# L'impianto regolatorio della società dell'informazione tra vecchi e nuovi equilibri. Il fenomeno del *deep fake*[*]

Giuseppe Proietti

## Abstract

Il contributo intende offrire un quadro della società dell'informazione plasmata dall'uso dei più recenti strumenti tecnologici inquadrando le opportunità e i rischi che ne derivano. L'analisi delle questioni sollevate da questi strumenti necessita di uno sforzo ermeneutico che mira a combinare normative sempre più complementari e interdipendenti. Quindi, oltre a un necessario riferimento all'importanza della normativa in materia di dati personali, ci si concentra sulla recente legislazione e sul suo impatto nel campo dell'informazione e della comunicazione, con un'attenzione particolare al fenomeno dei *deep fake*. L'analisi si basa sull'Artificial Intelligence Act e sul Digital Services Act, il quale mira a ridurre o eliminarne i contenuti illegali dagli ambienti digitali.

This paper aims to provide an overview of the information society shaped using the most recent technological tools by framing the opportunities and risks involved. The analysis of the issues raised by the tools requires a hermeneutical effort that seeks to combine increasingly complementary and interdependent regulations. The analysis, therefore, in addition to a necessary reference to the importance of personal data legislation, focuses on the recent legislation and its impact in the field of information and communication, with a particular focus on the phenomenon of deep fakes. The analysis is based on the Artificial Intelligence Act and the Digital Services Act, which aims to reduce or remove illegal content from digital environments.

## Sommario

1. Introduzione. – 2. Una premessa sul fenomeno del *deep fake*. – 3. Il nuovo regolamento europeo sui servizi digitali (regolamento (UE) 2022/2065) che sostituisce il previgente quadro della direttiva sul commercio elettronico. - 4. *Segue*: Gli obblighi previsti nel DSA. – 5. Il *deep fake* nell'*AI Act* (regolamento (UE) 2024/1689). – 6. *Segue*. Il dibattito e le sfide sulla normazione del *deep fake*. - 7. Il *deep fake* e il delicato rapporto con la protezione dei dati personali. – 8. Osservazioni conclusive. Prima parte. – 9. Osservazioni conclusive. Seconda parte.

[*] Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

## Keywords

società dell'informazione – *deep fake* – servizi digitali – intelligenza artificiale – servizi intermediari – *hosting provider*

## 1. Introduzione

Nel corso degli ultimi due lustri, il settore dei dati personali e, in generale, quello delle nuove tecnologie, sono stati investiti da un importante attività legislativa tale da comporre un vero e proprio "diritto digitale".

Gli interventi normativi, avvenuti per lo più con lo strumento del regolamento europeo, necessitano di una proficua e complessa attività di attuazione e di coordinamento, fondamentale per evitare il rischio di un "effetto sabbie mobili" nei vari settori.

Il saggio, perciò, si concentra sull'analisi di alcune normative che rientrano nel campo dell'informazione e della comunicazione, in relazione ad ambiti dove le nuove tecnologie hanno provocato considerevoli trasformazioni, talvolta positive e, talaltra, negative[1]. Tra questi ultimi si inserisce il tema del rischio di disinformazione, il quale si distingue a sua volta dalla misinformazione e dalla malinformazione[2].

Perciò, l'analisi si sviluppa su due linee direttrici. La prima si fonda sul recente regolamento europeo sui servizi digitali (Digital Services Act - DSA), il quale origina dall'esperienza della direttiva sul commercio elettronico[3]; la seconda, invece, sull'impatto che negli ambiti succitati possono registrare i *deep fake* e, in particolare, sulla loro regolamentazione inserita sia nel DSA che nel regolamento sull'intelligenza artificiale (AIA o AI Act).

Infine, seppure con un livello minore di approfondimento, verrà messa in luce l'im-

[1] Sul tema della libertà di informazione alla luce dell'evoluzione tecnologica e in una prospettiva di carattere costituzionale, si veda A. Lauro, *Siamo tutti giornalisti? Appunti sulla libertà di informazione nell'era social*, in questa *Rivista*, 2, 2021, 141 ss. Ma anche su ciò che porterebbe alla c.d. fisica sociale, ossia al tema inerente al flusso di idee e sul come le reti sociali le diffondono e le trasformano in comportamenti attraverso i *big data*, si veda A. Pentland, *Fisica sociale. Come si propagano le buone idee*, Milano, 2015; su questi temi cfr. altresì G. Ziccardi, *La democrazia elettronica tra social network, big data e problemi di sicurezza,* in *Diritto di Internet*, 1, 2019, 239 ss.

[2] Alcuni preferiscono parlare di "disinformazione" anziché di *fake news*, perché con la prima si fa riferimento e si inglobano tutte le «informazioni false, inaccurate o fuorvianti, artificiosamente create, le quali siano presentate e diffuse con lo scopo precipuo di trarre un profitto di carattere economico, politico o ideologico e/o di provocare un danno a livello pubblico, ivi inclusa l'ingerenza nei processi elettorali e democratici». In questo senso, O. Pollicino - P. Dunn, *Disinformazione e intelligenza artificiale nell'anno delle global elections: rischi (ed opportunità)*, in *federalismi.it*, 12, 2024, 6. Gli Autori distinguono la disinformazione dalla misinformazione; quest'ultima si caratterizzerebbe per l'elemento soggettivo, poiché non sussiste una volontà di diffusione delle informazioni false, concretizzandosi perciò nella diffusione di un materiale percepito come genuino. Il riferimento è alla ricondivisione nell'ambiente online di un contenuto falso ma che si ritiene essere vero. Ancor diversa sarebbe la malinformazione che si avrebbe con la diffusione di informazioni rispondenti al vero che vengono comunicate con l'obiettivo di «provocare un danno».

[3] Per una ricostruzione del percorso che ha portato alla adozione della direttiva sul commercio elettronico e sul suo contenuto si veda M. Bassini, *La rilettura giurisprudenziale della disciplina sulla responsabilità degli Internet service provider. Verso un modello di responsabilità "complessa"?*, in *federalismi.it*, 3, 2015, 1, spec. 7.

portanza della disciplina riguardante la protezione e il trattamento dei dati personali, profilo onnipresente e imprescindibile nei temi in discussione.
L'intero quadro deve essere calato all'interno di un ecosistema digitale in cui i mercati sono dominati da imponenti piattaforme che creano loro stesse le regole e influenzano le dinamiche tra utenti e operatori grazie al potere che hanno acquisito[4]. Si tratta delle cc.dd. *big tech*, talvolta indicate con l'acronimo di GAFAM, le quali vanno a comporre quelli che sono identificati come i "nuovi" poteri privati[5].

## 2. Una premessa sul fenomeno del *deep fake*

Prima di procedere con l'analisi normativa, è utile un preambolo sul recente e attuale fenomeno del *deep fake*, consistente in un contenuto che può estrinsecarsi in una immagine, video o audio generato o manipolato artificialmente.
Per rendere l'idea della portata dei *deep fake* si può far riferimento al recente episodio di truffa che ha indotto un funzionario di una multinazionale britannica con sede ad Hong Kong a trasferire 25 milioni di dollari credendo di interagire in video-conferenza con il proprio direttore finanziario, e non con un estraneo che si avvaleva proprio di una tecnica di *deep fake*[6].
L'origine del fenomeno (neologismo che deriva da una crasi tra "deep learning" e "fake")[7] viene solitamente fatto risalire al 2017, quando un utente della piattaforma Reddit pubblicò vari video in cui i volti di attrici famose venivano scambiati su video porno[8]. Nel gennaio del 2018, un altro utente della stessa piattaforma creò un programma in grado di rendere accessibile a tutti la possibilità di manipolare video[9]. Da

[4] F. Ruggeri, *Poteri privati e mercati digitali,* Roma, 2023, p. 113. L'A. ha rilevato come la capacità di alcune piattaforme di creare e imporre le regole più appropriate per il soddisfacimento delle proprie esigenze costituisce espressione dell'affermazione di specifici poteri privati, in questo caso di natura tecnologica che, nell'arco di pochi anni, sono diventati sempre più saldi e meno contendibili. Cfr. altresì S. Sileoni, *Autori delle proprie regole. I codici di condotta per il trattamento dei dati personali e il sistema delle fonti*, Milano, 2011, p. 9 che individua nel cambiamento del ruolo degli attori pubblici le cause dell'emersione di una sempre maggiore tendenza all'autoregolamentazione da parte dei privati; P. Bonini, *L'autoregolamentazione dei principali Social Network. Una prima ricognizione delle regole sui contenuti politici*, in *federalismi.it*, 11, 2020, p. 265.

[5] L'acronimo sta ad indicare le cinque piattaforme (occidentali) più influenti, ossia, Google, Amazon, Facebook (ormai, Meta), Apple e Microsoft.

[6] Il Sole 24 Ore, 8 febbraio 2024, 21.

[7] In particolare, si tratta della rete generativa avversaria (*Generative Adversarial Network* – GAN), costituita da «un paio di reti neurali di deep learning "avversarie". Il primo network, il falsificatore, cerca di generare qualcosa che sembri reale, per esempio l'immagine sintetizzata di un cane, sulla base di milioni di immagini di cani. L'altro network, l'investigatore, paragona l'immagine sintetizzata del cane creata dal falsificatore con delle effettive immagini di cani, e determina se l'output del falsificatore è reale o fasullo». In tal senso, K. Lee - C. Qiufan, *AI 2041*, Roma, 2023, 79.

