Il modello europeo di gestione delle crisi alla luce del *Digital Services Act* e dell'*AI Act*

di Andrea Spaziani

Abstract: *The European crisis management model in the light of the* Digital Services Act *and the* AI Act – The advent of new technologies has not only given rise to new opportunities but has also brought about the emergence of novel risks to the stability of democratic societies. Examples of this phenomenon include the spread of illegal content on the Internet and in social media, as well as the advancement of high-risk artificial intelligence systems. In response to these developments, the European Union has recently enacted two regulations: the *Digital Services Act* (DSA) and the *Artificial Intelligence Act* (AIA). However, the measures introduced by the Brussels legislator, particularly in the context of crisis situations, appear to encroach upon users' fundamental rights.

Keywords: European Union; Crisis management; Digital Services Act; Artificial Intelligence Act; EU law

1. Premessa

L'Unione europea, nel corso dell'ultimo decennio, si è trovata dinnanzi a molteplici situazioni straordinarie ed emergenziali che hanno richiesto il suo intervento anche, e soprattutto, da un punto di vista legislativo. Si pensi, come nel caso di questo contributo, alla diffusione di contenuti illegali e colmi di disinformazione che hanno invaso e continuano ad invadere l'ecosistema digitale – sfuggendo al controllo algoritmico delle *Big Tech* – e allo sviluppo di sistemi di Intelligenza Artificiale, i quali, oltre a fornire un'ampia gamma di benefici (economici, ambientali e sociali), possono «comportare rischi e pregiudicare gli interessi pubblici e i diritti fondamentali tutelati dal diritto dell'Unione»[1].

In merito alle ultime due circostanze descritte, il legislatore di Bruxelles è intervenuto di recente con due regolamenti: il *Digital Services Act* (d'ora in avanti, DSA)[2] e l'*Artificial Intelligence Act* (AIA)[3]. Lo sforzo legislativo europeo è coinciso con l'introduzione di misure che, specie nei casi

[1] *AI Act*, considerando 5.

[2] Reg. UE n. 2022/2065 del P.E. e del Cons., del 19-10-2022, relativo a un mercato unico dei servizi digitali e che modifica la Dir. CE n. 2000/31.

[3] Reg. UE n. 2024/1689 del P.E. e del Cons., del 13-6-2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti CE n. 300/2008, UE n. 167/2013, UE n. 168/2013, UE n. 2018/858, UE n. 2018/1139 e UE n. 2019/2144 e le direttive 2014/90/UE, UE n. 2016/797 e UE n. 2020/1828.

DPCE online
ISSN: 2037-6677

emergenziali, sembrerebbero non tutelare completamente alcuni diritti e valori su cui si basa la Carta dei diritti fondamentali e l'Unione europea stessa.

Obiettivo del presente lavoro è analizzare il modo in cui tali misure potrebbero avere una ricaduta negativa sui diritti fondamentali degli utenti attraverso una riflessione orientata a bilanciare questi ultimi con le azioni contrastive europee.

2. Crisi e diritti fondamentali: l'impatto del *Digital Services Act*

Con il Regolamento (UE) 2022/2065 relativo al mercato unico dei servizi digitali (anche noto come *Digital Services Act* – DSA) del 19 ottobre 2022 e volto a modificare la Direttiva CE n. 2000/31 (Direttiva *e-Commerce*), l'Unione europea ha dato continuità alle proprie attività di contrasto ai contenuti illegali[4] e propagatori di disinformazione[5] inaugurate nel 2015 con l'istituzione della *task force East StratCom* (ESCTF) e con l'attuazione dei primi codici di autoregolamentazione[6].

Obiettivo del DSA è rendere l'ambiente virtuale più sicuro e affidabile e tutelare i diritti fondamentali degli utenti, in particolare «la libertà di espressione e di informazione, la libertà di impresa, il diritto alla non discriminazione e il conseguimento di un livello elevato di protezione dei consumatori»[7]. Per raggiungere i suddetti intenti, il DSA abbandona l'iniziale approccio, fondato sul *laissez-faire* e sull'autoregolamentazione delle piattaforme online, preferendone uno co-regolamentatorio e maggiormente rigoroso al fine di ridimensione il potere dei grandi *player* dell'ecosistema digitale[8]. Pertanto, l'azione legislativa europea si è tradotta

[4] Per «contenuto illegale» si intende «qualsiasi informazione che, di per sé o in relazione a un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme al diritto dell'Unione o di qualunque Stato membro conforme con il diritto dell'Unione, indipendentemente dalla natura o dall'oggetto specifico di tale diritto» (DSA, art. 3, lett. h).

[5] Per la Commissione europea, la disinformazione è «un'informazione rivelatasi falsa o fuorviante concepita, presentata e diffusa a scopo di lucro o per ingannare intenzionalmente il pubblico, e che può arrecare un pregiudizio pubblico» in Com. UE n. 236/2018 della C.E., del 26-4-2018, al P.E., al Cons., al CESE e al CdR, *Contrastare la disinformazione online: un approccio europeo*, 4. Per una ricostruzione completa delle azioni anti-disinformazione dell'Unione Europea, si veda: S. Sassi, *Disinformazione contro costituzionalismo*, Napoli, 2021.

[6] Si fa riferimento a: E.C., *Code of Conduct on Countering Illegal Hate Speech Online*, Brussels, 30-6-2016, https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en; E.C., *Code of Practice on Disinformation*, Brussels, 2018, https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation.

[7] DSA, considerando 3.

[8] Un intento che si evince anche dalle parole di Thierry Breton, commissario europeo per il mercato interno e i servizi: «Grazie alla legge sui servizi digitali l'era delle grandi piattaforme online che pensano di essere al di sopra delle regole sta giungendo al termine» in C.E., *Legge sui servizi digitali: La Commissione accoglie con favore l'accordo politico sulle norme che garantiscono un ambiente online sicuro e responsabile*, comunicato stampa, 23-4-2022, https://ec.europa.eu/commission/presscorner/detail/it/ip_22_2545.

