Il riconoscimento biometrico alla luce della proposta di Regolamento Europeo sull'Intelligenza Artificiale: rischio "sorveglianza di massa" sventato in parte (per ora)

25 Gennaio 2024

di **Anna Licastro**

Il 9 dicembre del 2023 si è chiusa la trattativa sulla proposta di Regolamento Europeo in materia di Intelligenza Artificiale che ha visto coinvolti Commissione, Parlamento e Consiglio. L'accordo politico raggiunto dal "trilogo" vede l'Unione Europea fregiarsi, in materia di regolazione, ancora una volta del titolo di *primus inter pares*. Nella gara per la supremazia tecnologia, anche in tema di biometria, ciò che conta per le istituzioni eurounitarie è arrivare prima degli Stati Uniti, prima della Cina. Il timore di delegare alle due superpotenze la *governance* del digitale in territorio europeo è davvero troppo elevato per cui si è preferito afferrare il timone del potere trasformativo dei sistemi di AI per guidarne lo sviluppo sicuro, affidabile ed etico mediante un ampio quadro normativo rispettoso non solo della disciplina vigente in materia di diritti fondamentali e sicurezza, ma anche dei valori fondativi dell'Unione.

Una delle questioni più discusse sul tavolo dei negoziati ha riguardato la portata del divieto di riconoscimento facciale, una delle molteplici tecnologie biometriche che, per il tramite del trattamento algoritmico di immagini di volti umani precedentemente raccolte, è in grado di riconoscere automaticamente gli individui per "autenticarli" o identificarli. Il volto, come d'altra parte il DNA, le impronte digitali, l'iride, l'andatura e persino l'odore sono dati biometrici che consentono l'identificazione univoca della persona. Con riguardo alle tecnologie di riconoscimento facciale, la proposta prende in considerazione i sistemi di categorizzazione e di identificazione biometrica. I primi non si prefiggono come scopo principale di identificare la persona, quanto piuttosto di ricondurre il dato biometrico, estratto dall'immagine di un volto, come ad esempio l'età, l'etnia o il genere, ad una o più categorie in cui la persona può essere inserita, o meglio, classificata. È il caso dei tratti somatici di un viso che, una volta raccolti e processati da algoritmi di riconoscimento, consentono di risalire per l'appunto all'etnia di appartenenza della persona monitorata. I secondi, invece, si basano su una comparazione uno a molti (c.d. *one-to-many biometric systems*) in cui il modello biometrico costruito dall'algoritmo in base alle caratteristiche facciali processate, viene confrontato con volti simili presenti all'interno di una banca dati che ne raccoglie uno svariato numero. Non si verifica alcun contatto fisico fra il sistema di identificazione (una telecamera) ed il soggetto da identificare, tutte le operazioni di riconoscimento si effettuano a distanza. Il confronto e la verifica automatizzata possono avvenire all'istante oppure *ex post* a partire da immagini contenute in filmati video, già precedentemente registrate o reperite su Internet (in tale ultimo caso, si parla di *web scraping*).

La proposta di regolamento ha vietato in modo assoluto la categorizzazione biometrica ed i sistemi di identificazione remota "in tempo reale" o "a posteriori" usati in spazi accessibili al pubblico perché ritenute dal "trilogo" troppo pericolose. Rischi di discriminazione sono probabili e laddove si verificassero, sarebbero inaccettabili anche perché si porrebbero in palese contrasto con l'osservanza del articolo 21 della Carta di Nizza che vieta qualsiasi forma di discriminazione basata su sesso, razza, colore della pelle, origine etnica, lingua, opinioni politiche comprese le caratteristiche genetiche della persona.

In gioco, dunque, i diritti fondamentali quali il rispetto della vita privata, la tutela dei dati personali, a partire dagli stessi principi generali da rispettare nel trattamento dei dati personali (trasparenza, correttezza, finalità, *data minimization*, necessità e proporzionalità) o la stessa libertà di riunione visto che si potrebbero scoraggiare i cittadini dal partecipare a manifestazioni pubbliche e dall'esprimere le proprie idee. Sarebbe davvero intollerabile vedersi "schedati" in banche dati per aver semplicemente espresso le proprie opinioni. Ad essere pregiudicata, infine, è la pietra angolare sul quale si erige il diritto costituzionale europeo: l'ineludibile rispetto della dignità umana. Per tale ragione, è prevalsa la linea sostenuta dal Parlamento secondo cui la tutela dei diritti inviolabili

della persona va ritenuta prevalente sulle logiche di mercato e sulle istanze di potenziamento di misure di sicurezza nazionale.