[8] E. Meskys - A. Liaudanskas - J. Kalpokiene - P. Jurcys, *Regulating deep fakes: legal and ethical considerations*, in *Journal of Intellectual Property Law & Practice*, 15, 2020, 24 ss., spec. 26. Gli AA. specificano però che nella letteratura accademica il lavoro che maggiormente si avvicina al fenomeno del *deep fake* risalga al 2016 con un articolo di Thies presentato alla *Conference on Computer Vision and Pattern Recognition* in cui fu ideato un modo per consentire a una persona (sorgente) di controllare le espressioni facciali di altro soggetto (target) all'interno di un video.

[9] *Ibid.*

lì si sono venuti a moltiplicare i *software* che consentono di generare *deep fake*. Tuttavia, i più recenti programmi sono più efficienti sotto un profilo di dati e calcoli, sino al punto da essere in grado di "rianimare" immagini fisse[10].

In letteratura molti sostengono che i due elementi che definiscono i *deep fake* vanno rintracciati (i) nell'uso di tecnologie basate sull'intelligenza artificiale e (ii) nell'intento di ingannare[11].

Le tecniche odierne più diffuse, per video e immagini, consistono nella (i) manipolazione di attributi facciali (*face attribute manipulation*), attraverso cui vengono alterate alcune caratteristiche del volto di una persona ritratta, come ad esempio, l'invecchiamento o il ringiovanimento del viso; (ii) tecniche di scambio volti (*face swap*), attraverso le quali il volto presente nell'immagine o video originale viene sostituito da un altro; (iii) le tecniche di *face reenactment* e *lip synching* con cui un video viene sostanzialmente manipolato facendo in modo che sembri che la persona ritratta compia determinate azioni o renda determinate dichiarazioni[12].

In ogni caso, per un inquadramento definitorio del fenomeno del *deep fake*, stando a una accezione ristretta, bisognerebbe riferirsi a quelle creazioni mediante tecniche in grado di sovrapporre le immagini del volto di una persona *target* a un video di una persona *source* al fine di generare un video in cui la prima fa o dice cose che invece fa la seconda[13]. Seguendo invece una definizione più ampia, i *deep fake* sarebbero quei contenuti sintetizzati da sistemi di IA che possono rientrare anche in altre due categorie. La prima, rappresentata dai *lip-sync deep fake,* che si riferisce a video modificati per rendere i movimenti della bocca coerenti con una registrazione audio. La seconda, invece, ricomprende i *puppet-master*, i quali includono video di una persona *target* (*puppet*) che viene animata seguendo le espressioni facciali e i movimenti degli occhi e della testa di un'altra persona (*master*) seduta di fronte a una telecamera[14].

La tecnica, oltre ad aver sviluppato *software* per la creazione di *deep fake*, ha generato anche sistemi e metodi per il loro rilevamento[15]. Tuttavia, esistono a loro volta anche tecniche in grado di eludere i metodi di rilevamento esistenti, evidenziando, quindi, tutti i limiti e l'assenza di "robustezza" degli attuali approcci di rilevamento dei *deep fake*, nonché suggerendo l'opportunità di individuare metodi che raggiungono una migliore efficacia e resilienza a fronte dell'evoluzione della tecnica[16].

---

[10] Ivi, 27.

[11] A. Fernandez, *Regulating Deep Fakes in the Proposed AI Act*, in *medialaws.eu*, 23 marzo 2022.

[12] O. Pollicino - P. Dunn, *Disinformazione e intelligenza artificiale nell'anno delle global elections: rischi (ed opportunità)*, cit., 11 ss.

[13] Aa. Vv., *Deep learning for deepfakes creation and detection: A survey*, in *Computer Vision and Image Understanding*, 223, 2022, 103525.

[14] *Ibid.*

[15] F. R. Moreno, *Generative AI and deepfakes: a human rights approach to tackling harmful content*, in *International Review of Law, Computers & Technology*, 2024, 1 ss., spec., 4. L'A. annovera vari programmi sviluppati con questa finalità, tra cui Sensity, che riconosce contenuti manipolati dall'IA e tecniche di sintesi come volti creati dall'IA e scambi di volti in video realistici.

[16] W. Alkishri - S. Widyarto - J. H. Yousif, *Detecting Deepfake Face Manipulation Using a Hybrid Approach of Convolutional Neural Networks and Generative Adversarial Networks with Frequency Domain Fingerprint Removal*, consultabile su *ssrn.com,* 2023, 1 ss., spec. 16.

Non manca poi chi sostiene che le tecnologie di rilevamento dovrebbero svilupparsi come modelli *open source,* arrivando così a uno standard comune condiviso in grado di gestire il fenomeno[17]. La tecnologia della *blockchain*, per altro verso, viene considerata un altro valido strumento per "controllare" il fenomeno oltre a garantire l'autenticità di un'opera[18].

Alcuni, per analizzare il fenomeno da un punto di vista etico e normativo, distinguono quattro categorie principali di *deep fake*, a seconda del loro uso. Le prime due (*revenge porn* e *deep fake* politici), vengono definiti come casi "difficili", mentre i *deep fake* creati per contenuti commerciali o creativi sono socialmente utili e quindi sollevano meno preoccupazioni[19].

Dunque, l'utilizzo di questa tecnologia può provocare effetti negativi o positivi[20]. Tra i primi, ci può essere l'erosione della fiducia delle persone nei confronti dei contenuti mediatici o un aumento della disinformazione, l'incitamento all'odio e persino una sollecitazione di tensioni politiche[21]. Essi, però, possono avere anche un impatto creativo o produttivo nella fotografia, nei videogiochi, nella realtà virtuale, nelle produzioni cinematografiche e nell'intrattenimento, ad esempio nel doppiaggio di film stranieri, nel campo dell'istruzione attraverso la rianimazione di personaggi storici o nel provare indumenti virtualmente mentre si fanno acquisti[22].

Nel suo insieme, come anticipato, il fenomeno è stato disciplinato sia nel Regolamento europeo sui servizi digitali (DSA), sia nell'AI Act[23]. Nei successivi paragrafi, perciò, verrà dapprima analizzato l'impianto normativo del DSA e poi le previsioni del regolamento europeo sull'intelligenza artificiale sul tema.

---

17 E. Meskys - A. Liaudanskas - J. Kalpokiene - P. Jurcys, *Regulating deep fakes*, cit., 30.

18 L. Floridi, *Artificial Intelligence*, *Deepfakes and a Future of Ectypes*, in *Philos. Technol*, 31, 2018, 317, spec. 321. L'A. sottolinea come «*As a secure and distributed register of transactions, blockchain is being explored as a means of reliably certifying the origins and history of particular products: whether in terms of securing food supply chains, or in recording the many linked acts of creation and ownership that define the provenance of an artwork. In the future, we may adopt the same solution wherever there is a need to ensure (or establish) the originality and authenticity of some artefact, be it a written document, a photo, a video or a painting*».

19 Ivi, 28.

20 Una descrizione chiara del fenomeno, dei suoi effetti negativi e positivi, può essere rintracciata nel saggio di M. Westerlund, *The Emergence of Deepfake Technology: A Review*, in *Technology Innovation Management Review*, 2019, 39 ss.

21 A. Thanh Thi Nguyen - B. Quoc Viet Hung Nguyen - A. Dung Tien Nguyen - A. Duc Thanh Nguyen - C. Thien Huynh-The - D. Saeid Nahavandi - E.Thanh Tam Nguyen - F. Quoc-Viet Pham - Cuong M. Nguyen, *Deep learning for deepfakes creation and detection: A survey,* in *Computer Vision and Image Understanding*, 223, 2022, 103526. Il *deep fake,* secondo gli autori, può anche essere usato per generare false immagini satellitari della Terra contenenti oggetti che non esistono realmente per confondere gli analisti militari; ad esempio, creando un falso ponte su un fiume anche se in realtà non esiste.

22 *Ibid.*

23 V. M. Veake - F. Z. Borgesius, *Demystifying the draft EU Artificial Intelligence Act*, in *Computer Law Review International*, 4, 2021, 97 ss., spec., 108, per una critica al testo originario dell'AI Act, proposto dalla Commissione europea, in ordine alla disciplina dedicata al *deepfake*.

## 3. Il nuovo regolamento europeo sui servizi digitali (regolamento (UE) 2022/2065) che sostituisce il previgente quadro della direttiva sul commercio elettronico

Il regolamento europeo sui servizi digitali (regolamento (UE) 2022/2065), meglio conosciuto come Digital Services Act, è entrato in vigore il 16 novembre 2022 e la sua integrale applicazione, però, si è avuta a partire dal 17 febbraio 2024[24]. Con questo intervento normativo è stato parzialmente modificato l'approccio seguito con la direttiva 2000/31/CE dedicata al commercio elettronico e recepita in Italia con il d.lgs. 70 del 2003[25].

L'obiettivo dichiarato e perseguito con il DSA è quello di contribuire al corretto funzionamento del mercato interno dei servizi intermediari stabilendo le norme per un ambiente online sicuro, prevedibile e affidabile che faciliti l'innovazione e in cui siano tutelati i diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea.

Il regolamento in questione nasce da alcune esigenze del web, il quale ha generato una disintermediazione digitale tale da condurre a una marginalità degli operatori professionali nel settore dell'informazione, con una amplificazione di informazioni su piattaforme digitali, *social network* e blog[26]. Questo scenario, secondo alcuni, favorirebbe la propagazione delle cc.dd. *fake news* e renderebbe arduo orientarsi a causa della difficoltà nell'individuazione delle fonti affidabili[27]. Il lato positivo, però, è quello di avere un ambiente pluralistico che, talvolta, consente la diffusione di notizie trascurate dai circuiti *mainstream*. Rintracciare un punto di equilibrio costituisce l'operazione più difficile da compiere.