in un Regolamento orientato ad assegnare obblighi ai diversi operatori digitali, basandosi su ruolo, numero di utenti raggiunti dai propri servizi e impatto sull'ecosistema digitale. Come già accennato, responsabilità più stringenti sono assegnate ai c.d. VLOPs (*Very Large Online Platforms*) e VLOSEs (*Very Large Online Search Engines*), ovvero le piattaforme e i motori di ricerca che raggiungono, con i loro servizi, oltre 45 milioni di utenti al mese[9]. Il considerando 41, difatti, stabilisce che gli obblighi fondamentali sono applicabili a tutti i prestatori di servizi intermediari, mentre obblighi supplementari, relativi alla gestione dei rischi sistemici, sono in capo agli attori di cui sopra. È la sezione V del DSA a far luce su tali ulteriori disposizioni. I colossi digitali sono chiamati ad effettuare valutazioni circa eventuali rischi sistemici[10] (contenuti illegali[11] ed eventuali effetti negativi su esercizio dei diritti fondamentali[12], dibattito civico, processi elettorali e sicurezza pubblica[13], violenza di genere e protezione della salute pubblica e dei minori[14]) causati dalla progettazione o dal funzionamento dei loro servizi e sistemi, compresi quelli algoritmici. Per scongiurare il verificarsi di simili scenari, gli stessi attori possono adottare misure di attenuazione[15], comprendenti l'adeguamento della progettazione o del funzionamento dei loro servizi, delle condizioni generali, delle procedure di moderazione dei contenuti, dei sistemi algoritmici (compresi quelli di raccomandazione) o dei sistemi di pubblicità[16], il rafforzamento dei processi interni relativi al rilevamento dei rischi[17], la cooperazione con i segnalatori attendibili o con altri fornitori di piattaforme online o di motori di ricerca online[18], l'adozione di misure di sensibilizzazione o di interfacce online con maggiori informazioni per gli utenti o di tutela dei diritti dei minori[19], il ricorso a un contrassegno ben visibile che segnali la presenza di un contenuto *deepfake*[20]. Oltre all'implementazione di un meccanismo di risposta alle crisi[21] – su cui ci si soffermerà – alle piattaforme e ai motori di ricerca di grandi dimensioni è richiesto di sottoporsi, almeno una volta l'anno, a revisioni indipendenti (art. 37), di assicurare almeno un'opzione per ciascuno dei loro sistemi di raccomandazione (art. 38), di fornire ulteriore trasparenza circa la pubblicità presente nella loro interfaccia (art. 39) o l'accesso, al coordinatore dei servizi digitali del luogo di stabilimento o alla Commissione, ai dati per monitorare la conformità al suddetto regolamento (art. 40). Inoltre, essi sono obbligati a predisporre una funzione di controllo della conformità (art. 41), a sottoporsi ad ulteriori obblighi in materia di relazioni di trasparenza (art. 42) e a farsi carico di un contributo annuale per le attività di vigilanza (art. 43).

[9] Si fa riferimento, tra gli altri, a: Amazon Store, Apple Store, Booking.com, Google, YouTube, LinkedIn, Meta, Bing, Pinterest, Snapchat, TikTok, X, Wikipedia, Zalando.
[10] DSA, art. 34.
[11] DSA, art. 34.1, lett. a).
[12] DSA, art. 34.1, lett. b).
[13] DSA, art. 34.1, lett. c).
[14] DSA, art. 34.1, lett. d).
[15] DSA, art. 35.
[16] DSA, art. 35.1, lett. a, b, c, d, e).
[17] DSA, art. 35.1, lett. f).
[18] DSA, art. 35.1, lett. g, h).
[19] DSA, art. 35.1, lett. i, j).
[20] DSA, art. 35.1, lett. k).
[21] DSA, art. 36.

DPCE online
ISSN: 2037-6677

Accanto alle disposizioni relative ai rischi sistemici poc'anzi menzionate, il DSA prevede anche misure aggiuntive che le piattaforme e i motori di ricerca di grandi dimensioni devono adottare in tempi di crisi[22]. Secondo il considerando 91, una crisi ha luogo al verificarsi di «circostanze eccezionali che possono comportare una minaccia grave per la sicurezza o la salute pubblica nell'Unione o in parti significative della stessa»[23]. Il Regolamento colloca, nel novero delle minacce, i conflitti armati o gli atti di terrorismo, compresi conflitti o atti di terrorismo emergenti, catastrofi naturali quali terremoti e uragani, nonché pandemie e altre gravi minacce per la salute pubblica a carattere transfrontaliero. In presenza di simili circostanze, infatti, la Commissione potrebbe chiedere a tali attori privati, su raccomandazione del Comitato europeo per i servizi digitali («comitato»), di attuare con urgenza delle misure di risposta come indicato dal meccanismo di risposta alle crisi (art. 36) e dai protocolli di crisi volontari (art. 48).

Per quanto riguarda il meccanismo di risposta alle crisi, secondo l'art. 36 la Commissione può spingere i fornitori di grandi dimensioni ad intraprendere azioni quali: i) valutare se i propri servizi contribuiscano, o possano contribuire, a generare in maniera significativa una grave minaccia[24]; ii) individuare e applicare misure specifiche, efficaci e proporzionate per prevenire, eliminare o limitare tale contributo alla grave minaccia[25]; iii) inviare una relazione alla Commissione contenente le azioni emergenziali intraprese e l'impatto qualitativo e quantitativo delle stesse e qualsiasi altra questione connessa a tali valutazioni o misure[26]. Il considerando 91 tenta di far luce sulle misure specifiche, di cui al par. 1, lett. b), fornendo esempi al riguardo come «l'adeguamento dei processi di moderazione dei contenuti e l'aumento delle risorse destinate alla moderazione dei contenuti, l'adeguamento delle condizioni generali, i sistemi algoritmici e i sistemi pubblicitari pertinenti, l'ulteriore intensificazione della cooperazione con i segnalatori attendibili, l'adozione di misure di sensibilizzazione, la promozione di informazioni affidabili e l'adeguamento della progettazione delle loro interfacce online»[27]. In sintesi, ai sensi dell'art. 36, la Commissione può spingere le piattaforme *online* e i motori di ricerca di grandi dimensioni a prevedere l'impiego di misure straordinarie in occasioni

[22] In origine, il DSA avrebbe dovuto prevedere solo un regolamento sulla risposta volontaria alle crisi. Tuttavia, lo scoppio del conflitto in Ucraina unito alle azioni propagandistiche della Federazione Russa che prendono di mira «la società civile dell'Unione e dei Paesi limitrofi, distorcendo gravemente i fatti e manipolando la realtà» (in Reg. UE n. 350/2022, considerando 7) – e alle quali ha fatto seguito la sospensione della diffusione sul suolo europeo delle emittenti Russia Today, Rossiya RTR, RTR Planeta, Rossiya 24, Russia 24, TV Centre International e l'agenzia Sputnik –, hanno portato all'inserimento del meccanismo di risposta alle crisi (art. 36) all'interno del DSA.

[23] DSA, considerando 91.

[24] DSA, art. 36.1, lett. a.