Al divieto assoluto di utilizzo di questi sistemi, fanno da contraltare una serie di casi – ben circoscritti – in cui il ricorso a queste tecnologie è ammesso, previa autorizzazione giudiziaria. Gli strumenti di identificazione biometrica, in tal caso, vengono classificati quali sistemi di AI ad alto rischio la cui immissione nel mercato è subordinata ad una previa valutazione di conformità.

L'articolo 5, paragrafo 1, *lett. d)* elenca fra questi:

1. la ricerca di potenziali vittime di reato (il sequestro di persona);
2. la prevenzione da minaccia di attacchi terroristici;
3. l'identificazione e localizzazione di una persona sospettata di aver commesso un grave reato (terrorismo, pedopornografia, crimini ambientali o contro l'umanità, per citarne alcuni).

Nei casi poc'anzi descritti, la proposta richiede di effettuare un corretto bilanciamento fra le conseguenze che si sarebbero prodotte per il mancato uso delle tecnologie biometriche e la valutazione dell'impatto che esse potrebbero avere sulla tutela dei diritti fondamentali, laddove, al contrario, il loro uso si renda necessario e venga eccezionalmente autorizzato. Considerato, inoltre, il pericolo piuttosto frequente di eventuali corrispondenze non corrette in fase di identificazione, il testo della proposta ha previsto, come per tutti i sistemi ad alto rischio, una supervisione umana nell'utilizzo degli stessi. Ne deriva che il risultato prodotto dal sistema di identificazione biometrica deve essere, dunque, verificato e confermato separatamente da almeno due persone fisiche prima che, in forza dello stesso, venga assunta qualsiasi decisione. Ritorna, quindi, l'idea che il riconoscimento biometrico, debba essere, al pari di molti altri sistemi di AI, valutato secondo un approccio umanistico ed antropocentrico attribuendo, dunque, all'essere umano un ruolo di primo piano nel processo di «re-ontologizzazione del digitale», come ricorda Luciano Floridi. Difatti, eventuali *bias* rendono questi strumenti tecnologicamente immaturi e come tali defettibili, se lasciati liberi di operare senza alcun intervento umano.

È pur vero che, nella lotta al terrorismo, a partire dai tragici eventi dell'11 settembre 2001, la sorveglianza sociale attuata per il tramite dei sistemi di identificazione biometrica ha rappresentato per i governi nazionali l'unica risposta possibile nei confronti di una crescente richiesta di sicurezza. Una finalità che si è voluto far prevalere su tutte le altre, compresa la tutela della *privacy*. C'è da domandarsi se gli Stati negli anni non si siano lasciati prendere un po' troppo la mano. L'ansia spasmodica di raccogliere informazioni sui propri cittadini e processarle per il tramite di sistemi algoritmici predittivi al fine di fermare *ex ante* eventuali minacce per l'incolumità pubblica, pare aver spinto i governi nazionali ad auto-generare un sistema di controllo governativo talmente pervasivo da trasmutarsi in sorveglianza di massa. È vero, infatti, che in un aeroporto sistemi di riconoscimento facciale in tempo reale, messi in molti casi a disposizione delle forze dell'ordine per i relativi controlli di sicurezza agli imbarchi, consentono di effettuare, senza che vi sia alcun contatto col passeggero, verifiche istantanee con notevoli risparmi di tempo, ma chi garantisce al cittadino che quel sistema sviluppato da un'impresa privata, magari una delle note *Big Tech*, non sia usato per scopi di *marketing* o commerciali, senza che sia stato espresso il previo consenso per il perseguimento di finalità ulteriori rispetto a quelle iniziali? Quale prezzo, dunque, pagherebbero i cittadini per effetto di un'identificazione biometrica senza limiti? Per farsene un'idea, anche approssimativa, basterebbe volgere lo sguardo ad Oriente. In Cina, le tecnologie di riconoscimento biometrico sono talmente diffuse che la Cyberspace Administration of China ha proposto di vietarne l'uso non solo all'interno delle strutture ricettive e museali, ma anche nei camerini dei negozi e nei bagni pubblici.