Quindi, il DSA prevede un primo gruppo di norme che si ispira e che riprende il contenuto delle regole della direttiva sul commercio elettronico, le quali definiscono il perimetro delle esenzioni da responsabilità dei prestatori di servizi intermediari e, un secondo gruppo, che sancisce gli obblighi che fanno capo a questi ultimi. Le norme volte a individuare gli obblighi a carico dei fornitori mutano l'impianto normativo di riferimento derivante dalla direttiva sul commercio elettronico[28].

---

[24] Per una analisi giuridica, etica e sociale del DSA, anche in un'ottica comparativa con la direttiva sul commercio elettronico, si veda F. Wilman - S. L. KalÄda - P.J. Loewenthal, *The EU Digital Services Act*, in *Oxford Academic*, 2024; A. Turillazzi - M. Taddeo - L. Floridi - F. Casolari, *The digital sevices act: an analysis of its ethical, legal, and social implications*, in *Law Innovation and Technology*, 15, 1, 2023, 83 ss. Sul DSA e sul possibile "effetto Bruxelles" da una prospettiva statunitense, si veda A. Chander, *When the Digital Services Act Goes Global*, in *Berkeley Technology Law Journal*, 38, 3, 2023, 1067 ss.

[25] Su questo tema si veda G. Finocchiaro, *Responsabilità delle piattaforme e tutela dei consumatori*, in *Giornale di diritto amministrativo*, 6, 2023, 730; G. Monga, *Responsabilità degli intermediari. Il Digital Services Act*, in M. Maggiore (a cura di), *Il commercio elettronico*, Torino, 2024, 194 ss.

[26] B. Grazzini, *Piattaforme e content moderation - Fake news e disinformazione*, in *Giurisprudenza Italiana*, 2, 2024, 491, spec. 493.

[27] *Ibid.* Sul tema della disinformazione e sulla diffusione di notizie tra utenti si veda anche M. Del Vicario - A. Bessi - F. Zollo - W. Quattrociocchi, *The spreading of misinformation online*, in *PNAS*, 13, 3, 2016, 554 ss.

[28] G. Finocchiaro, *Responsabilità delle piattaforme e tutela dei consumatori*, cit., 733.

Il regolamento, quindi, si incentra sui prestatori di determinati servizi della società dell'informazione così come definiti dalla direttiva (UE) 2015/1535; vale a dire, coloro che prestano qualsiasi servizio, normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario[29].

In altri termini, la normativa riguarda molti degli operatori del mercato digitale, dai *social network* alle piattaforme *e-commerce,* fino ai motori di ricerca.

Lo scopo principale del regolamento è quello di impedire, o quantomeno di ridurre, la diffusione di contenuti illegali nell'ambiente online, dettando le regole che definiscono i casi in cui i prestatori di servizi intermediari non sono responsabili e i relativi obblighi da rispettare.

Da una analisi complessiva della normativa in questione, ciò che emerge come fulcro centrale è rappresentato dal potere del prestatore di servizi intermediari di procedere con l'adozione diretta di una misura restrittiva in caso di contenuti illegali, senza la necessità di un previo provvedimento di un'autorità. Ciò è in linea con la giurisprudenza europea che, anche in tempi recenti, ha stabilito che un motore di ricerca può dar seguito alla richiesta di deindicizzazione se il richiedente riesce a fornire un *fumus* di prova della "manifesta inesattezza" delle notizie indicizzate, senza necessità di una precedente pronuncia di una autorità giudiziaria[30].

Il modello di responsabilità dei fornitori di servizi digitali muta rispetto a quello della direttiva 2000/31/CE poiché in quest'ultima venivano collocati in una posizione privilegiata, con una responsabilità limitata (regime del *safe harbour*), mentre con il DSA è l'utente che costituisce il fulcro della tutela[31].

---

[29] Il riferimento normativo all'elemento del «normalmente dietro retribuzione» può essere considerato uno degli elementi che pone l'esigenza di comporre in modo univoco e definitivo la questione attinente alla fallace gratuità di alcuni servizi di operatori digitali, tra cui i *social network*, per la quale sussiste un importante riluttanza nel considerare il trattamento dei dati personali dell'utente come un corrispettivo o una controprestazione. Se tali servizi venissero considerati come servizi "gratuiti", si potrebbero avere problematiche di applicazione soggettiva anche del DSA là dove richiede – tramite un rinvio alla direttiva (UE) 2015/1535 – un servizio reso «normalmente dietro retribuzione». Sul tema della gratuità sia consentito il rinvio a G. Proietti, *Algoritmi e interesse del titolare del trattamento nella circolazione dei dati personali*, in *Contratto e Impresa,* 3, 2022, 880, spec. 897.

[30] CGUE, C-460/20, *Google LLC* (2022); sul diritto/obbligo alla deindicizzazione la giurisprudenza di legittimità è intervenuta a più riprese, anche recentemente. Si veda, infatti, Cass. civ., sez. I, 27 dicembre 2023, n. 36021, in *Foro It.*, 2024, 1, 2, 455. Nel sistema previgente, ossia con la direttiva sul commercio elettronico, il legislatore nazionale aveva optato per un diverso sistema, discostandosi dal regime comunitario per i servizi di *hosting*, ossia l'art. 16 del d.lgs. 70/2003 subordinava l'obbligo di intervento del fornitore alla previa notifica da parte di un'autorità competente.

[31] G. Finocchiaro, *Responsabilità delle piattaforme e tutela dei consumatori*, cit., 733-734, secondo cui «il consumatore, sul web, non è solo un fruitore dei servizi digitali, ma è un *prosumer*, ossia un consumatore e un produttore che, fruendo dei servizi digitali, contribuisce alla produzione di tali servizi. I motori di ricerca, il commercio elettronico, i blog e i social network basano il proprio funzionamento anche sulla collaborazione dell'utente-consumatore, che, mentre naviga e vive la sua onlife, contribuisce a determinare il prezzo delle inserzioni pubblicitarie o a costruire la reputazione di un venditore o di un prodotto». Un ulteriore elemento di complessità sarebbe costituito dal fatto che esiste un noto «livello di asimmetria tecnologica e informativa tra gli utenti e gli operatori del web. Non si tratta soltanto di un disequilibrio di natura economica, ma soprattutto di un disequilibrio causato da una disparità di conoscenze tecniche e di informazione. Tale asimmetria può influire sulla corretta formazione della volontà, anche contrattuale, dell'utente. Considerato che, al momento della conclusione di un contratto on line, generalmente esiste una notevole differenza fra le conoscenze delle parti contraenti, tale information gap può generare erronee aspettative o un illegittimo affidamento nei confronti del

Per rendere più efficace l'applicazione del DSA è stato poi istituito il Centro europeo per la trasparenza algoritmica (ECAT), al fine di vigilare, in particolare, sull'utilizzo dei sistemi algoritmici.
L'ECAT è chiamato a coadiuvare la Commissione europea per garantire che i sistemi algoritmici utilizzati dalle piattaforme e dai motori di ricerca di grandi dimensioni rispettino i requisiti in tema di gestione e di attenuazione dei rischi.
Un altro elemento centrale è il concetto di «contenuto illegale» che, stando al DSA, deve rispecchiare quello corrispondente all'applicazione delle norme nell'ambiente offline. Questo concetto è definito in senso lato, in modo da coprire anche le informazioni riguardanti i contenuti, i prodotti, i servizi e le attività illegali.
Con "contenuto illegale" deve intendersi il riferimento a informazioni, indipendentemente dalla loro forma che, ai sensi del diritto applicabile, sono da considerarsi illegali, come l'illecito incitamento all'odio o i contenuti terroristici illegali e i contenuti discriminatori, o che «le norme applicabili rendono illegali in considerazione del fatto che riguardano attività illegali»[32]. Tra queste figurano, a titolo esemplificativo, «la condivisione di immagini che ritraggono abusi sessuali su minori, la condivisione non consensuale illegale di immagini private, il *cyberstalking* (pedinamento informatico), la vendita di prodotti non conformi o contraffatti, la vendita di prodotti o la prestazione di servizi in violazione della normativa sulla tutela dei consumatori, l'utilizzo non autorizzato di materiale protetto dal diritto d'autore, l'offerta illegale di servizi ricettivi o la vendita illegale di animali vivi. Per contro, un video di un testimone oculare di un potenziale reato non dovrebbe essere considerato un contenuto illegale per il solo motivo di mostrare un atto illecito quando la registrazione o la diffusione di tale video al pubblico non è illegale ai sensi del diritto nazionale o dell'Unione»[33].
I prestatori di servizi intermediari, secondo il DSA, hanno la facoltà di svolgere indagini proprie per scovare i contenuti illegali, ma non sono tenuti a sorvegliare le informazioni e i contenuti che trasmettono o memorizzano, né sono tenuti ad accertare i fatti o le circostanze che inducono a ritenere sussistente la presenza di attività illegali. Quest'ultimo profilo non è nuovo, poiché già sotto la vigenza della direttiva sul commercio elettronico si dibatteva, escludendolo, circa l'esistenza di un generale obbligo di sorveglianza da parte degli operatori digitali. L'esclusione di una simile impostazione si giustificava per il fatto che il fornitore diverrebbe un vero e proprio censore privato, oltre al fatto che un obbligo del genere andrebbe a minare le fondamenta della libertà

fornitore del servizio fino al limite a giungere a viziare il momento di formazione della volontà»; sul regime previgente e relativo alla direttiva sul commercio elettronico si veda E. Andreola, *Profili di responsabilità civile del motore di ricerca*, in *NGCC*, 2, 2012, 127.