[25] Inoltre, nell'individuare e applicare tali misure, i prestatori di servizi devono tenere debitamente conto «della criticità della grave minaccia […], dell'urgenza delle misure e delle implicazioni effettive o potenziali per i diritti e gli interessi legittimi di tutte le parti interessate, compresa l'eventuale inosservanza dei diritti fondamentali sanciti dalla Carta» (DSA, art. 36.1, lett. b).

[26] DSA, art. 36.1, lett. c.

[27] DSA, considerando 91.

di situazione inconsuete che rappresentano una minaccia per la tenuta e la stabilità dell'Unione europea. Nonostante il chiarimento offerto, le misure previste suscitano qualche perplessità, poiché appare poco chiaro la promozione di informazioni affidabili che VLOPs e VLOSEs potrebbero attuare. L'art. 48 specifica che tali informazioni si riferiscono alla situazione di crisi e vengono fornite dalle autorità degli Stati membri o da altri organismi competenti affidabili (art. 48.2, lett. a). L'opacità del concetto si ravvede nei mancati chiarimenti su cosa si intenda realmente con il termine «informazioni affidabili» e sulla delucidazione riguardante quali contenuti rientrino o meno nella categoria delle informazioni affidabili. In aggiunta, resta ignoto a quale attore coinvolto (piattaforme e motori di ricerca, Commissione europea o Stati membri) spetta la decisione di stabilire se un contenuto appartiene o meno alla sfera delle informazioni affidabili. Infine, sebbene l'art. 48 suggerisca che tali informazioni siano fornite dalle autorità degli Stati membri o da altri organismi competenti, «it does not clarify who appoints those reliable bodies and what information qualifies as reliable or trustworthy»[28].

Oltre al già citato art. 36 anche l'art. 48, relativo all'attuazione di protocolli di crisi volontari, può essere chiamato in causa in occasione di situazioni di crisi che possano in qualche modo minare la stabilità unionale e degli Stati membri. Il considerando 108 sottolinea come la Commissione possa avviare l'elaborazione di tali protocolli quando, ad esempio, le *Internet platforms* «sono utilizzate in modo improprio per la rapida diffusione di contenuti illegali o disinformazione o in cui sorge la necessità di divulgare velocemente informazioni affidabili»[29]. A differenza del meccanismo di risposta alle crisi, la Commissione, nell'art. 48, non impone una decisione ai colossi digitali, ma li incoraggia e li facilita ad elaborare, sperimentare e applicare tali protocolli di crisi[30].

Stando così le cose, dunque, la Commissione sembrerebbe esercitare un ruolo meno coercitivo nei riguardi degli attori privati interessati in presenza di contesti emergenziali. Tali protocolli prevedono l'attuazione di una delle seguenti misure: a) la visualizzazione, ben in evidenza, di informazioni sulla situazione di crisi fornite dalle autorità degli Stati membri o a livello di Unione o, a seconda del contesto della crisi, da altri organismi competenti affidabili; b) la designazione di uno specifico punto di contatto per la gestione delle crisi; c) ove opportuno, l'adeguamento delle risorse

[28] D. Buijs, I. Buri, *The DSA's Crisis Approach: Crisis Response Mechanism and Crisis Protocols*, in *DSA Observatory*, 21-2-2023, https://dsa-observatory.eu/2023/02/21/the-dsas-crisis-approach-crisis-response-mechanism-and-crisis-protocols/.

[29] DSA, considerando 108.

[30] Inoltre, nel processo di elaborazione e supervisione dei protocolli di crisi, la Commissione può coinvolgere le autorità degli Stati membri, gli organi e le istituzioni dell'UE e le organizzazioni della società civile o altre organizzazioni competenti (DSA, art. 48.3).

DPCE online
ISSN: 2037-6677

destinate a garantire il rispetto degli obblighi di cui agli articoli 16[31], 20[32], 22[33], 23[34] e 35[35] alle esigenze che sorgono dalla situazione di crisi.

La Commissione, inoltre, vigila affinché i medesimi protocolli contengano tutti i seguenti elementi: a) i parametri specifici per determinare che cosa costituisca la specifica circostanza eccezionale che il protocollo di crisi intende affrontare e gli obiettivi che persegue; b) il ruolo dei singoli partecipanti e le misure che devono mettere in atto durante la fase preparatoria e in seguito all'attivazione del protocollo di crisi; c) una procedura chiara che stabilisca quando attivare il protocollo; d) una procedura chiara che indichi il periodo – strettamente limitato a quanto necessario per far fronte alle specifiche circostanze eccezionali in questione – durante il quale applicare tali misure dopo l'attivazione del protocollo; e) le garanzie necessarie in caso di eventuali effetti negativi sull'esercizio dei diritti fondamentali, in particolare la libertà di espressione e di informazione e il diritto alla non discriminazione; f) una procedura che consenta di riferire pubblicamente in merito alle misure adottate, alla loro durata e ai loro esiti[36]. Infine, qualora ritenga che un protocollo non affronti efficacemente le situazioni di crisi in corso o possa incidere negativamente sui diritti fondamentali, la Commissione invita i partecipanti a rivederlo, anche adottando misure supplementari[37]. Come già analizzato per quel che concerne il meccanismo di risposta alle crisi con riferimento alla propagazione di informazioni affidabili, anche in questo caso l'espressione «misure supplementari» risulta opaca[38], non chiarendo efficacemente l'oggetto e le conseguenze derivanti dall' applicazione di misure aggiuntive, specie qualora possano avere effetti negativi a cascata verso i diritti fondamentali.

Similmente, si riscontrano ulteriori passaggi contorti e difformi anche nel periodo di impiego di tali misure emergenziali. Per il meccanismo di risposta alle crisi, tale periodo non può superare i tre mesi (art. 36.3, lett. c) ma, qualora la situazione di crisi dovesse protrarsi, la Commissione potrebbe prorogare tali disposizioni per un periodo non superiore ai tre mesi (art. 36.8, lett. b). Nell'adozione dei protocolli di crisi, invece, non viene specificata una durata minima o massima di attuazione degli stessi, bensì, un «periodo strettamente limitato a quanto necessario per far fronte alle specifiche circostanze eccezionali in questione»[39].