Un esempio evidente dell'esercizio del potere pubblico cinese per scopi di controllo di massa si registra non solo nell'uso spregiudicato dei sistemi di riconoscimento facciale, ma anche nell'adozione dei sistemi di *social scoring* grazie ai quali si attribuisce un punteggio sociale alle persone a partire dai loro comportamenti. Già nel 2014 il Presidente XI Jinping ha proposto di istituire un sistema di crediti sociali (SCS) in cui il controllo governativo sistemico delle informazioni relative alle condotte di imprese e cittadini si traduce nell'attribuzione ad ognuno di essi di un punteggio, previa preventiva valutazione della loro affidabilità creditizia e reputazione sociale. Al momento, la Cina sembra aver fatto un passo indietro sull'uso di quello che pare essere un vero e proprio sistema

di sorveglianza digitale su base reputazionale, applicato per ora solo alle imprese. Tuttavia, il rischio di una sua estensione a tutti i cittadini cinesi pare possibile e, tra l'altro, non sembra che XI Jinping vi abbia rinunciato del tutto.

Spiare ogni azione mediante un'intrusione incontrollata, significa non solo mandare in fumo il «nucleo duro dell'esistenza della persona, […] l'indecidibile», come sostiene Stefano Rodotà, ma anche gli ideali e i valori di una società democratica governata dallo Stato di diritto, come è stato di recente affermato dalla stessa Corte Europea dei Diritti dell'Uomo, chiamata a pronunciarsi sull'uso della tecnologia di riconoscimento facciale per la localizzazione e l'arresto di un cittadino russo nel corso di una manifestazione pacifica (Corte Europea dei Diritti dell'Uomo, *Glukhin v.* Russia, decisione del 4 luglio 2023, n. 11519/20).

Il testo approvato dal "trilogo" sembra sventare il rischio di "sorveglianza di massa" generalizzata almeno per ora. Nei prossimi incontri saranno i tecnici a dover "perfezionare" la proposta. Si passerà poi all'approvazione finale da parte del Parlamento. Sino a quel momento, meglio essere cauti e sperare che l'uso dei sistemi di identificazione biometrica non ritorni ad avere la meglio, questa volta in via definitiva, sullo Stato di diritto che si prefigge di garantire i diritti nei confronti del potere, anche di quello digitale e, fra i diritti, lo insegna Stefano Rodotà, il rispetto della dignità umana rappresenta un limite invalicabile; il che non è poca cosa, ricordiamocelo.

Riferimenti bibliografici

Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale, Bruxelles, 21 aprile 2021, COM (2021) 206 final, disponibile *online* nell'ultima versione.

A. APOSTOLI, *La dignità sociale come orizzonte della uguaglianza nell'ordinamento costituzionale*, in *Costituzionalismo*, n.3, 2019, pp.1-36;

B. MARCHETTI, L. PARONA, *La regolazione dell'Intelligenza Artificiale: Stati Uniti e Unione Europea alla ricerca di un possibile equilibrio*, in *DPCE online*, n.1, 2022, pp.237- 252;

F. BILANCIA, *Gli interessi finanziari dell'Unione europea e il mutamento della concezione (europea) della Rule of Law,* in *Diritto Pubblico*, n.3, 2022, pp. 677-702;

G. BELLOMO, *Biometria e digitalizzazione della pubblica amministrazione,* in L. Ferrara, D. Sorace, *A 150 anni dall'unificazione Amministrativa Italiana*, Vol. IV, S. Civitarese Matteucci, L. Torchia (a cura di), *La tecnificazione*, Firenze University Press, Firenze, 2016, pp. 60-72;

K. CRAWFORD, *Né intelligente né artificiale. Il lato oscuro dell'AI*, Il Mulino, Bologna, 2021, pp.5-312;

G. REPETTO, *La dignità umana e la sua dimensione sociale nel diritto costituzionale europeo*, in *Diritto Pubblico*, n. 1, 2016, pp. 247 – 305;

L. FLORIDI, *Etica dell'Intelligenza artificiale. Sviluppi, opportunità, sfide,* Raffaello Cortina Editore, Milano, 2022, pp. 7- 347;

S. RODOTÀ, *Il diritto di avere diritti*, Editori Laterza, Bari, 2012, pp.18-427;

S. CIVITARESE MATTEUCCI, *Umano troppo umano. Decisioni amministrative automatizzate e principio di legalità*, in *Diritto Pubblico*, n.1, 2019, pp. 5-41;

X. QIANG, *President Xi's Surveillance State*, in *Journal of Democracy*, Vol. 30, no.1, January 2019, pp. 53-67.