[32] In tal senso il considerando n. 12 del DSA. Sul tema riguardante i «contenuti illegali» ci si chiede «quando le fake news costituiscono espressione di libertà di manifestazione del pensiero esercitata in modo non conforme all'ordinamento (ma, ancor prima, cosa debba intendersi per fake news) ed in quali (non sempre sovrapponibili) casi esse possono venire inibite senza che si entri in frizione con le regole ed i principi fondamentali, di livello costituzionale». In questo senso, B. Grazzini, *Piattaforme e content moderation*, cit., 496. Sulla definizione di contenuto illegale ai sensi del DSA si veda anche G. Monga, *Responsabilità degli intermediari. Il Digital Services Act*, cit., 194, il quale sottolinea il carattere generale e onnicomprensivo della nozione che include ogni violazione di legge o del diritto europeo, «a prescindere da quale sia il diritto o la norma di legge concretamente violata».

[33] In tal senso sempre il considerando n. 12 del DSA.

di impresa in capo agli *Internet service provider*[34].

La giurisprudenza europea si è espressa sul tema proponendo soluzioni differenti a seconda della possibilità di qualifica del fornitore come "neutro", ossia quando realizza una attività prettamente di carattere passivo e tecnico[35], oppure, invece, quando è "attivo" e può essere quindi ritenuto responsabile[36]. Su questo tema si è espressa anche la giurisprudenza di merito, sino a recenti pronunce in cui, nonostante il fornitore fosse considerato come un *host provider* passivo, il Tribunale lo ha ritenuto responsabile per i contenuti pubblicati da terzi[37]. Si può notare poi che, sia nel contesto della giurispru-

[34] M. Bassini, *La rilettura giurisprudenziale della disciplina sulla responsabilità degli Internet service provider*, cit., 11.

[35] Una pronuncia rilevante in questo senso è quella della Corte di giustizia, CGUE, C-236/08, C-238/08, *Google France SARL* (2010), in *Foro It.*, 4, 2010, 458. Si considera "neutro", e quindi non responsabile secondo la allora vigente normativa sul commercio elettronico, quel soggetto che esegue un'attività di tipo puramente tecnico e passivo, senza alcun obbligo relativo a un controllo delle informazioni trasmesse o che va a memorizzare. In particolare, si legge che «L'art. 14 della Direttiva n. 2000/31/CE sul commercio elettronico deve essere interpretato nel senso che la norma ivi contenuta si applica al prestatore di un servizio di posizionamento su Internet qualora detto prestatore non abbia svolto un ruolo attivo atto a conferirgli la conoscenza o il controllo dei dati memorizzati. Se non ha svolto un siffatto ruolo, detto prestatore non può essere ritenuto responsabile per i dati che egli ha memorizzato su richiesta di un inserzionista, salvo che, essendo venuto a conoscenza della natura illecita di tali dati o di attività di tale inserzionista, egli abbia omesso di prontamente rimuovere tali dati o disabilitare l'accesso agli stessi». Per un commento su questa sentenza si veda M. Tavella - S. Bonavita, *La Corte di Giustizia sul caso "AdWords": tra normativa marchi e commercio elettronico*, in *Riv. dir. ind.*, 5, 2010, 429.

[36] Per i casi in cui la Corte di giustizia ha riconosciuto la qualifica di prestatore "attivo", si veda la sentenza CGUE, C-324/09, *eBay c. L'Oréal* (2011), in *Dir. giust.*, dove chi si trovava a gestire un mercato online veniva convenuto in giudizio perché aveva consentito ai propri utenti di vendere prodotti contraffatti oppure privi dei requisiti di legge necessari per la vendita. Si veda altresì CGUE, C-523/10, *Wintersteiger AG* (2012).

[37] Il riferimento è alla sentenza del Trib. Roma con il quale è stato condannato Facebook (oggi, Meta) in quanto «Sebbene l'hosting provider c.d. "passivo" non possa essere soggetto ad un obbligo generale di sorveglianza, va affermata la responsabilità della società che gestisce un social network ove venga messa a conoscenza, da parte del titolare dei diritti lesi, del contenuto illecito dei contenuti pubblicati dagli utenti su un profilo telematico ove non si sia attivata per rimuoverli o impedire l'accesso agli stessi». In tal senso, Trib. Roma, sez. spec. in materia di imprese, 15 febbraio 2019, n. 3512, nota di B. Tassone, in *Riv. dir. ind.*, 4, 2019, 372. Lo stesso Trib. Roma si era pronunciato nel senso che «ai fini dell'affermazione della responsabilità dell'hosting provider "attivo" occorre in ogni caso dimostrare che questi fosse a conoscenza o potesse essere a conoscenza dell'illecito commesso dall'utente mediante l'immissione sul portale del materiale audiovisivo in violazione dei diritti di sfruttamento economico detenuti dal titolare dei diritti lesi. Ciò in quanto anche all'hosting provider "attivo" si applica il divieto, previsto dall'art. 15 della direttiva 2000/31/CE (e dall'art. 17 del decreto attuativo n. 70/2003), di un obbligo generalizzato di sorveglianza preventiva sul materiale trasmesso o memorizzato e di ricerca attiva di fatti o circostanze che indichino la presenza di attività illecite da parte degli utenti del servizio. Correlativamente, neppure può essere esclusa la responsabilità dell'*hosting provider* "passivo" ogniqualvolta sia stato messo a conoscenza, da parte del titolare dei diritti lesi, del contenuto illecito delle trasmissioni e ciononostante non si sia attivato prontamente per rimuovere le stesse e abbia proseguito, invece, nel fornire agli utenti gli strumenti per la prosecuzione della condotta illecita». In quest'ultimo senso, Trib. Roma, Sez. spec. in materia di imprese, 10 gennaio 2019, n. 693, nota di M. Iaselli, *Riv. dir. ind.*, 4, 2019, 387. Per pronunce meno recenti sul tema si veda altresì Trib. Roma, 16dicembre 2009, nota di G. Schiavone, in *Obbl. e Contr.*, 4, 2010, 304; App. Milano, Sez. spec. in materia di imprese, 7 gennaio 2015, n. 29, nota di E. Marvasi, in *Riv. dir. ind.*, 5, 2015, 455. Con quest'ultima sentenza la Corte di appello ha rilevato che la memorizzazione permanente di contenuti da parte di un *hosting provider*, benché arricchita da servizi ulteriori non comporta una automatica qualificazione del soggetto come "attivo" tale da portare a una esclusione dei casi di esenzione da responsabilità. Per la giurisprudenza di legittimità si veda Cass. civ., sez. I, 19 marzo 2019, n. 7708, in *quot. giur.*, 2019; Cass. civ., sez. I, 19 marzo 2019, n. 7709, in *Foro It.*,

denza europea che in quella nazionale, le pronunce sorgono per lo più su fattispecie relative alla violazione del diritto d'autore. Rispetto ai primi anni duemila, ossia quando prendeva forma la normativa inerente al commercio elettronico, si è andata via via sfocando quella figura dell'*hosting provider* neutro (o passivo), che faceva leva sull'art. 14 della Direttiva E-Commerce[38].

## 4. *Segue*: Gli obblighi previsti nel DSA

Gli orientamenti della giurisprudenza della corte di giustizia sono stati in parte assorbiti dal legislatore europeo con la Direttiva Copyright (direttiva (UE) 2019/790) e poi, dal canto suo, il Digital Services Act ha prodotto ulteriori novità.
In un confronto con la direttiva sul commercio elettronico, gli elementi di novità offerti dal DSA riguardano, in particolare, la disciplina applicabile all'*hosting provider*. Quest'ultimo regolamento, benché comporti l'abrogazione delle disposizioni "centrali" della Direttiva E-Commerce (artt. 12-15), ne riproduce il contenuto con qualche opportuna modifica, rimettendo a una valutazione caso per caso l'inapplicabilità delle esenzioni a quelle ipotesi in cui il *provider* non si limita a una fornitura "neutra" dei servizi[39].
In buona sostanza, il DSA prevede un approccio *a strati*, vale a dire doveri di diligenza differenti a seconda dei soggetti coinvolti[40]. Infatti, ci sono obblighi applicabili indistintamente a tutti i prestatori, tra i quali quello di specificare, nelle condizioni generali di contratto, in modo conciso, intellegibile e accessibile, le informazioni riguardanti le restrizioni che vengono imposte sull'uso dei loro servizi, tra cui le politiche, le procedure, le misure e gli strumenti utilizzati ai fini della moderazione dei contenuti, incluso il processo decisionale algoritmico e la verifica umana, oltre alle regole procedurali del loro sistema interno per la gestione dei reclami.
I prestatori sono tenuti ad agire in modo diligente, obiettivo e proporzionato, tenendo conto dei diritti e degli interessi di tutte le parti coinvolte, tra cui la libertà di espressione, il pluralismo dei media e altri diritti e libertà sanciti dalla Carta[41].
Nel caso in cui il prestatore di servizi di memorizzazione di informazioni adotti una misura restrittiva, questa deve essere accompagnata da un'idonea motivazione contenente una serie di informazioni, salvo che la misura sia la conseguenza di un ordine da parte di una Autorità.
Perciò, il DSA non prevede una disciplina focalizzata sulla individuazione di ciò che online costituirebbe un contenuto illegale, benché tenti di delinearlo indirettamente,

1, 2019, 2045.