Da quanto appena detto, dunque, dinanzi a situazioni di crisi in grado di destabilizzare la sicurezza e la salute pubblica unionale sembrerebbe configurarsi uno scenario censorio – dalla durata preventiva di almeno tre mesi – che metterebbe a repentaglio alcuni diritti fondamentali degli utenti: libertà di espressione e di informazione (art. 11 della Carta dei diritti fondamentali dell'UE), su tutti. Uno scenario nel quale gli utenti, già

[31] Meccanismo di segnalazione e azione (DSA, art. 16).
[32] Sistema interno di gestione dei reclami (DSA, art. 20).
[33] Segnalatori attendibili (DSA, art. 22).
[34] Misure e protezione contro gli abusi (DSA, art. 23).
[35] Attenuazione dei rischi (DSA, art. 35).
[36] DSA, art. 48.4.
[37] DSA, art. 48.5.
[38] D. Buijs, I. Buri, *op. cit.*
[39] DSA, art. 48.4, lett. d.

soggiacenti a bolle informative (le c.d. *filter bubbles*) derivanti da una selezione algoritmica che mostra loro esclusivamente i contenuti che rispondono maggiormente alle preferenze espresse in precedenza, rischierebbero di abitare un ecosistema digitale ulteriormente polarizzato e perimetrato alle sole informazioni affidabili e provenienti da fonti attendibili (come le autorità degli Stati membri o da altri organismi competenti) circa la situazione emergenziale per un periodo che potrebbe protrarsi anche oltre i semplici tre mesi. Nonostante il chiaro tentativo del legislatore europeo di contrastare la disinformazione, apparirebbero configurarsi circostanze emergenziali poco edificanti per i cibernauti, costretti a veder relegate – in termini di visibilità – le proprie opinioni e i propri contenuti a vantaggio di quelli maggiormente attendibili e attinenti alla situazione di crisi in corso. D'altro canto, però, non va sottovalutata la perigliosità della disinformazione che, insieme alla misinformazione, vengono rappresentate come principali rischi globali del prossimo biennio, collocandosi al di sopra perfino di eventi climatici estremi, polarizzazione sociale, insicurezza cibernetica, conflitto armato interstatale, mancanza di opportunità economiche, inflazione, migrazioni involontarie, crisi economica e inquinamento[40]. Tuttavia, data la riconosciuta pericolosità del fenomeno in questione, così facendo si correrebbe il rischio di fronteggiare una situazione estrema con provvedimenti che, da un lato, mirano a bloccare i contenuti disinformativi, ma che dall'altro, minacciano di oscurare i diritti e i valori fondamentali su cui poggia l'ordinamento europeo e quello degli Stati membri. Infine, sembrerebbe delinearsi un ritratto poco positivo degli utenti, incapaci di discernere le informazioni attendibili da quelle inattendibili e, per questa ragione, messi in salvo dal lavoro di "cernita" operato, in contesti emergenziali, dalle piattaforme e dai motori di ricerca online sotto l'attenta guida della Commissione europea. Occorre, quindi, interrogarsi se una maggiore fiducia nelle capacità di giudizio e di analisi dei cittadini non possa dar vita ad una risposta più opportuna e proficua di fronte alla diffusione della disinformazione. Si scongiurerebbe, così, il pericolo di chi sostiene che

> «[o]nce the EU's intervention have shaken citizens' confidence in the freedom of opinion-forming processes, combating a crisis would truly have triggered an ever greater crisis. All parties involved must therefore bear the risk in mind when applying the DSA's crisis response mechanisms»[41].

Dall'analisi appena condotta, dunque, parrebbe delinearsi nel DSA, in presenza di situazioni di crisi, uno scenario censorio sia con l'attuazione del meccanismo di risposta alle crisi e sia con l'elaborazione di protocolli di crisi. I due articoli, difatti, mostrerebbero punti critici per quanto riguarda la tutela della libertà di espressione e di informazione in contesti emergenziali e/o di crisi.

3. L'UE e la corsa alla regolamentazione dell'IA: l'*AI Act*

[40] World Economic Forum, *The Global Risks Report 2024*, 10-1-2024, https://www.weforum.org/publications/global-risks-report-2024/.
[41] J.F. Ferreau, *Crisis? What Crisis? The Risk of Fighting Disinformation with the DSA's Crisis Response Mechanism*, in 16(1) *J. Media L.* 57, 64 (2024).

DPCE online
ISSN: 2037-6677

Nella competizione globale alla regolamentazione dell'Intelligenza Artificiale[42], l'Unione europea è la prima autorità sovranazionale a dotarsi di una normativa – l'*Artificial Intelligence Act*, meglio nota come *AI Act* (AIA)[43] – anticipando la concorrenza di Stati Uniti e Cina[44]. In vigore dallo scorso 1° agosto 2024 e pienamente applicabile nel giro di due anni, l'AIA ha come obiettivo quello di «migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione»[45]. L'esigenza di un simile

[42] Un sistema di intelligenza artificiale viene definito 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» in *AI Act*, art. 3.1.

[43] Il 17 maggio 2024, a Strasburgo, nel corso dell'incontro ministeriale annuale del Comitato dei Ministri, il Consiglio d'Europa ha adottato la Convenzione quadro sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto (Cets 225). Tale trattato internazionale, aperto alla firma il 5 settembre dello stesso anno a Vilnius, definisce un quadro giuridico applicabile, a livello globale, vincolando gli Stati a disciplinare le attività all'interno del ciclo di vita dei sistemi di intelligenza artificiale al fine di evitare che si verifichino impatti negativi sui diritti umani, sulla democrazia e sullo Stato di diritto (art. 1). In particolare, il capitolo III della presente Convenzione stabilisce i principi che ciascuna Parte deve ottemperare. Tra questi figurano il rispetto della dignità umana e dell'autonomia individuale (art. 7), la previsione di adeguati requisiti di trasparenza e supervisione (art. 8), il rispetto del principio di accountability (art. 9), la non discriminazione e la tutela dell'uguaglianza (art. 10), nonché la tutela della privacy e della protezione dei dati personali (art. 11), l'affidabilità dei sistemi di intelligenza artificiale e dei loro risultati (art. 12) e la promozione di un'innovazione sicura (art. 13). Per consultare la Convenzione: Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law*, 5-9-2024, https://rm.coe.int/1680afae3c. Per approfondire, invece, si rimanda a: G. Zaccaroni, *Intelligenza artificiale e principio democratico: riflessioni a margine dell'emersione di un quadro normativo europeo*, in *Quad. AISDUE*, 2024, 2, 19, 27-36.

