AI Act all’italiana

Più sorveglianza, meno garanzie, controllori del Governo. I punti critici dei decreti attuativi delle norme europee sull’AI. In un Paese dove la sorveglianza illegale è già oggi un fatto impunito, strumenti tecnologici avanzati a disposizione delle forze dell’ordine senza controllo giudiziario effettivo possono creare una gabbia per i diritti fondamentali rivestita di legalità.

Franco Padella

Pubblicato il 02.07.2026: https://centroriformastato.it/ai-act-allitaliana/

Lo scorso 10 giugno il Consiglio dei ministri ha approvato due decreti legislativi per regolamentare l'uso dell'intelligenza artificiale in Italia[1]. In coerenza con le disposizioni dell'AI Act europeo, il nostro Paese si è mosso per primo in Europa, definendo in un primo atto le autorità di controllo, le norme su lavoro, formazione e alfabetizzazione, e in un secondo decreto la disciplina sull'uso dell'IA nelle attività di polizia. Obiettivo dichiarato: coniugare innovazione tecnologica e rispetto dei diritti fondamentali.

Nel comunicato ufficiale del Governo, cosi come nella conferenza stampa espositiva, viene affermata la piena adesione italiana all’AI Act europeo, valutazione per lo più confermata dalla maggior parte dei commentatori. Le dichiarazioni, tuttavia, non evitano di rimandare alla memoria la opposizione manifestata a suo tempo dal Governo verso norme di maggior garanzia da inserire nell’atto europeo, un dato di per se sufficiente per una lettura più approfondita delle attuali norme approvate.

Nel seguito viene esposta una prima valutazione critica dei contenuti dei decreti così come reperibili in bozza (qui e qui), pur con l’avvertenza che il testo finale approvato potrebbe aver subito delle modifiche nella discussione in CDM.

L'analisi fa emergere un panorama che in più punti stride con l'AI Act europeo, a partire dalle autorità di garanzia previste come indipendenti, ma che tali non sono. A questo si aggiungono, in particolare nel documento relativo all'uso dell'IA nelle attività di polizia, eccezioni, ambiguità e controlli deboli che rischiano di svuotare le garanzie europee, esse stesse indebolite dal *Digital Omnibus*[2].

Parole rassicuranti, ma le norme sono ambigue

In un contesto democratico, disciplinare e limitare l'uso dei sistemi di IA da parte delle forze di polizia in accordo con normative di garanzia individuale è un'azione che non può che essere ben accolta. Punti particolarmente sensibili riguardano la possibilità di etichettare e categorizzare dati biometrici (art. 7), l'identificazione biometrica remota in tempo reale per finalità di prevenzione e ricerca (art. 8), e la creazione di database facciali di tutti i partecipanti a eventi pubblici (art. 10). A supporto della cornice di dichiarata garanzia, viene anche introdotto un nuovo reato per chi altera i sistemi IA od omette misure di sicurezza[3].

Sulla carta, sembra un passo avanti verso una regolazione adeguata. La conferenza stampa governativa avalla questa tesi: il sottosegretario Mantovano ha parlato di "cornice antropocentrica" e di "governare l'innovazione". Il ministro dell'Interno Piantedosi ha garantito: "Nessun Grande Fratello, nessuna schedatura di massa, vietato l'uso di banche dati biometriche create con raccolta massiva e generalizzata di dati dal web. Vietato prendere decisioni che incidano negativamente sulla persona basandosi solo sul risultato del riconoscimento facciale".

Ma è davvero così?

Passiamo al vaglio le affermazioni del ministro dell'Interno. Il decreto autorizza la raccolta dei volti di tutti i partecipanti a eventi pubblici – comprese manifestazioni politiche e sociali – e la loro conservazione per sette giorni in un database locale[4]. Pur non raccogliendo dati dal web, nei fatti viene realizzato un database biometrico di massa senza alcun sospetto individuale. Inoltre, se il riconoscimento facciale non può essere l'unico fondamento per una decisione negativa[5], quale indizio rende il riconoscimento "non unico fatto"? Può, ad esempio, bastare un capo di abbigliamento? La decisione potrebbe essere formalmente basata su più fonti,

ma sostanzialmente rimanere centrata sull'IA. L'ambiguità è un escamotage che rende la norma facilmente aggirabile.