38 Sul tema, O. Pollicino, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider,* in *Percorsi Costituzionali*, 1, 2014, 46 ss.

39 In questo senso depone il considerando 18 del DSA.

40 G. Monga, *Responsabilità degli intermediari. Il Digital Services Act*, cit., 214.

41 Infatti, in dottrina è stato evidenziato che «*one of the main objectives pursued by the DSA is the need to strike a fair balance between various fundamental rights and other interests at stake in the context of the provision of intermediary services*», F. Wilman, *The EU Digital Services Act*, cit., 16; si veda altresì P. Church - C. Necati Pehlivan, *The Digital Services Act (DSA): A New Era for Online Harms and Intermediary Liability*, in *Global Privacy Law Review,* 4, 1, 2023, 53 ss.

ma il fulcro del sistema si concentra sulle politiche aziendali dei prestatori e nelle condizioni contrattuali da loro predisposte. Come evidenziato in dottrina, quindi, si tratta di un sistema che consegna il governo della moderazione dei contenuti all'autonomia privata[42]. Sul piano della correttezza contrattuale di un rifiuto o rimozione di contenuti pubblicati entrano in gioco differenti interessi dei vari attori coinvolti. Da un lato, occorre considerare la libertà della piattaforma di scegliere quali contenuti rifiutare e, dall'altro, quella dell'utente che, invece, fa valere la lesione della propria libertà di parola oppure l'illegittimità di clausole "limitanti"[43].

Ebbene, il bilanciamento tra i diritti fondamentali che sono in gioco e di cui i prestatori sono sostanzialmente "arbitri" è un tema annoso e delicato, oggetto di dibattito dottrinale e di orientamenti giurisprudenziali, sia nel contesto domestico che europeo[44].

Il DSA prevede poi obblighi (e poteri) aggiuntivi – rispetto a quelli sopra elencati - per i fornitori di "piattaforme online".

Con piattaforme online il legislatore europeo intende una sottocategoria rispetto ai prestatori di servizi di memorizzazione. Si intendono, infatti, le piattaforme di *social network* o quelle "piattaforme che consentono ai consumatori di concludere contratti a distanza con operatori commerciali" (quindi, quelle piattaforme che operano nell'*e-commerce*). Esse sono classificate come prestatori di servizi di memorizzazione di informazioni che, non solo memorizzano informazioni fornite dai destinatari del servizio su richiesta di questi ultimi, ma le diffondono al pubblico su richiesta dei destinatari.

Il DSA prevede poi la discutibile figura del "segnalatore attendibile". Si tratta di una qualifica riconosciuta, su richiesta di qualunque ente, dal Coordinatore in cui è stabilito il richiedente che, in caso di segnalazioni sulla illegalità di contenuti online, avrebbe priorità rispetto agli altri segnalatori[45]. È necessario, per avere tale riconoscimento, che siano dimostrate capacità e competenze particolari per l'individuazione, l'identificazione e la notifica di contenuti illegali, una indipendenza rispetto a qualsiasi fornitore di piattaforme online e capacità di svolgimento dell'attività in modo diligente, accurato e obiettivo.

Inoltre, il DSA prevede obblighi supplementari per i fornitori di piattaforme online

---

[42] U. Ruffolo, *Piattaforme e content moderation - Piattaforme e content moderation negoziale*, in *Giurisprudenza Italiana,* 2, 2024, 442. L'A. inquadra poi i *provider* come i "nuovi arbitri della libertà di espressione".

[43] Ivi*,* 446.

[44] A. Spagnolo, *Bilanciamento tra libertà d'espressione su internet e tutela del diritto d'autore nella giurisprudenza recente della Corte europea dei diritti umani*, in *federalismi.it*, 2013, 1; M.D. Birnhack, *Acknowledging the Conflict between Copyright Law and Freedom of Expression under the Human Rights Act*, in *Tel Aviv University Law Faculty Papers*, 2008, 1. Uno degli interventi più importanti in materia è indubbiamente quello della Corte di giustizia nel celebre caso *Google Spain* con il quale è stato precisato, *inter alia*, l'obbligo a carico dei gestori di motori di ricerca di deindicizzare, dietro apposita richiesta, i contenuti pubblicati sul web senza una precisazione circa i criteri su cui si fonda la decisione: CGUE, C-131/12, *Google Spain SL c. AEPD, González* (2014). Con la sentenza *Google Spain* è stato peraltro ritenuto che il motore di ricerca riveste la qualifica di titolare del trattamento dei dati personali.

[45] In Italia, il Coordinatore dei servizi digitali è stato designato con il d.l. 123/2023 convertito con modificazioni dalla L. 159/2023, che lo ha affidato all'Autorità per le garanzie nelle comunicazioni (AGCOM). Con la delibera n. 40/2024, l'AGCOM ha avviato una consultazione pubblica per acquisire osservazioni ed elementi d'informazione, da parte dei soggetti interessati, sullo schema di regolamento di procedura per il riconoscimento della qualifica di segnalatore attendibile, nonché sulle modalità operative e le aree di competenza.

(VLOP) e di motori di ricerca online di "dimensioni molto grandi" (VLOSE). È la Commissione europea che ha il compito di stabilire quali sono queste piattaforme. Questo avviene quando tali soggetti presentano un numero medio mensile di destinatari attivi del servizio nell'UE pari o superiore a quarantacinque milioni[46].
Tra gli obblighi per questi operatori di grandi dimensioni è prevista la sottoposizione a revisioni annuali e indipendenti di propria iniziativa affinché sia valutata la conformità agli obblighi previsti al capo III, agli obblighi assunti con i codici di condotta e ai protocolli di crisi. È previsto che, in caso di sistemi di raccomandazione, i fornitori devono assicurare almeno un'opzione che non preveda la profilazione di cui all'art. 4, par. 4, GDPR.
Tra le varie prescrizioni a loro carico è prevista anche la predisposizione di una relazione annuale per individuare, analizzare e valutare gli eventuali rischi sistemici derivanti dalla progettazione o dal funzionamento del loro servizio e dei suoi sistemi, compresi quelli algoritmici. Questi rischi riguardano la diffusione di contenuti illegali, eventuali effetti negativi prevedibili per l'esercizio dei diritti fondamentali, o sul dibattito civico, sui processi elettorali e sulla sicurezza pubblica, oltre a quelli relativi alla violenza di genere, alla protezione della salute pubblica e dei minori.
L'art. 40 DSA prevede poi che i fornitori di grandi dimensioni sono tenuti a fornire (al Coordinatore dei servizi digitali o alla Commissione) l'accesso ai dati necessari per monitorare e valutare la conformità al regolamento; se richiesto, devono fornire chiarimenti sulla progettazione, logica, funzionamento e sperimentazione dei loro sistemi algoritmici, compresi i loro sistemi di raccomandazione; in alcuni casi, possono essere tenuti a fornire l'accesso ai ricercatori abilitati che soddisfano alcuni specifici requisiti per condurre ricerche che contribuiscano al rilevamento, all'individuazione e alla comprensione dei rischi sistemici nell'Unione e per la valutazione dell'adeguatezza, dell'efficienza e degli impatti delle misure di attenuazione dei rischi.
È previsto inoltre che, per attenuare tali rischi sistemici, il fornitore è tenuto all'attuazione di una serie di misure. Tra queste prevede anche il ricorso a un contrassegno visibile per far sì che un elemento di una informazione (immagine, audio, video generati o manipolati) che assomigli a persone, oggetti, luoghi o altro, e che a una persona appaia falsamente autentico, sia distinguibile quando è presentato sulle loro interfacce online. Deve essere fornita una funzionalità che consenta ai destinatari del servizio di indicare tale informazione. Si tratta di quelle fattispecie in cui rientra la succitata tecnica del *deep fake* disciplinata anche nel più recente regolamento sull'intelligenza artificiale.

## 5. Il *deep fake* nell'*AI Act* (regolamento (UE) 2024/1689)

L'AI Act (regolamento (UE) 2024/1689) è stato pubblicato nella G.U. dell'UE il 12 luglio 2024 e, nella sua formulazione definitiva, disciplina il fenomeno del *deep fake* all'art. 50 che apre (e chiude) il capo IV dedicato agli obblighi di trasparenza per i fornitori e i

[46] La prima designazione è avvenuta il 25 aprile 2023. Le piattaforme online designate sono diciassette, ossia, Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando. I motori di ricerca sono solamente due, ossia Google Search e Bing.