[44] A differenza di Stati Uniti e Cina, inclini ad uno sviluppo di tale tecnologia per fini economici, occupazionali e legati agli investimenti esteri ed interni, l'approccio europeo si basa su una «logica protettiva dei diritti, che, combinata con il benessere europeo, imporrebbe all'industria digitale globale di adeguarsi al fine di vendere i propri prodotti nei territori UE, mentre ispirerebbe anche altre giurisdizioni a raggiungere analoghi livelli di tutela» in A. Pin, L. Scaffardi, *Tra protezione dei dati e intelligenza artificiale, in Europa e oltre*, in *DPCE Online*, 2024, 2, 1029, 1029-1030. Al riguardo, si veda anche: S. Aceto di Capriglia, *Intelligenza artificiale: una sfida globale tra rischi, prospettive e responsabilità. Le soluzioni assunte dai governi unionale, statunitense e sinico. Uno studio comparato*, in *Federalismi.it*, 2024, 9, 1. Per una prospettiva comparata (USA-Cina) sulle fonti giuridiche dell'IA si rinvia a: E. Stradella, *Le fonti nel diritto comparato: analisi di scenari extraeuropei (Stati Uniti e Cina)*, in *DPCE Online*, 2022, 1, 219. Per una comparazione tra l'approccio europeo e quello statunitense sul tema dell'intelligenza artificiale, invece, si segnala: B. Marchetti, L. Parona, *La regolazione dell'intelligenza artificiale: Stati Uniti e Unione Europea alla ricerca di un possibile equilibrio*, in *DPCE Online*, 2022, 1, 237; E. Chiti, B. Marchetti, *Divergenti? Le strategie di Unione europea e Stati Uniti in materia di intelligenza artificiale*, in *Riv. reg. mer.*, 2020, 1, 29.

[45] *AI Act*, art. 1.1.

intervento legislativo nasce dalla constatazione che tale tecnologia, oltre ad avere un impatto positivo nella vita dei cittadini europei (si pensi ai miglioramenti nel settore sanitario, agricolo, climatico, ambientale e difensivo), possa generare rischi potenziali, quali «meccanismi decisionali opachi, discriminazioni basate sul genere o di altro tipo, intrusioni nelle vite private o utilizzi per scopi criminali»[46]. Per affrontare queste sfide, la scelta del legislatore di Bruxelles è ricaduta su «a horizontal regulatory approach to AI, meaning that it provides rules for all kinds of AI, rather than a vertical approach that focuses only on one specific aspect of AI»[47]. Insieme ad un approccio orizzontale, l'*AI Act* ha fatto proprio anche un approccio *risk-based*. In virtù di ciò, i sistemi di intelligenza artificiale vengono suddivisi in quattro livelli di rischio: inaccettabile, elevato, limitato e minimo o nullo.

Alla luce di questa categorizzazione, la presente analisi si concentrerà sulle pratiche di IA vietate – enunciate all'art. 5 dell'AIA – con particolare riguardo ai sistemi di identificazione biometrica. Secondo il suddetto articolo, infatti, sono vietate le pratiche di IA: i) che utilizzano tecniche subliminali per «distorcere materialmente il comportamento di una persona o di un gruppo di persone, pregiudicando in modo considerevole la loro capacità di prendere una decisione informata»[48]; ii) che sfruttano le vulnerabilità individuali o collettive per distorcere il loro comportamento e causar loro un danno significativo[49]; iii) i c.d. sistemi di "*social scoring*", utilizzati per effettuare una valutazione o una classificazione di persone o gruppi di persone in base al loro comportamento sociale o alle loro caratteristiche personali o della personalità noti[50]; iv) che effettuano «valutazioni del rischio relative a persone fisiche al fine di valutare o prevedere il rischio che una persona fisica commetta un reato, unicamente sulla base della profilazione di una persona fisica o della valutazione dei tratti e delle caratteristiche della personalità [...]»[51]; v) che «creano o ampliano le banche dati di riconoscimento facciale mediante *scraping* non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso»[52]; vi) che inferiscono le emozioni di un individuo nel luogo di lavoro o nelle scuole[53]; vii) i sistemi di categorizzazione biometrica che individuano le persone mediante i loro dati biometrici, usati per trarre deduzioni su dati sensibili quali razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche e orientamento sessuale[54]; viii) i «sistemi di identificazione biometrica remota 'in tempo reale' in spazi accessibili al pubblico a fini di attività di contrasto [...] »[55].

[46] Com. UE n. 65/2020 della C.E., del 19-2-2020, Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia, 1.
[47] R.J. Neuwirth, *Prohibited Artificial Intelligence Practices in the Proposed EU Artificial Intelligence Act* (*AIA*), in 48 *Comput. L. & Sec. Rev.* 2 (2023).
[48] *AI Act*, art. 5.1, lett. a).
[49] *AI Act*, art. 5.1, lett. b).
[50] *AI Act*, art. 5.1, lett. c).
[51] *AI Act*, art. 5.1, lett. d).
[52] *AI Act*, art. 5.1, lett. e).
[53] *AI Act*, art. 5.1, lett. f).
[54] *AI Act*, art. 5.1, lett. g).
[55] *AI Act*, art. 5.1, lett. h).

DPCE online
ISSN: 2037-6677

Proprio su quest'ultima pratica vietata di IA occorrono alcune precisazioni concettuali. Si tratta, innanzitutto, di tecnologie appartenenti al settore della biometria[56] e che permettono di «distinguere un soggetto in forza di caratteristiche fisiche uniche, come le impronte digitali, il DNA, la forma dell'iride, la struttura vascolare della retina, la struttura venosa della mano, oppure attraverso i tratti differenziali del suo comportamento, come il modo di camminare o il timbro della voce»[57]. Le tecnologie biometriche più note e maggiormente diffuse sono quelle relative al riconoscimento facciale (TRF), che si basano «su complessi procedimenti algoritmici che consentono di identificare una persona a partire dall'immagine del suo volto»[58]. Il processo di identificazione, all'interno di simili tecnologie, avviene mediante il trattamento di dati biometrici, ovvero di particolari «dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali le immagini facciali o i dati dattiloscopici»[59]. Dunque, con il termine "identificazione biometrica" si fa riferimento al «riconoscimento automatizzato delle caratteristiche umane fisiche, fisiologiche, comportamentali o psicologiche allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di individui memorizzati in una banca dati»[60]. Un sistema di identificazione biometrica remota – pratica di IA vietata ai sensi dell'art. 5 del presente regolamento e al centro di diverse discussioni e critiche già agli albori dell'*AI Act*[61] – concerne, invece, «l'identificazione di persone fisiche, senza il loro

[56] La biometria è costituita da tutte quelle tecniche che consentono «l'identificazione o 'misurazione' dell'essere umano attraverso la rilevazione di determinate caratteristiche fisiche e comportamentali che vengono tradotte in sequenze matematiche e conservate in banche dati elettroniche» in Comitato Nazionale per la Bioetica, *L'identificazione del corpo umano: profili bioetici della biometria*, 2010, 3. Un settore, quello della biometria, in notevole crescita negli ultimi anni grazie allo sviluppo tecnologico e all'avvento dei c.d. *Big Data*, con applicazioni sia in ambito pubblico (sanitario, scolastico, ordine pubblico) che privato (sia per scopi di sicurezza che commerciali).