Avendo in memoria un Governo capace di emanare quattro decreti sicurezza in due anni[6], comprensivi di fermi preventivi e DASPO per ragioni previsionali di sicurezza, forse è lecito pensare che pur se non c'è ancora un Grande Fratello, qualcosina di piccolo piccolo sia forse sul punto di nascere.

Cosa non quadra sui dati biometrici

Il cuore del problema sta nella disciplina dei dati biometrici. Nella normativa si evidenziano almeno 5 nodi critici.

Categorizzazione per "somiglianza" e possibilità di discriminazione indiretta.

Il decreto italiano consente l'etichettatura e la categorizzazione di dati biometrici[7], purché non siano finalizzate a dedurre caratteristiche sensibili come razza, religione o orientamento sessuale. L'AI Act, invece, vieta in modo assoluto i sistemi che classificano le persone per dedurre tali caratteristiche[8], senza subordinazione ad alcunché. La formulazione italiana – che richiede solo che la *finalità* non sia discriminatoria – non impedisce che la categorizzazione per somiglianza produca indirettamente cluster etnici o di genere.

Raccolta biometrica di massa in assenza di sospetto.

Viene autorizzata la memorizzazione dei volti di tutti i partecipanti a eventi pubblici – stadi, concerti, manifestazioni politiche, cortei di massa – per sette giorni[4]. L'AI Act vieta espressamente le pratiche di sorveglianza di massa indiscriminata, come lo *scraping* non mirato di immagini facciali da internet o da circuiti chiusi[9]. Il divieto viene semplicemente eluso dal decreto italiano spostando l'attivazione della sola pratica di riconoscimento facciale a dopo la commissione di un reato. Nel frattempo, la raccolta preventiva viene effettuata e rimane a tutti gli effetti un'azione di sorveglianza di massa.

Identificazione biometrica in tempo reale per 15 giorni (prorogabili).

L'autorizzazione del procuratore della Repubblica per l'identificazione biometrica in tempo reale può durare fino a 15 giorni, rinnovabile per altri 15[10]. L'AI Act richiede che l'uso sia "strettamente limitato nel tempo e nel contesto dell'evento specifico"[11]. Quindici giorni, che possono diventare un mese, non sono una "stretta limitazione", ma una sorveglianza continuativa.

Attivazione d'urgenza senza autorizzazione scritta preventiva.

In caso di urgenza viene consentito alla polizia di attivare il sistema di identificazione biometrica in tempo reale con una semplice comunicazione anche orale al pubblico ministero, chiedendo l'autorizzazione entro 12 ore[12]. L'AI Act richiede un'autorizzazione preventiva da parte di un'autorità giudiziaria o amministrativa indipendente[13]. La procedura italiana svuota il controllo giudiziario ex ante.

Notifica al Garante della privacy differibile.

La notifica dell'uso dei sistemi di identificazione biometrica al Garante della privacy può essere ritardata fino a tre mesi (e rinnovata una volta) per esigenze di segretezza[14]. L'AI Act impone la notifica "senza indugio e al più tardi entro 24 ore"[13]. Tre mesi sono una eternità rispetto al termine europeo.

Un piedino nella porta…

In coerenza con l'AI Act, le azioni di polizia predittiva, attraverso strumenti di inferenza digitali in grado di prevedere dove o chi commetterà un reato, non sono autorizzate. Ma la prevista formazione obbligatoria del personale su "analisi predittiva"[15] prepara il terreno per futuri utilizzi, in assenza di un divieto operativo esplicito. L'AI Act europeo vieta esplicitamente la profilazione predittiva individuale basata su tratti della personalità[16], ma lascia spazio a sistemi "location based" o a supporto di valutazioni umane su fatti oggettivi. Il decreto italiano non restringe queste eccezioni. Così, tra formazione, collaborazioni con privati[17] e database biometrici di massa, il "piedino" nella porta verso la polizia predittiva inizia comunque a intravvedersi.

Autorità di controllo: indipendenti o di nomina governativa?

