

Proposta di legge di Noi Moderati Presentata alla Camera dalle deputate Carfagna, Semenzato, Brambilla e Cavo
Presentata al Senato dalle senatrici Gelmini e Versace

“Disposizioni in materia di tutela dell'identità personale e dell'integrità dell'immagine contro le riproduzioni digitali non autorizzate e per il contrasto della diffusione di contenuti illegali nella rete internet”

Onorevoli Colleghi!

Negli ultimi anni, lo sviluppo dell'intelligenza artificiale ha consentito la creazione di contenuti digitali iper-realistici capaci di simulare l'aspetto, la voce e i movimenti di una persona reale. Tali contenuti, comunemente noti come *deepfake*, pongono gravi rischi per la reputazione, la privacy, la sicurezza e la dignità delle persone.

Secondo uno studio pubblicato da Deeptech Labs, il numero di video *deepfake* disponibili online è aumentato del 900% tra il 2018 e il 2023. Inoltre, il 96% del materiale rilevato nel 2023 è stato utilizzato per fini non consensuali o illeciti, inclusi contenuti diffamatori, pornografia non autorizzata, disinformazione politica e truffe finanziarie.

Attualmente l'ordinamento italiano non prevede una normativa specifica sui *deepfake*, affidandosi a disposizioni generali in materia di tutela della privacy, diffamazione, o violazione del diritto d'autore.

In Europa, solo il Ministero della Cultura danese ha recentemente presentato una proposta di legge che rafforza la protezione dell'identità personale tramite l'introduzione di un diritto esclusivo sulla propria immagine e voce, esteso anche alle performance artistiche.

Fermo restando il contributo fondamentale della rete internet all'universalizzazione della conoscenza e dell'informazione, come anche al collegamento—attraverso siti web e piattaforme di condivisione—di milioni di utenti e migliaia di istituzioni provenienti da tutto il mondo, negli ultimi anni si stanno intensificando le attività illegali a mezzo web, anche grazie all'ausilio di nuove e nuovissime tecnologie quale l'Intelligenza artificiale generativa. Tali attività illegali spesso comportano la pubblicazione, da parte degli utenti o degli stessi gestori dei siti web e delle piattaforme di condivisione, di contenuti illegali di varia natura (testuale o audiovisiva).

L'identificazione, nelle ultime settimane, di numerosi siti web a sfondo sessista - che calpestano e offendono la dignità non solo delle donne direttamente coinvolte, ma del genere femminile nel suo insieme - ha mostrato come i responsabili della pubblicazione e condivisione di contenuti illegali si nascondano dietro il privilegio dell'anonimato, cosa che al momento possono fare in quanto non sussistono obblighi, per i gestori, né di acquisizione dell'identità digitale degli utenti che pubblicano e condividono contenuti, né di contrasto della diffusione dei contenuti illegali. Il presente disegno di legge mira a colmare questa lacuna, stabilendo anche regole più stringenti per la pubblicazione di contenuti realizzati mediante l'uso dell'Intelligenza artificiale generativa.

Il diritto all'anonimato può continuare a sussistere online, purché chi lo esercita non travalichi i confini della legalità. Qualora accada, è giusto che le autorità competenti possano identificare tempestivamente chi si sospetta che abbia infranto la legge. A maggior ragione considerato che viviamo in un mondo in cui i media facenti capo alla rete hanno un peso

preponderante, e sempre più ne avranno negli anni a venire. Oltretutto è la stessa natura capillare della rete - il meccanismo dei like e della condivisione istantanea e indiscriminata - a coadiuvare la rapida diffusione di contenuti illegali, molto più della pagina di un giornale o una trasmissione TV. All'inizio di quest'anno la Direttrice esecutiva di Europol, Catherine De Bolle, ha giustamente ribadito che l'anonimato non è un diritto inalienabile degli utenti della rete, e che i gestori dei siti web e delle piattaforme hanno la responsabilità di condividere con le forze dell'ordine le informazioni personali degli utenti sospettati di aver commesso un cybercrimine - che sia esso a sfondo sessuale come quelli venuti alla luce o ascrivibili alla sfera del pericoloso hate speech.