[57] E. Learned-Miller et al., *Facial Recognition Technologies in the Wild: A Primer*, in *Ctr. Integrative Rsch. Comput. & Learning Scis.*, 29-5-2020, 8, https://people.cs.umass.edu/~elm/papers/FRTprimer.pdf. G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021, 11.

[58] Più specificatamente le stesse, attraverso una foto o un video che riprendono una persona, permettono di «risalire alla sua identità grazie al confronto automatizzato dell'immagine estrapolata con altra immagine appartenente alla stessa persona nella quale era stata previamente identificata» in G. Mobilio, *Tecnologie di riconoscimento facciale*, *op. cit.*, 11.

[59] *AI Act*, considerando 34.

[60] *AI Act*, considerando 35.

[61] Sul tema si segnala, C. Muller, V. Dignum, *Artificial Intelligence Act. Analysis & Recommendations*, in *ALLAI*, 6-8-2021, https://allai.nl/wp-content/uploads/2021/08/EU-Proposal-for-Artificial-Intelligence-Act-Analysis-and-Recommendations.pdf; EDRi, *Remote Biometric Identification: A Technical & Legal Guide*, 23-01-2023, https://edri.org/our-work/remote-biometric-identification-a-technical-legal-guide/; EDPB, EDPS, *Joint Opinion 05-2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, 18-6-2021, https://www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

coinvolgimento attivo, tipicamente a distanza mediante il confronto dei dati biometrici di una persona con i dati biometrici contenuti in una banca dati di riferimento»[62]. Lo stesso può avere una duplice forma in base al periodo di impiego: in tempo reale e a posteriori. Il primo prevede che «il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono senza ritardi significativi»[63] e comprende sia le identificazioni istantanee e sia quelle che «avvengono con brevi ritardi limitati al fine di evitare l'elusione»[64]. Di conseguenza, tali sistemi implicano l'utilizzo di materiale «dal vivo o quasi dal vivo (ad esempio filmati) generato da una telecamera o da un altro dispositivo con funzionalità analoghe»[65]. Nei sistemi di identificazione a posteriori, invece, il rilevamento dei dati biometrici è già avvenuto, mentre il confronto e l'identificazione vengono realizzati con un ritardo significativo. Come specificato nel considerando 17, si tratta di «materiale, come immagini o filmati generati da telecamere a circuito chiuso o da dispositivi privati, che è stato generato prima che il sistema fosse usato in relazione alle persone fisiche interessate»[66]. Come già accennato, tali pratiche sono vietate nell'UE, ai sensi dell'art. 5 AIA. Tuttavia, l'utilizzo dei sistemi di identificazione biometrica remota in *real-time* in spazi accessibili al pubblico a fini di attività di contrasto è consentito solo se si è in presenza di situazioni emergenziali[67], quali: «i) la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse; ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico; iii) la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'allegato II, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni»[68]. Il paragrafo 2 introduce, poi, ulteriori specifiche per ciò che attiene tale sistema. Il suo utilizzo può avvenire solo per confermare l'identità della persona interessata, tenendo conto della gravità del danno in caso di mancato utilizzo e, viceversa, delle conseguenze per i diritti e le libertà di tutte le persone interessate. Inoltre, l'uso del sistema di identificazione biometrica remota «in tempo reale» deve essere prima autorizzato dall'autorità di contrasto, la

[62] *AI Act*, considerando 41.
[63] *AI Act*, considerando 42.
[64] *Ibidem.*
[65] *AI Act*, considerando 17.
[66] *Ibidem.*
[67] A differenza del DSA – in cui il meccanismo di risposta alle crisi e i protocolli di crisi volontari risultano applicabili in contesti normativizzati (come in caso di crisi e/o situazioni di crisi) – l'AIA non normativizza il regime di emergenza e l'utilizzo dei sistemi di identificazione biometrica remota in tempo reale in spazi accessibili al pubblico è contingentato al raggiungimento di obiettivi a fini di attività di contrasto alla criminalità. Per un'analisi più approfondita sulla regolamentazione dell'intelligenza artificiale nel settore dell'identificazione biometrica, si rimanda a: F.P. Levantino, I. Neroni Rezende, *Rischio inaccettabile: usi proibiti*, in O. Pollicino, et al. (cur.), *La disciplina dell'intelligenza artificiale*, Milano, 2025, 188 ss.
[68] *AI Act*, art. 5.1, lett. h).

DPCE online
ISSN: 2037-6677

quale si occupa di completare una valutazione d'impatto sui diritti fondamentali e di registrare il sistema nella banca dati UE. Tuttavia, dinnanzi a situazioni di estrema emergenza, lo stesso può essere utilizzato anche senza la registrazione nella banca dati UE, a condizione che la stessa venga completata senza alcun ritardo. I suddetti sistemi, in aggiunta, prima di essere impiegati necessitano di «un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente, la cui decisione è vincolante, dello Stato membro in cui deve avvenire l'uso [...]»[69]. Anche in questo caso, tuttavia, qualora si verificasse una situazione impellente, la tecnologia in questione può essere utilizzata ugualmente se e solo se l'autorizzazione viene richiesta senza indebito ritardo (al massimo entro 24 ore). Se l'autorizzazione non dovesse essere concessa, invece, il sistema di identificazione biometrica cesserebbe la sua funzione e tutti i dati raccolti verrebbero eliminati.

Agli Stati membri, infine, spetta il compito di decidere se autorizzare, in parte o totalmente e ai fini dell'applicazione della legge, l'uso di queste tecnologie di IA purché non si violino le condizioni di cui al paragrafo 1, 2 e 3. Le autorità nazionali, se del caso, stabiliscono «nel proprio diritto nazionale le necessarie regole dettagliate per la richiesta, il rilascio, l'esercizio delle autorizzazioni di cui al paragrafo 3, nonché per le attività di controllo e comunicazione ad esse relative»[70]. Tali regole, poi, vanno notificate alla Commissione entro 30 giorni dalla loro adozione. Ciononostante, nulla vieta agli Stati di vietare completamente l'uso dei sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto.