Il punto forse più critico dell'intero impianto dei decreti riguarda chi deve vigilare sull'uso dell'IA e dei suoi strumenti. Vengono designate quali "Autorità nazionali per l'intelligenza artificiale" l'Agenzia per l'Italia Digitale (AgID) e l'Agenzia per la Cybersicurezza Nazionale (ACN)[18]. Entrambe le agenzie hanno vertici nominati dal Consiglio dei Ministri, con un grado di indipendenza politica che non è sbagliato supporre scarso. L'AI Act, in contrasto, richiede autorità di vigilanza indipendenti[19]. Il Garante per la protezione dei dati personali, autorità indipendente con componenti di nomina parlamentare, ha chiesto formalmente di designare l'Agenzia come autorità competente per i sistemi IA ad alto rischio. La sua richiesta è stata sostanzialmente ignorata. Il risultato è un sistema di controlli debole, privo di terzietà e senza risorse aggiuntive. Si investe un miliardo di euro per i sistemi IA, ma zero euro per i controlli indipendenti.

Intanto, in Europa

Mentre l'Italia allarga le maglie dell'AI Act, a Bruxelles si consuma un'operazione parallela e altrettanto preoccupante: il *Digital Omnibus*. Presentato a fine 2025 come un intervento tecnico di "semplificazione" delle norme digitali, è in realtà, come denunciano oltre 120 organizzazioni della società civile, un programma di deregolamentazione che indebolisce le tutele fondamentali dell'AI Act prima ancora che entrino pienamente in vigore. Tra le altre cose, il *Digital Omnibus* rinvia a dicembre 2027 le regolamentazioni dei sistemi di IA ad alto rischio. Un rinvio che significa mano libera per un ulteriore anno per i sistemi IA ad alto rischio, per le big tech che li producono, e per la violazione dei diritti fondamentali delle persone.

Il paradosso è che l'Italia, con il suo decreto che già allarga le maglie dell'AI Act, si trova ora in una condizione in cui, da un lato, le norme nazionali più stringenti potrebbero essere considerate "eccessive" rispetto al nuovo livello europeo, offrendo al Governo un pretesto per abbassare ulteriormente le tutele; dall'altro, il sistema di controllo nazionale, già debole e affidato ad agenzie governative, diventa ancora più inefficace in assenza di una trasparenza europea su cui fare affidamento. L'effetto combinato è un indebolimento dei diritti digitali su due livelli: le tutele

europee arretrano, quelle italiane non sono mai state robuste, e i cittadini restano con meno strumenti per difendersi. Come ha scritto EDRI (European Digital Rights), "se le leggi sui diritti digitali appena adottate possono essere riaperte ancor prima ancora di entrare in vigore, gli attori potenti possono trattare l'attuazione come una seconda possibilità per indebolire le regole che non gradiscono".

Conclusione, in un Paese che trova normale spiare giornalisti e attivisti

Prima di chiudere, vale la pena ricordare il contesto reale in cui queste norme andranno a operare. Nel 2025 è scoppiato lo scandalo legato allo spyware Graphite, con cui sono stati spiati il direttore di Fanpage.it Francesco Cancellato, gli attivisti di Mediterranea Saving Humans Luca Casarini e Beppe Caccia, don Mattia Ferrari, cappellano di bordo di Mediterranea e altri giornalisti. Le intercettazioni abusive sono state confermate da perizie tecniche. Il Governo ha ammesso che i servizi segreti hanno spiato legalmente gli attivisti, ma nega di aver preso di mira il giornalista. I procedimenti penali sono ancora "contro ignoti". A oggi, nessun responsabile è stato identificato o sanzionato. Istantanea di un Paese dove la sorveglianza colpisce cittadini e giornalisti, e l'identità degli infiltratori rimane segreta. Un segreto di Stato.

Ora, a questo scenario già compromesso, il decreto aggiunge: database biometrici di massa, riconoscimento facciale in tempo reale per 15 giorni, categorizzazione per "somiglianza", e supervisione sulla IA affidata ad agenzie di nomina governativa. Se già oggi, con strumenti meno potenti, si spiano i giornalisti e nessuno paga, cosa succederà domani, quando la polizia potrà attivare l'identificazione biometrica d'urgenza con una semplice telefonata al PM entro mezza giornata? Chi vigilerà affinché quei database di 7 giorni non diventino dossier nascosti nei cassetti? Chi sanzionerà l'agente che usa il riconoscimento facciale per seguire un attivista?