*deployer* di determinati sistemi di IA, ossia le regole che valgono per i sistemi di IA non ad alto rischio.
Il Regolamento sull'IA definisce il *deep fake* come una «immagine o un contenuto audio o video generato o manipolato dall'IA che assomiglia a persone, oggetti, luoghi, entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona» (art. 3, n. 60, AIA).
Sempre nell'articolo dedicato alle definizioni, con "fornitore" il Regolamento intende quel soggetto che sviluppa o fa sviluppare un sistema di IA e lo immette sul mercato con il proprio nome o marchio. Con *deployer* intende, invece, quel soggetto che utilizza un sistema di IA sotto la propria autorità, fatta eccezione di un utilizzo per attività personale non professionale.
Per i fornitori di sistemi di IA che generano audio, immagini, video o testuali sintetici è sancito l'obbligo di garantire che quanto generato sia marcato in un formato intellegibile attraverso soluzioni tecniche solide e affidabili[47]. A questa regola fa eccezione il caso in cui i sistemi di IA svolgano funzioni di assistenza per l'*editing standard* o nel caso in cui non modifichino in modo sostanziale i dati immessi dal *deployer*.
I *deployer* di un sistema di IA che manipola o genera immagini o contenuti audio o video «che costituiscono un "deep fake"» sono tenuti a rendere noto che quel contenuto è stato artificialmente generato o manipolato. Se, però, si tratta di creazioni artistiche, creative, satiriche o fittizie, l'obbligo di trasparenza è limitato e non può ostacolare «l'esposizione o il godimento dell'opera».
Anche nel caso di generazione o di manipolazione di un testo (*deep fake* testuale), finalizzato all'informazione su questioni di interesse pubblico, i *deployer* sono tenuti a rendere noto che il testo è stato artificialmente manipolato o generato, salvo il caso in cui il contenuto generato sia stato sottoposto a un processo di revisione umana o di controllo editoriale e un soggetto è il responsabile editoriale della pubblicazione.
Tutti gli obblighi in questione trovano eccezione nel caso in cui l'uso del sistema di IA sia stato autorizzato per l'accertamento, l'indagine o la prevenzione di reati.
Infine, viene incoraggiata e agevolata – per il tramite dell'ufficio per l'IA – l'elaborazione di codici di buone pratiche volte a facilitare un'attuazione efficace degli obblighi sulla rilevazione e sulla etichettatura dei contenuti artificialmente manipolati o generati. Viene fatta salva la facoltà della Commissione UE di adottare atti di esecuzione per approvare tali codici.

## 6. *Segue*. Il dibattito e le sfide sulla normazione del *deep fake*

Si è già aperto un ampio dibattito in letteratura sulla normazione del *deep fake*. Si discute, ad esempio, sulla categoria di rischio previste dall'AI Act entro cui dovrebbe rientrare. Alcuni sostengono che la categoria più opportuna sarebbe quella dell'alto rischio e che l'attuale disciplina dedicata al fenomeno sia in realtà inadeguata poiché non forni-

[47] Si noti che l'AIA prevede un obbligo anche in merito ai "testuali sintetici", ma questi ultimi non rientrano nella definizione di *deep fake* di cui all'art. 3, n. 60, AIA.

sce un quadro giuridico chiaro in termini di responsabilità per gli sviluppatori di queste tecnologie, ponendosi enfasi su misure preventive, piuttosto che sanzionatorie[48].
Altri li ritengono rientranti in classificazioni di rischio "limitate" o "specifiche" o, comunque, in una categoria a sé stante[49]. Altri, ancora, hanno evidenziato che qualunque categorizzazione non può soffermarsi sulla tecnologia in sé, sostanzialmente neutrale, ma sull'uso che ne viene fatto, il quale può essere finanche positivo[50]. Quindi, il contesto e l'uso sarebbero gli elementi che possono costituire un fattore chiave nella valutazione del rischio[51].
Non manca chi, invece, ha ritenuto possibile una loro sussunzione nell'ambito delle pratiche vietate di cui all'art. 5, par. 1, lett. a), AIA, poiché vi potrebbe essere uno sfruttamento dei dati dei *social media* e di sistemi di IA per generare *deep fake* di individui ignari, spesso prendendo di mira gruppi vulnerabili[52].
D'altra parte, alcuni sottolineano una discrasia e una differente classificazione di questi fenomeni nell'ambito della disinformazione elettorale nella loro disciplina dell'AIA e del DSA, i quali verrebbero assoggettati a rischi tra loro diversi[53].
Viene poi criticata la parte dell'AIA che esonera i sistemi di IA gratuiti e *open source* dai requisiti di trasparenza imposti ai modelli di IA di uso generale. Ciò perché, in questo modo, alcune piattaforme che consentono agli utenti di produrre *deep fake* di specifici individui sarebbero in grado di operare liberamente, a meno che non siano ritenute a rischio sistemico. Questa potrebbe, perciò, costituire una "scappatoia" per lo sfruttamento di tecniche per un uso dannoso, tra cui il furto di identità o campagne di disinformazione, oltre alla possibilità di ottenere vantaggi ingiusti rispetto ad altre imprese concorrenti che invece operano in modo corretto, distorcendo potenzialmente la concorrenza[54]. Tale "esonero", tuttavia incontra limiti allorché si tratti di modelli di IA per finalità generali, categoria in cui potrebbe ricadere un *deep fake*[55].

---

[48] C. Vanberghen, *The AI Act vs. deepfakes: A step forward, but is it enough?*, in *euractiv.com*, 26 febbraio 2024.

[49] F. R. Moreno, *Generative AI and deepfakes*, cit., 3.

[50] M. Labuz, *Regulating Deep Fakes in the Artificial Intelligence Act*, in *Applied Cybersecurity & Internet Governance*, 2, 1, 2023, 1 ss., spec. 11; per gli aspetti positivi che possono derivare dai *deep fake* si veda J. Silbey - W. Hartzog, *The Upside of Deep Fakes*, in *Maryland Law Review*, 78, 4, 2019, 960-966.

[51] *Ibid.*

[52] F. R. Moreno, *Generative AI and deepfakes*, cit., 7.

[53] Ivi, 16. L'A. fa riferimento al considerando n. 132 AIA sui rischi specifici derivanti da generazione di contenuti che creano rischi "specifici". Il considerando n. 120 e n. 136 del DSA che fa rientrare nel rischio sistemico la disinformazione da *deepfake*. Infine, riporta il considerando n. 62 AIA, rilevandolo come una contraddizione, poiché classifica come "ad alto rischio" quei sistemi atti a influenzare l'esito di elezioni o referendum o il comportamento di voto delle persone fisiche nell'esercizio del voto alle elezioni.

[54] Ivi, 21. Quindi, l'A. sostiene che l'attuale formulazione dell'AIA non raggiunge un giusto equilibrio tra *privacy* degli utenti, protezione dei dati, diritti di proprietà intellettuale e libertà commerciale delle società di IA, rischiando di violare il principio di proporzionalità della CEDU ai sensi dell'art. 8, par. 2, e dell'art. 10, par. 2.

[55] Il considerando n. 103 dell'AI Act prevede che i componenti di IA liberi e *open source* forniti a pagamento o altrimenti monetizzati, anche tramite la fornitura di assistenza tecnica o altri servizi, ad esempio attraverso una piattaforma software, in relazione al componente di IA, o l'utilizzo di dati personali per motivi diversi dal solo miglioramento della sicurezza, della compatibilità o dell'interoperabilità del *software*, ad eccezione delle transazioni tra microimprese, non dovrebbero beneficiare delle eccezioni previste per

Al di là del tema riguardante la classificazione del rischio, il dibattito si è generato anche sugli obblighi di trasparenza previsti nell'AIA. In altri termini, ci si chiede se tali obblighi siano in grado di tutelare effettivamente i destinatari di un processo di disinformazione. Alcuni sostengono che possono avere un ruolo nel ridurre il numero di *deep fake* in circolazione, ma non possono essere considerati un vero e proprio strumento di deterrenza[56]. Secondo un'analoga tesi, la classificazione di queste tecnologie come sistemi a rischio limitato, imponendo solo requisiti di trasparenza, senza prevedere alcuna esplicita sanzione, non realizza sufficienti incentivi per il rispetto della norma[57]. Altri ancora rilevano che le disposizioni stabilite nell'AIA, nonostante la loro accurata formulazione, non comprenderebbero salvaguardie sostanziali e dovrebbero essere previste definizioni chiare, nonché una supervisione trasparente e responsabile, oltre a solide garanzie, sia per gli utenti che per i fornitori[58].
Il dibattito generale è aperto e riguarda anche quella parte della normativa che prevede le varie deroghe alle regole generali[59], oltre ai profili che si intersecano con la disciplina a tutela dei dati personali.

## 7. Il *deep fake* e il delicato rapporto con la protezione dei dati personali

Tra le sfide poste dai *deep fake* rientrano anche quelle che si legano alla tutela dei dati personali. Stante la definizione di dato personale sancita nel GDPR, quando un *deep fake* ritrae un individuo reale, rientra chiaramente nell'ambito di applicazione della normativa europea del GDPR[60].
Però, ci si chiede se, in caso di *deep fake* fittizio, ossia non riproduttivo di una persona realmente esistente, i dati utilizzati per generarlo vadano qualificati come dati personali[61]. Secondo alcuni la risposta dovrebbe essere positiva se si vanno ad analizzare i dati *input*. Vale a dire che, sebbene generato casualmente, l'opera potrebbe riflettere in qualche modo i caratteri degli individui realmente utilizzati per l'addestramento del sistema e tali impronte potrebbero essere sfruttate per una loro reidentificazione[62]. Seguendo questa tesi, si dovrebbe concludere che anche gli sviluppatori che non creano

i componenti di IA liberi e *open source*. Infine, precisa che la messa a disposizione di componenti di IA tramite archivi aperti non dovrebbe, di per sé, costituire monetizzazione. Il successivo considerando n. 104 prevede che i fornitori di questi modelli le cui informazioni parametri sono messi pubblicamente a disposizione dovrebbero essere soggetti ad eccezioni, salvo che presentino un rischio sistemico.

[56] M. Labuz, *Regulating Deep Fakes*, cit., 19.

[57] A. Fernandez, *Regulating Deep Fakes in the Proposed AI Act*, cit., 1.

