitiveness*, *cit.*, p. 8.

[92] V. K. MASCHER, *Epistemic Power and EU Digital Law*, Working Paper, April 2025, disponibile all'indirizzo https://ssrn.com/abstract=5209728, pp. 30-31