Tuttavia, come già discusso nell'analisi riguardante il DSA, anche in questo caso sorgono delle considerazioni relative all'implementazione di tali sistemi di intelligenza artificiale, i quali, in situazioni emergenziali e/o di crisi, potrebbero avere riflessi negativi soprattutto sulla tutela dei diritti fondamentali. In primo luogo, essi potrebbero dar vita, in alcuni frangenti, a risultati non accurati, che genererebbero falsi-positivi o falsi-negativi dei volti catturati e, di conseguenza, false decisioni. Al di là di un mero "errore tecnologico"[71], esistono varie forme di manipolazione delle immagini, i c.d. *deepfake*, in grado di ingannare tali sistemi di identificazione biometrica. Pertanto, ai limiti tecnologici poc'anzi menzionati è associato il rischio di intaccare l'art. 21 della Carta dei diritti fondamentali dell'UE, ovvero quello relativo alla non discriminazione. Si pensi, a tal proposito, a ciò che è accaduto negli Stati Uniti, dove diversi cittadini afroamericani sono stati arrestati «sulla base di errori compiuti da sistemi di riconoscimento facciale, i quali vengono tratti in inganno dal colore della pelle o della conformazione del viso, senza che agli interessati venisse concessa prontamente

[69] *AI Act*, art. 5.3.
[70] *AI Act*, art. 5.5.
[71] Si pensi al c.d. *black box problem*, con il quale si fa riferimento sia a «recording device, like the data-monitoring systems in planes, trains and cars» e sia «a system whose workings are mysterious; we can observe its inputs and outputs, but we cannot tell how one becomes the other» in F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Cambridge, 2015, 3.

l'opportunità di smentire gli algoritmi»[72]. Nondimeno, il legislatore europeo, conscio dei pericoli derivabili da simili tecnologie, ha scelto di adottare delle misure di sicurezza, assegnando un ruolo di primaria importanza alla componente umana. Ciò è riscontrabile, in particolare, all'art. 14 del presente regolamento, concernente l'obbligo di sorveglianza umana grazie al quale l'uomo è in grado di supervisionare il lavoro della macchina al fine di prevenire o ridurre eventuali rischi per la salute, la sicurezza o i diritti fondamentali.

In secondo luogo, sebbene perimetrati a circostanze eccezionali e non ordinarie, i sistemi di identificazione biometrica remota in tempo reale celerebbero pericoli relativi alla profilazione e alla privacy dei cittadini. Vale la pena ricordare che tali dispositivi utilizzano dati biometrici nel processo di identificazione e sono annoverabili, quindi, nella categoria dei dati personali come previsto dal GDPR (art. 4), dalla Direttiva UE n. 2016/680 (art. 3) e dallo stesso *AI Act* (art. 3). E come tali necessitano di estrema attenzione. Si prenda, ad esempio, il caso in cui i sistemi di identificazione biometrica vengano utilizzati, all'interno di uno spazio accessibile al pubblico, per localizzare un individuo sospettato di aver commesso un reato. Si supponga, poi, che al medesimo luogo abbiano avuto accesso anche altre persone, diverse da quella ricercata. A questo punto sembrerebbe lecito chiedersi se i dati di tali soggetti vengano utilizzati in qualche modo o se, data la loro scarsa utilità ai fini di attività di contrasto, subiscano un'immediata cancellazione? Sebbene risulti chiaro che l'impiego di tali sistemi sia subordinato al verificarsi di eventi estremi e non convenzionali, è altrettanto importante sottolineare come alle persone non interessate dalla straordinaria disposizione sia garantita la tutela dei diritti fondamentali, quali il diritto alla libertà e alla sicurezza (art. 6), il rispetto della vita privata e della vita familiare (art. 7) e la protezione dei dati di carattere personale (art. 8). Se ciò non fosse garantito, si aprirebbe uno scenario nel quale sussiste il pericolo di «invade the privacy of people unaware of the identification process and their identity in a huge and uncontrollable way»[73].

In aggiunta, è possibile menzionare la pronuncia della Corte europea dei diritti dell'uomo intervenuta, per la prima volta, con riferimento alle tecnologie di riconoscimento facciale (appartenenti alla macrocategoria delle tecnologie biometriche), in merito al caso *Glukhin c. Russia* del 4 luglio 2023[74]. In breve, l'organo ha accolto positivamente le istanze presentate da

[72] G. Mobilio, *Tecnologie di riconoscimento facciale*, *op. cit.*, 106. Inoltre, secondo uno studio condotto dal Massachusetts Institute of Technology (MIT) e dalla Standard University, i *software* di analisi facciale mostrano tasso di errore mai superiori dello 0,8% per gli uomini bianchi e superiori al 34% (in due casi su tre) per le donne dalla carnagione scura in L. Hardesty, *Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems*, in *MIT News*, 11-2-2018, https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.

[73] K. Czaplicki, *Use of Artificial Intelligence in Remote Biometric Identification Systems*, in 3(2) *GIS Odyssey J.* 112 (2023).

[74] Corte EDU, no. 11519/20, *Glukhin c. Russia*, 4-7-2023. Sul tema si vedano anche le seguenti analisi: G. Mobilio, *La Corte EDU condanna il ricorso alle tecnologie di riconoscimento facciale per reprimere il dissenso politico: osservazioni a partire dal caso Glukhin c. Russia*, in *DPCE Online*, 2024,1, 695; C. Nardocci, *Il riconoscimento facciale sul "banco" degli imputati. Riflessioni a partire, e oltre, Corte EDU Glukhin c. Russia*, in *BioLaw*, 2024,

DPCE online
ISSN: 2037-6677

Nikolay Sergeyevich Glukhin, arrestato il 30 agosto 2019 dalla polizia russa, a seguito dell'identificazione mediante l'utilizzo di sistemi di riconoscimento facciale, per aver organizzato una manifestazione e aver espresso il proprio dissenso verso il governo di Mosca. La Corte EDU, infine, ha condannato la Russia per aver violato gli articoli 8 (Diritto al rispetto della vita privata e familiare) e 10 (libertà di espressione) della CEDU. Il caso appena citato rappresenta un precedente che potrebbe rivelarsi utile per disciplinare future controversie simili.

Dall'analisi appena condotta, risulta evidente come l'utilizzo dei sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto, seppure in situazioni relative a questioni emergenziali, possano avere un impatto nei confronti dei diritti fondamentali dei cittadini. Una circostanza analoga a quanto già affermato in precedenza sui rischi ascrivibili al DSA in momenti di crisi[75].