[58] F. R. Moreno, *Generative AI and deepfakes*, cit., 24. L'A. aggiunge che solo in questo modo l'AIA potrà regolamentare efficacemente i *deepfakes* senza diventare un'arma contro le stesse libertà che cerca di salvaguardare.

[59] M. Labuz, *Regulating Deep Fakes*, cit., 25.

[60] F. R. Moreno, *Generative AI and deepfakes*, cit., 11.

[61] M.J. van der Helm, *Harmful deepfakes and the GDPR*, *Tilburg Law School – Institute for Law, Technology and Society*, in arno.uvt.nl, 1.

[62] F. R. Moreno, *Generative AI and deepfakes*, cit., 11.

direttamente *deepfake* sarebbero sottoposti alla normativa in materia di dati personali allorché utilizzino dati personali per l'addestramento degli algoritmi. Allo stesso modo, i creatori e i distributori sono sottoposti a controlli a causa dell'utilizzo di tali dati nella creazione e condivisione di *deep fake*[63].

In merito alla base giuridica suscettibile di essere invocata in queste circostanze, si ritiene che il consenso e l'interesse legittimo siano le basi astrattamente utilizzabili. Nel caso del consenso, gli individui, sia nell'ambito del contenuto originario che in quello manipolato, devono aver acconsentito attivamente al trattamento dei dati personali e aver ricevuto informazioni comprensibili, facilmente accessibili e concise sui rischi e sui benefici derivanti dal trattamento dei dati[64].

In caso di interesse legittimo, invece, sarebbe necessaria un'attenta valutazione dei potenziali rischi per i diritti e le libertà individuali derivanti dall'uso dei *deepfake*. Pertanto, sarebbe indispensabile accertare i potenziali vantaggi del trattamento dei dati personali per i *deep fake* rispetto ai potenziali danni ai diritti individuali e alle libertà degli interessati.

Quelle opere utilizzate per scopi artistici, satirici o di fantasia (v. considerando n. 134 AIA) potrebbero rientrare nella libertà di espressione e di arte dei creatori in conformità agli artt. 11 e 13 della Carta. Tuttavia, la creazione e la diffusione di disinformazione elettorale o di materiale estorsivo o di contenuti sessuali illeciti, benché generati dall'IA, richiederebbe di dare priorità alla protezione degli interessati, conformemente agli artt. 7 e 8 della Carta europea[65].

Una delle soluzioni che vengono proposte per mitigare i rischi derivanti dall'utilizzo di queste tecnologie, a beneficio degli interessati e del trattamento dei loro dati personali, è rappresentata dall'uso dei dati sintetici[66].

Secondo questa tesi, i dati sintetici sarebbero in grado di impedire che i modelli di IA ereditino e amplifichino i pregiudizi sociali, riducendo così al minimo il rischio di *deep fake* discriminatori. In secondo luogo, rafforzerebbero la *privacy* e la sicurezza riducendo la dipendenza dalle informazioni personali e diminuendo il rischio di violazioni della *privacy* e di un loro utilizzo non autorizzato. In terzo luogo, i processi di generazione dei dati sintetici possono essere più trasparenti e più facili da spiegare, mitigando i rischi derivanti dal tipico fenomeno della *black box* che caratterizza molti sistemi di IA[67].

## 8. Osservazioni conclusive. Prima parte

Negli ultimi anni si sono venuti a consolidare alcuni neologismi come algocrazia[68], ca-

[63] *Ibid.*

[64] Il tema viene peraltro affrontato con una rappresentazione "estrema" ma molto efficace nella puntata della serie TV *Black Mirror* dal titolo *Joan is Awful.*

[65] F. R. Moreno, *Generative AI and deepfakes*, cit., 12.

[66] Ivi, 14.

[67] *Ibid.*

[68] L. Francalanci, *Dall'algocrazia all'algoretica: il potere degli algoritmi*, in *Italiano digitale*, XIV, 3, 2020, 97; G. Cerrina Feroni, *Intelligenza artificiale e sistemi di scoring sociale. Tra distopia e realtà*, in *Diritto dell'Informazione e*

pitalismo della sorveglianza[69], regime dell'informazione[70] o dataismo[71]. Tutte locuzioni valide che esprimono concetti più o meno moderni e che hanno un denominatore comune: lo sfruttamento massivo dei dati e delle informazioni che vengono costantemente fornite dagli individui negli ambienti digitali.

Si è, quindi, consolidato un sistema in cui i singoli individui non sono più soggetti passivi, ma trasmettitori attivi[72].

In questo panorama si innesta anche il tema della circolazione di notizie false, il quale è, per vero, un fenomeno antico e sempre esistito. Nei tempi recenti, però, si assiste a una metamorfosi dei meccanismi della loro propagazione, sia per la pervasività dei *social media*, sia per lo sviluppo di nuovi sistemi, anche tecnologici, che hanno dato vita a nuovi paradigmi, portando alla formazione della società dell'informazione che oggi conosciamo[73].

Si è visto che il DSA, in questo senso, benché riprenda buona parte dei principi già espressi nella direttiva sul commercio elettronico, si prefigge un cambiamento nella direzione di una responsabilizzazione dei prestatori di servizi intermediari al fine di

*dell'Informatica*, 1, 2023, 1, spec. 21-24; P. Benanti, *Oracoli. Tra algoretica e algocrazia*, Roma, 2018; A. Celotto, *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*, in *Analisi giuridica dell'economia*, 1, 2019, 47 ss.; M. Sciacca, *Algocrazia e sistema democratico. Alla ricerca di una mite soluzione antropocentrica*, in *Contratto e impresa,* 4, 2022, 1173.

[69] In particolare, ci si riferisce al testo di S. Zuboff, *Il capitalismo della sorveglianza*, I, Roma, 2019.

[70] Concetti che ritroviamo nella lucida ricostruzione del filosofo Byung-Chul Han, *Infocrazia*, Torino, 2021, 3-13, il quale distingue il regime dell'informazione da quello disciplinare poiché, nel primo, vengono sfruttate informazioni e dati, non corpi ed energie; ciò che conta è l'accesso alle informazioni che vengono poi utilizzate per finalità di sorveglianza psicopolitica, di controllo e di previsione dei comportamenti, declassando così gli uomini a bestie da dati e consumo. L'A. sottolinea come tutto si incentra sulla connessione e più dati vengono generati, più intensivamente si comunica e tanto più efficiente diviene la sorveglianza. Il "dataismo" fa parte del regime dell'informazione e aspira a un sapere totale per calcolare tutto ciò che è presente e sarà nel futuro; quindi, le narrazioni cedono il passo ai calcoli algoritmici. Su questo tema si veda anche B. Romano, *Civiltà dei dati libertà giuridica e violenza*, Petrocco (a cura di), Torino, 2020, 45-50, secondo cui alcuni trattamenti di dati personali attraverso algoritmi finiscono per ridurre gli atti degli uomini in dati calcolabili e «trattare i naviganti nella rete come freddi dati spersonalizzati si concretizza nel manipolarli come cose, merci, ovvero nel situarli in un processo di reificazione, che esaurisce gli esseri umani nello stesso statuto degli oggetti, privi di personalità originale, capace di concepire e realizzare dei progetti, trasformativi del mondo mediante l'attività, storica e creativa del lavoro»; cfr. altresì G. Ziccardi, *Sorveglianza elettronica, data mining e trattamento indiscriminato delle informazioni dei cittadini tra esigenze di sicurezza e diritti di libertà*, in *Ragion pratica*, 1, 2018, 29 ss.

[71] Con "dataismo" si intende quella cultura che sostiene una conoscenza interamente fondata su dati informatici e sulla loro elaborazione, ritenendo ormai superflua la creazione di tesi e ipotesi filosofiche o scientifiche.

[72] Byung-Chul Han, *Infocrazia*, cit., 23.

[73] Si pensi al recente caso X-Grok, ossia un *chat-bot* della piattaforma X che cura e gestisce le notizie di tendenza amplificandone la loro diffusione, anche se non si tratta di notizie vere ma solo di tendenza. In tempi recenti è infatti accaduto che sia stata promossa nella *homepage* di centinaia di milioni di utenti una notizia falsa riguardante il fatto che "L'Iran colpisce Tel Aviv con missili pesanti". La notizia è consultabile al sito mashable.com. Sul tema del rapporto tra informazione e algoritmi e, in particolare, sul ruolo di questi nel creare e diffondere e nel contrastare le notizie (false), si veda G. Marchetti, *Le fake news e il ruolo degli algoritmi*, in questa *Rivista*, 1, 2020, 29 ss. Su questa linea occorre considerare il rapporto tra le *fake news* e la verità che Byung-Chul Han, *Infocrazia*, cit., 33, mette in evidenza, ossia che in un sistema di infodemia, le prime hanno già esercitato il loro pieno effetto prima ancora che si sia dato avvio a un processo di verifica e sfrecciano davanti alla verità senza poter essere più raggiunte da questa.

tutelare l'utente. Facendo propri i principi elaborati dalla giurisprudenza, oggi non si ricorre più a una netta e astratta distinzione tra *provider* attivo e neutro (o passivo), rimettendo l'analisi a una valutazione caso per caso.