Già nel 2015, l'Unione Europea ha preso posizione contro fenomeni d'odio a mezzo web, attraverso la raccomandazione di politica generale n. 15 della Commissione contro il razzismo e l'intolleranza del Consiglio d'Europa. I minorenni, soprattutto i più fragili e vulnerabili, tendono a subire il peggio di queste dinamiche, come ha illustrato l'ultimo rapporto (risalente al 2023) del servizio analisi criminale del Dipartimento della pubblica sicurezza, che documenta l'esposizione crescente dei minori in rete all'adescamento, al cyberbullismo e al revenge porn.

Nella presente legislatura, il Parlamento è intervenuto in tal senso attraverso il Decreto-legge 15 settembre 2023, n. 123, convertito, con modificazioni, dalla legge 13 novembre 2023, n. 159, che introduce delle importanti disposizioni per la sicurezza dei minorenni in ambito digitale. Questo a integrazione del regolamento UE 2022/2065 del Parlamento europeo e del Consiglio (19 ottobre 2022) - il cosiddetto Digital Service Act (DSA) - che ha modificato la direttiva CE 2000/31 prescrivendo misure severe di contrasto della diffusione di contenuti illegali online. L'adozione di normativa nazionale integrativa è tra l'altro prevista dallo stesso DSA.

Allo stesso modo, il 25 giugno di quest'anno, il Parlamento ha approvato una legge delega in materia di Intelligenza artificiale. Si tratta della prima norma italiana in materia di IA e un primo passo in funzione dell'adeguamento della normativa del nostro Paese al regolamento UE 2024/1689 del Parlamento Europeo e del Consiglio (1 agosto 2024) - il cosiddetto EU AI Act. Ma riteniamo che sia necessario intervenire tempestivamente per obbligare i gestori a segnalare adeguatamente la pubblicazione di contenuti realizzati mediante l'uso dell'Intelligenza artificiale generativa. Da qui l'inclusione dell'Intelligenza artificiale generativa nel disegno di legge.

Attraverso la presente proposta di legge si vuole tutelare maggiormente sia chi vede la propria immagine, senza consenso, manipolata sia chi è vittima di raggiri spesso economici derivanti dalla diffusione di *deepfake*.

Si intende introdurre il reato di diffusione fraudolenta di contenuti *deepfake*, prevedendo un aggravamento di pena in caso di *deepnude* o ove il reato venga commesso ai danni di persona offesa minore di età o di soggetto vulnerabile e regolamentare la responsabilità dei prestatori dei servizi intermediari.

Art. 1

(Definizioni)

1. Ai fini della presente legge, si intende per:

1. Chiunque generi o diffonda *deepfake* prodotti con sistemi di intelligenza artificiale è tenuto a integrare una marcatura esplicita, da rendere visibile all'atto della pubblicazione.

a) *deepfake*: un'immagine o un contenuto audio o video generato o manipolato da programmi informatici o applicazioni digitali, anche mediante sistemi di intelligenza artificiale, che assomiglia a persone, oggetti, luoghi, entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona;

b) gestori: i prestatori di servizi intermediari, come definiti ai sensi del regolamento UE 2022/2065 del Parlamento europeo e del Consiglio (19 ottobre 2022), i cui servizi online pubblicano e diffondono in Italia immagini, video e contenuti di altra natura inseriti da parte degli utenti.

c) log: i registri informatici che documentano le operazioni compiute in relazione alla pubblicazione, modifica o rimozione di contenuti digitali, comprensivi di dati tecnici utili all'individuazione dell'autore e alle verifiche delle autorità competenti.

Art. 2

(Marcatura obbligatoria per deepfake prodotto con sistemi di intelligenza artificiale)

Art. 3

(Compiti di controllo e vigilanza del Garante per la protezione dei dati personali e dell'Autorità per le garanzie nelle comunicazioni)

1. L'Autorità per le garanzie nelle comunicazioni (AGCOM) ha il compito di verificare: a) l'adozione e l'efficacia delle misure di marcatura previste;
2. Il Garante per la protezione dei dati personali può: a) effettuare ispezioni, richieste documentali, audit tecnici; b) segnalare alla competente autorità sanzionatoria eventuali omissioni.