4. Considerazioni conclusive

Il *Digital Services Act* e l'*Artificial Intelligence Act* rappresentano il tentativo concreto del legislatore europeo di rispondere ad annose questioni che rischiano di destabilizzare le democrazie europee, in ragione della diffusione dei contenuti illegali e/o disinformativi presenti nell'ambiente digitale.

Per quanto concerne il DSA, al di là di aspetti già messi in luce in presenza di situazioni di crisi e/o emergenziali, il legislatore europeo ha scelto di inserire nella sfera della tutela dei diritti fondamentali dei cittadini i grandi *player online*. Piattaforme e motori di ricerca, nonostante un grado di responsabilità più stringente, continuano ad avere – seppur sotto la supervisione della Commissione europea – un potere importante nel decidere cosa sia disinformazione e cosa non lo sia o nello stabilire se un contenuto rientri o meno nella categoria dei contenuti illegali. Da questo consegue che i suddetti attori hanno la possibilità, durante le attività di moderazione, di rimuovere contenuti non disinformativi o, al contrario, di non procedere alla rimozione di quelli chiaramente ingannevoli. Inoltre, si tratta di attori che hanno come unico obiettivo quello di conseguire utili e, dunque, il loro operato resta improntato alla logica capitalistica del profitto. Di conseguenza sembrerebbe possibile affermare che, nell'esercitare l'importante ruolo assegnatogli dall'UE, essi risponderanno, in prima battuta, a tale logica e non certo a quella – ispirata ai valori iscritti nelle Costituzioni – che invece orienta l'operato dei pubblici poteri, sia nazionali che europei. Il pericolo è che così facendo si possa incidere sulla delicatissima sfera dell'informazione pubblica con l'intermediazione di poteri che assomigliano sempre più a servizi pubblici e che si confrontano con Stati membri e Unione europea dall'alto di significative posizioni di forza, assurgendo al ruolo di nuovi "censori" della libertà di manifestazione del pensiero. Coinvolgere i colossi digitali nell'esercizio della libertà di espressione e d'informazione è la strada giusta da intraprendere? In questo modo il DSA non finirebbe per accrescere

1, 279; G. Gallo, *Tecnologie di riconoscimento facciale e diritti fondamentali a rischio: il caso Glukhin c. Russia dinanzi alla Corte europea dei diritti dell'uomo*, in *Media Laws*, 2023, 3, 189.

[75] Cfr., *supra*, § 3.

il loro potere anziché limitarlo? E, ancora: il pluralismo, elemento essenziale per il corretto funzionamento dei nostri ordinamenti costituzionali-democratici, ne viene rafforzato da tale provvedimento? Tutti interrogativi che solo le prime applicazioni del regolamento potrebbero chiarire. Ciò che preme sottolineare è il tentativo dell'UE di intervenire con vari strumenti per rendere più sicuro l'ambiente digitale. Una volontà che appare evidente anche e soprattutto in relazione ai "timidi" tentativi regolatori delle piattaforme e dei motori di ricerca *online* all'alba dei primi codici di condotta.

Con l'approvazione del recente *AI Act*, invece, l'UE dal canto suo, conscia dei potenziali pericoli provenienti da tali sistemi basati sull'IA, è stata la prima autorità sovranazionale a dotarsi di un regolamento che possa bilanciare il progresso tecnologico con la salvaguardia dei diritti fondamentali. Una sfida rischiosa e complicata, a cui questo *unicum* a livello normativo tenta di rispondere mediante un approccio orizzontale e *risk-based*. Particolare menzione merita l'articolo 5 dell'*AI Act*, che individua le pratiche di intelligenza artificiale vietate. Tra queste, come ampiamente illustrato, figurano i sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto. Fin dalla proposta iniziale – pubblicata nell'aprile 2021 dalla Commissione europea – i dibattiti maggiori hanno riguardato proprio questa tecnologia specifica. Il legislatore europeo, di conseguenza, ne ha vietato l'uso per attività di contrasto tranne in tre casi ben circoscritti. Ciononostante, la difficile salvaguardia dei diritti fondamentali, in particolare gli artt. 7, 8, 10, 11, 12 e 21 della Carta dei diritti fondamentali dell'UE ("Carta"), continua a tenere banco. Trattandosi di per sé di tecnologie "invasive", l'Unione europea ha tracciato la strada da percorrere anche per gli Stati membri, i quali possono attenersi, sul piano nazionale, al modello europeo o vietare completamente l'uso di tali sistemi di identificazione. Si tratta, pertanto, di una delimitazione importante per evitare di far sì che l'impiego di simili tecnologie non porti le istituzioni statali ad abusarne per ragioni di ordine pubblico o per il rafforzamento del proprio potere interno, come nel caso delle tecnologie di riconoscimento facciale da parte di alcuni Paesi della c.d. BRICS (Cina, Russia e India)[76].

All'Unione europea è attribuibile il merito di aver cercato quantomeno di gettare le basi presenti e future per la regolamentazione dell'intelligenza artificiale e delle nuove tecnologie o, come sottolineato da alcuni, di aver tentato una scommessa: quella della

> «'fuga in avanti' rispetto agli altri competitor mondiali – tra cui gli USA – scommettendo sulla armonizzazione normativa e sulla certezza del diritto per gli operatori, con l'obiettivo di recuperare posizioni sul piano dello sviluppo tecnologico e – perché no – garantire ai cittadini dell'UE un quadro maggiormente rispettoso dei diritti fondamentali»[77].

[76] A. Mitka, *The Use of 'Real Time' Remote Biometric Identification Systems for Law Enforcement – Comments in Light of Legislative Work on the Artificial Intelligence Act*, in 21 *Int'l Eur. & Compar. L. Rev.* 183, 188 (2023).
[77] A. Orlando, *La regolamentazione delle tecnologie di riconoscimento facciale nell'UE e negli USA: alea iacta est?*, in *DPCE Online*, 2024, 2, 1128.

DPCE online
ISSN: 2037-6677

Solo il tempo e le prime applicazioni in materia potranno avvalorare o meno la strada legislativa intrapresa dall'Unione europea. Occorre, infine, notare che lo sviluppo tecnologico, e nello specifico quello dell'intelligenza artificiale, non fermerà certamente la sua corsa. E, di fronte ad una simile situazione, è necessario che il regolatore si faccia trovare pronto per non dissipare quanto già fatto ed evitare di incappare nel c.d. *pacing problem* ed escludere, così, che diritto e tecnologia viaggino a ritmi completamente diversi.

Andrea Spaziani
Dip.to di Scienze Politiche
Università degli Studi di Teramo
aspaziani@unite.it