L'impianto normativo che si ricava dal DSA offre gli strumenti utili per l'attenuazione dei rischi derivanti dalla diffusione di contenuti illegali online e dalla loro amplificazione e, sebbene non stabilisca ciò che costituisce un contenuto illegale - per il quale bisogna rifarsi alla normativa europea e nazionale -, delinea un approccio *a strati* in cui si stabiliscono i casi in cui il prestatore di servizi sarebbe esonerato da responsabilità e quelli che sono gli obblighi ai quali deve conformarsi. Tra questi obblighi viene valorizzato il ruolo centrale delle condizioni contrattuali che l'utilizzatore del servizio deve rispettare. È in tali formulazioni negoziali, trasparenti e intellegibili che il prestatore definisce anche le sue facoltà e i suoi poteri di "moderazione" dei contenuti che possono essere limitati o rimossi[74].

Di qui entra in gioco il delicatissimo bilanciamento tra il potere della piattaforma e la libera espressione dell'utente che il DSA non intende scalfire. Dunque, il regolamento sui servizi digitali definisce un quadro generale che, nel suo dettaglio, dev'essere inquadrato dal prestatore del servizio con specifiche condizioni contrattuali. Perciò, il fornitore ricopre un ruolo di moderatore tutt'altro che semplice, il quale non può e non deve sfociare nella funzione di "Ministero della Verità".

Il tema del potere di moderazione delle piattaforme non è ovviamente circoscritto ai confini europei. Recentemente, infatti, negli Stati Uniti è intervenuta la Corte Suprema che ha rinviato alle Corti statali la questione attinente proprio ai poteri delle piattaforme online, sollecitando, *inter alia*, una revisione, in conformità al primo emendamento, di quelle leggi statali che limitano il loro margine di intervento[75].

Ad ogni modo, nell'intero quadro di bilanciamento degli interessi in gioco dovrebbe considerarsi anche il principio di autoresponsabilità dell'utente finale. In altri termini, nonostante non vi sussista alcun dubbio sulla necessità di moderare i contenuti illegali che si traducono in fattispecie di reato, il discorso si complica per la manifestazione di opinioni che si discostano da una narrazione "ufficiale" o socialmente accettata[76].

---

[74] Per una analisi critica delle condizioni generali applicate dalle principali piattaforme digitali alla luce del DSA, si veda E. Poddighe - V. Zeno-Zencovich, *La «correttezza» nelle condizioni generali di contratto delle grandi piattaforme online*, in *Comparazione e diritto civile*, 1, 2024, 1.

[75] Supreme Court of the United States, No. 22, *Moody, Attorney General of Florida, Et Al. V. Netchoice, Llc, Dba Netchoice, Et Al., No. 22, NetChoice, LLC, dba NetChoice, et al. v. Paxton*, *Attorney General of Texas,* July 1, 2024, in *supremecourt.gov.*

[76] Opera una distinzione tra "notizie false" e "opinioni" B. Grazzini, *Piattaforme e content moderation*, cit., 497-498. L'A. rileva peraltro che «da un punto di vista strettamente civilistico, l'importanza della distinzione fra notizie e opinioni si stempera nell'ottica risarcitoria, poiché anche quando non è consentito inibire un illecito è possibile responsabilizzare il suo autore. In questa prospettiva le false notizie, ma anche le opinioni esternate in modo lesivo, possono venire ricondotte a diverse fattispecie, e per tale via generare responsabilità (ma anche, in alcune ipotesi, possibilità di inibitoria) secondo i presupposti da ciascuna di queste previsti: può trattarsi di illecito aquiliano ex art. 2043 c.c. (da diffamazione, da violazione della riservatezza o di altri diritti della persona); oppure, qualora celino un atto di concorrenza sleale, integrare gli estremi dell'art. 2598 c.c. (ed in simile ipotesi è l'art. 2599 c.c. a prevedere espressamente l'inibitoria, a prescindere dall'esistenza dei requisiti soggettivi indispensabili per il risarcimento del danno); inoltre, le fake news diffuse nel contesto della comunicazione commerciale possono assumere i contorni di un illecito pubblicitario, che a sua volta può atteggiarsi ad atto concorrenzialmente sleale, ma altresì ricadere nella disciplina in materia di pratiche commerciali scorrette ai sensi degli artt. 18 e segg. del Codice del

Queste ultime, in una società pluralistica, devono essere sempre salvaguardate, benché non condivise dai più, anche in considerazione di un principio di autoresponsabilità dell'utente finale (o lettore), il quale non può essere supposto come un soggetto manipolabile.

## 9. Osservazioni conclusive. Seconda parte

Nella società dell'informazione che si è sommariamente descritta, una tecnica che può talvolta ingannare anche i soggetti più avveduti è indubbiamente quella del *deep fake*[77]. Un fenomeno che, per una ragione ignota, è regolata sia dal Digital Services Act, sia dall'Artificial Intelligence Act.

La regolazione di questa tecnica non è banale e dipende dall'approccio che si intende seguire. Ad esempio, Il Regno Unito ha di recente annunciato una proposta legislativa che criminalizza la creazione di *deep fake* sessualmente espliciti attraverso una nuova fattispecie di reato che si basa su reati già previsti per la condivisione di immagini intime "deepfake", già introdotti con la Online Safety Act. È un approccio normativo che si focalizza sull'utilizzo di uno strumento, e non sullo strumento in sé. In termini di approccio legislativo, il DSA sembra andare in questa direzione poiché, con l'art. 40, circoscrive l'adozione di alcune misure - a carico di alcuni fornitori (VLOSE e VLOP) – volte a mitigare i rischi sistemici, tra cui il ricorso a un contrassegno visibile per far sì che un elemento di una informazione (immagine, audio, video generati o manipolati) sia distinguibile quando è presentato sulle loro interfacce online.

Ebbene, nella normativa del DSA non viene descritto né disciplinato lo *strumento* con il quale si genera il contenuto potenzialmente manipolatorio; esso non viene circoscritto ai sistemi di IA, come quelli disciplinati nell'AI Act, ma si focalizza sull'adozione di una misura volta a rendere trasparenti alcune forme di manipolazione di video, immagine o audio (non viene menzionato un testo). In queste ipotesi rientra, senz'altro, anche la tecnica del *deep fake*.

Nella disciplina contemplata nell'AI Act, invece, l'approccio sembra essere differente. Invero, sebbene vengano prescritti obblighi di trasparenza, si deve trattare di una manipolazione (anche di un testo) che si estrinseca per il tramite di un sistema di IA, così come definito nel regolamento in questione (art. 3, par. 1, lett. a, AIA)[78]. Quindi, si tratta di una normazione che si incentra prima di tutto sullo strumento tecnologico, oltreché sul suo utilizzo.

Peraltro, la normativa delineata nell'AI Act può provocare alcuni problemi applicativi.

consumo (d.lgs. 6 settembre 2005, n. 206), alla stregua di pratica commerciale ingannevole o di pratica commerciale aggressiva».

[77] Si è sopra riportato, ad esempio, il recente caso della truffa che ha portato al trasferimento di 25 milioni di dollari da parte di un funzionario di una multinazionale britannica con sede ad Hong Kong, il quale credeva di interagire in video conferenza con il proprio direttore finanziario, e non con un estraneo che si avvaleva di una tecnica di *deep fake*; cfr. nota 18.

[78] Sulla definizione di sistema di IA alla luce del regolamento sull'intelligenza artificiale sia consentito il rinvio a G. Proietti, *Definire l'indefinibile? I sistemi di intelligenza artificiale alla ricerca di un inquadramento sistematico*, in *Contratto e impresa*, 3, 2024, 882.

Un primo problema può derivare dalla definizione di *deployer*, il quale è il soggetto che utilizza un sistema di IA sotto la propria autorità, fatta eccezione di un utilizzo per attività "personale non professionale". Ebbene, molti usi della tecnica del *deep fake*, non rientrando nell'ambito di una attività professionale, rischiano di ridurre in modo rilevante il perimetro di applicazione delle disposizioni previste all'art. 50 AIA dedicate all'utilizzatore (*deployer*). Un altro elemento che riduce il perimetro applicativo della normativa è rappresentato dalle eccezioni ivi previste che, suscettibili di una valutazione ampiamente discrezionale, possono dar vita a facili elusioni.

I *deep fake*, sebbene vi siano critiche sulla loro classificazione di rischio, ricevono una disciplina *ad hoc* che li fa rientrare nella categoria di "rischio limitato". Tuttavia, quando sono rappresentati da contenuti, video o immagini che sono il frutto di modelli di IA generativa, possono (e devono) soggiacere anche alla più articolata disciplina (e ai relativi obblighi) dedicata ai modelli di IA per finalità generali disciplinati nel capo V del regolamento sull'intelligenza artificiale.

Si può immaginare che la disciplina dell'AI Act dedicata a queste tecniche di manipolazione dei contenuti, soprattutto per il suo reale perimetro applicativo, non sarà risolutiva. Essa potrà essere di ausilio all'utente nel comprendere quand'è che si è al cospetto di un *deep fake*, e quindi di una rappresentazione artificiale, ma non ridurrà la loro diffusione che, in ogni caso, non pare essere lo scopo legislativo.

In un simile scenario, gli strumenti giuridici tradizionali sembrano essere, in molti casi, i più adatti per arginare o mitigare i rischi di alcuni utilizzi di certe tecniche rispetto a quanto tenti di innovare l'AI Act. In un classico esempio di truffa tramite *deep fake*, la normativa penale e civile consente di tutelare il danneggiato. Da un'altra prospettiva, invece, le novità apportate dal DSA sul punto, benché focalizzate solo su alcuni operatori, potrebbero essere utili per gli utilizzi che provocano disinformazione ma, di certo, non possono di per sé far presagire una soluzione definitiva alle complesse questioni che solleva il tema.