Art. 4

(Obblighi dei gestori)

1. I gestori sono tenuti a: a) integrare sistemi obbligatori di identificazione degli utenti, mediante documento di identità o strumenti di identità digitale riconosciuti (SPID, CIE, eIDAS), per l'iscrizione alle piattaforme digitali; b) predisporre meccanismi rapidi per la segnalazione e la rimozione dei contenuti *deepfake* non autorizzati; c) nominare un responsabile del monitoraggio dei contenuti, pubblicati dagli stessi gestori

o dagli utenti, che sono stati realizzati mediante l'uso di intelligenza artificiale;

- d) definire idonee procedure per il riconoscimento di contenuti realizzati mediante l'uso di intelligenza artificiale;
- e) conservare per almeno 12 mesi i dati tecnici relativi alla pubblicazione del contenuto segnalato;
- f) fornire tempestivamente all'autorità giudiziaria *log* e dati tecnici utili all'individuazione degli autori di contenuti illeciti;
- g) consentire all'utente la rimozione immediata e gratuita dei contenuti dallo stesso immessi all'interno delle piattaforme digitali, fermo restando l'obbligo di cui alla lettera e);
- h) eseguire senza indugio gli ordini di oscuramento o rimozione di account e contenuti impartiti dall'AGCOM.

Articolo 5

(Regolamento AGCOM)

1. L'AGCOM stabilisce, entro novanta giorni dalla data di entrata in vigore della presente legge, sentito il Garante per la protezione dei dati personali, le modalità tecniche e di processo che i gestori sono tenuti ad adottare per il rispetto degli obblighi sanciti dall'articolo 5. Entro nove mesi dall'entrata in vigore della presente legge, i gestori devono dotarsi, qualora non abbiano già provveduto, di sistemi adeguati per adempiere agli obblighi di cui sopra.

Articolo 6

(Sanzioni)

1. L'AGCOM vigila sulla corretta applicazione della presente legge e, in caso di inadempimento, contesta ai gestori, anche d'ufficio, la violazione, ai sensi della legge 31 luglio 1997, n. 249, all'articolo 1, e li diffida ad adeguarsi entro trenta giorni. In caso di inottemperanza, l'AGCOM procede all'oscuramento delle piattaforme diffuse fino al ripristino, da parte dei gestori, di condizioni di erogazione del servizio conforme alla richiesta dell'AGCOM.

2. Ai gestori non ottemperanti agli obblighi di acquisizione dell'identità digitale degli utenti di cui all'articolo 5, comma 1, lettera a), si applica la sanzione amministrativa pecuniaria da 200.000 a 1.000.000 euro.

3. Ai gestori non ottemperanti agli obblighi di cui all'articolo 5, comma 1, lettere da b) a h), si applica la sanzione amministrativa pecuniaria da 100.000 a 500.000 euro.

4. Contro le decisioni dell'AGCOM ai sensi del presente articolo è sempre ammesso il ricorso al giudice ordinario.

Art. 7

(Diffusione fraudolenta di contenuti deepfake)

1. Dopo l'articolo 171-ter della legge 22 aprile 1941, n. 633, è inserito il seguente:

“Art. 171-quater

(Diffusione fraudolenta di contenuti deepfake)

1. Chiunque, al fine di danneggiare, ingannare, ottenere un profitto o ledere la reputazione di terzi, diffonde contenuti *deepfake* senza il consenso delle persone rappresentate, è punito con la reclusione da uno a cinque anni o con la sanzione amministrativa pecuniaria da euro 10.000 a euro 100.000. La pena è aumentata se il contenuto è a carattere sessualmente esplicito o ha ad oggetto minori o soggetti vulnerabili.

2. Non costituisce reato la diffusione di contenuti che, pur rientrando nella definizione di cui al comma 1, siano chiaramente destinati a fini di satira, parodia o espressione artistica, purché non ledano in modo concreto la dignità, la reputazione o la sicurezza delle persone.

3. Il reato è perseguibile d'ufficio se commesso a danno di minori o con finalità discriminatorie.”

Art. 8

(Clausola di invarianza finanziaria)

1. Dall'attuazione della presente legge non derivano nuovi o maggiori oneri a carico della finanza pubblica.

2. Le amministrazioni competenti provvedono agli adempimenti con le risorse umane, finanziarie e strumentali disponibili a legislazione vigente.