L'AI Act italiano, così come disegnato, non si limita a regolare l'uso dell'IA: fornisce un impianto legale che legittima e potenzia la preesistente vena repressiva dell'esecutivo. In un contesto in cui il Governo ha già mostrato una spiccata attitudine a inasprire le misure di controllo e repressione (si pensi ai decreti sicurezza, alla gestione delle proteste, ai fermi preventivi e ai DASPO),

questo nuovo corpo normativo mette a disposizione delle forze di polizia strumenti tecnologici avanzatissimi – riconoscimento facciale in tempo reale, database biometrici di massa, procedure d'urgenza senza controllo giudiziario effettivo. La "cornice antropocentrica" evocata da Mantovano può diventare facilmente, nella pratica, una gabbia per i diritti fondamentali, rivestita di legalità.

La risposta, al momento, è inquietante: nessuno, o quasi, controllerà davvero l'uso di questi strumenti. Il decreto italiano non solo non rafforza le tutele, ma allarga le maglie dell'AI Act e indebolisce i controlli, in un Paese dove la sorveglianza illegale è già oggi un fatto impunito.

Le rassicurazioni di Mantovano e Piantedosi suonano come indirette veline ai giornalisti. Il Grande Fratello, se non è ancora tra noi come annunciato, è già nato, ed è pronto a crescere velocemente.

Riferimenti normativi

[1] Decreto legislativo di adeguamento al Regolamento (UE) 2024/1689 – approvato in esame preliminare dal Consiglio dei Ministri il 10 giugno 2026.

[2] *Digital Omnibus* – proposta della Commissione europea del 19 novembre 2025; accordo politico in trilogo il 7 maggio 2026.

[3] Nuovo art. 437-bis del codice penale (introdotto dall'art. 14 del decreto).

[4] Art. 10, commi 3 e 6 del decreto (raccolta e conservazione per 7 giorni dei volti dei partecipanti a eventi pubblici).

[5] Art. 10, comma 9 del decreto (divieto di decisioni negative basate *unicamente* sul riconoscimento facciale).

[6] Decreti-legge sicurezza: D.L. n. 48/2025, D.L. n. 159/2025, D.L. n. 23/2026, e bozza di un quarto decreto a maggio 2026.

[7] Art. 7, comma 1, lett. a del decreto (categorizzazione biometrica consentita purché non finalizzata a dedurre caratteristiche sensibili).

[8] Art. 5, par. 1, lett. g del Regolamento (UE) 2024/1689 (divieto assoluto di sistemi che classificano persone per dedurre caratteristiche sensibili).

[9] Considerando 43 del Regolamento (UE) 2024/1689 (divieto di *scraping* non mirato di immagini facciali e di sorveglianza di massa indiscriminata).

[10] Art. 8, comma 5 del decreto (durata dell'autorizzazione fino a 15 giorni, prorogabile per altri 15).

[11] Art. 5, par. 1, lett. h del Regolamento (UE) 2024/1689 (uso "strettamente limitato nel tempo e nel contesto dell'evento specifico").

[12] Art. 8, comma 6 del decreto (attivazione d'urgenza con comunicazione orale al PM, richiesta di autorizzazione entro 12 ore).

[13] Art. 5, par. 4 del Regolamento (UE) 2024/1689 (autorizzazione preventiva e notifica al Garante entro 24 ore).

[14] Art. 9, comma 4 del decreto (notifica al Garante differibile fino a 3 mesi, rinnovabile una volta).

[15] Art. 6, comma 2, lett. b del decreto (formazione obbligatoria su "analisi predittiva").

[16] Art. 5, par. 1, lett. d del Regolamento (UE) 2024/1689 (divieto di profilazione predittiva individuale basata su tratti della personalità).

[17] Art. 4 del decreto (collaborazioni con privati per ricerca e sviluppo di sistemi IA).

[18] Art. 2, comma 1, lett. n del secondo decreto (designazione di AgID e ACN quali "Autorità nazionali per l'intelligenza artificiale"), in coerenza con l’art. 20, comma 1, della legge 23 settembre 2025, n. 132 (Disposizioni e deleghe al governo in materia di intelligenza artificiale”

[19] Art. 5, par. 4 e capo VII del Regolamento (UE) 2024/1689 (requisito di indipendenza delle autorità di vigilanza).