

Rete per i Diritti Umani Digitali

Osservazioni e raccomandazioni nell'ambito del parere sull'A.G. n. 418 relativo all'uso di intelligenza artificiale da parte delle forze di polizia e in materia di responsabilità penale e civile

Premesse

La **Rete per i Diritti Umani Digitali** riunisce le principali organizzazioni della società civile in Italia impegnate a promuovere i diritti umani nel contesto digitale e contrastare il diffondersi di fenomeni discriminatori e pratiche di sorveglianza di massa attraverso sistemi di intelligenza artificiale. Le organizzazioni che compongono la coalizione sono: The Good Lobby, Privacy Network, Hermes Center, Strali, Period Think Tank e Amnesty International Italia, Sloweb, Italiani Senza Cittadinanza, Antigone e Comunicazione pubblica.

All'interno di questa cornice, la Rete per i Diritti Umani Digitali ha costantemente ribadito la propria posizione a favore di un divieto totale dell'utilizzo dei sistemi di riconoscimento biometrico, sia "in tempo reale", sia "a posteriori" (ossia quando il riconoscimento avviene su materiale video già registrato), ritenendo che tali tecnologie presentino gravi criticità in termini di fallibilità e opacità e possano, di conseguenza, generare ingiustizie, violazioni dei diritti fondamentali e abilitare pratiche di sorveglianza indiscriminata.

La Rete chiede alle Commissioni competenti per la redazione dei pareri di fare proprie e integrare le seguenti osservazioni, tenendo conto dei profili critici evidenziati e delle raccomandazioni formulate.

Sommario

1. Art. 10: riconoscimento biometrico a posteriori in luoghi o eventi pubblici
2. Art. 8: identificazione biometrica remota in tempo reale
3. Procedura d'urgenza in forma orale
4. Rapporto tra art. 8 e art. 359-ter c.p.p.
5. Profili di incostituzionalità della delega
6. Relazione annuale al Parlamento sugli utilizzi e sull'impatto sui diritti
7. Valutazioni d'impatto: diritti fondamentali e protezione dei dati
8. Esclusione del traffico illecito di stupefacenti dall'ambito del tempo reale

Osservazioni e raccomandazioni in materia di utilizzo di intelligenza artificiale nell'ambito delle attività di polizia

1. **Utilizzo di sistemi di riconoscimento facciale a posteriori sulle persone che accedono a luoghi o ad eventi rispetto ai quali sussistono esigenze di ordine e sicurezza pubblica, ex art. 10, Schema di decreto sulle attività di polizia.**

Chiediamo al Parlamento di esprimere un parere contrario sull'articolo 10, esigendone la soppressione integrale. In subordine, escludere l'applicazione dell'art.10 in occasione di manifestazioni pubbliche.

L'articolo 10, disponendo che si può disporre l'uso dei sistemi di riconoscimento facciale a posteriori su persone che accedono a luoghi o ad eventi, rischia di trasformare il riconoscimento biometrico in misura ordinaria di raccolta e trattamento azionabile tutte le volte in cui vengano invocate generiche esigenze di ordine e sicurezza pubblica. In tal modo, si normalizza una forma di sorveglianza biometrica di massa incompatibile con i principi di necessità, proporzionalità e tutela dei diritti fondamentali, che si pone in netto contrasto con il diritto europeo.

Soprattutto, tale specificazione non trova riscontro nell'AI Act e dunque la *ratio* del suo inserimento risulta ambigua e preoccupante. L'articolo dovrebbe pertanto essere eliminato. In subordine, ove si

intendesse mantenerlo, sarebbe comunque necessario escluderne espressamente l'applicazione in occasione di manifestazioni pubbliche.

L'uso di cui al comma 3 costituisce un'aperta violazione dell'art. 5 lett. e) Al Act, che vieta l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA 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.

Inoltre, si ritiene che il tempo di conservazione di sette giorni sia troppo lungo e sproporzionato dal punto di vista dell'oggetto del trattamento, considerato che si tratta di dati biometrici di persone in nessun modo collegate a un reato.

L'art. 10 dovrebbe inoltre essere coordinato con l'art. 8, relativo all'uso in tempo reale dei sistemi di identificazione biometrica. Le due disposizioni disciplinano ipotesi tra loro strettamente connesse, ma che sono costruite secondo schemi normativi significativamente diversi, producendo un'incoerenza sistematica interna alla disciplina. Il parere congiunto dell'EDPB (European Data Protection Board) e dell'EDPS (European Data Protection Supervisor) aveva già evidenziato la criticità di acuire una differenza che, nella pratica, è del tutto sfumata e non granitica come invece vorrebbe intendersi dalla disposizione normativa.

In particolare, l'art. 10 esplicita la necessità di svolgere una DPIA (Data Protection Impact Assessment, o Valutazione d'Impatto sulla Protezione dei Dati), individua il titolare del trattamento e disciplina i tempi di conservazione dei dati. Tali elementi, invece, non risultano previsti con analoga chiarezza nell'art. 8, nonostante l'uso in tempo reale presenti profili di rischio particolarmente elevati e richieda, semmai, garanzie rafforzate.

Si chiede che le due disposizioni siano quindi meglio coordinate, tenendo conto della diversa intensità dei rischi connessi all'utilizzo in tempo reale rispetto all'utilizzo a posteriori. In particolare, sarebbe opportuno assicurare che anche per i sistemi impiegati in tempo reale siano previste garanzie espresse in materia di valutazione d'impatto, titolarità del trattamento, conservazione dei dati e controllo sulle modalità di autorizzazione.

Sarebbe infine opportuno chiarire cosa debba intendersi per "banca dati salvata in locale". Qualora si intenda fare riferimento a una banca dati normalmente conservata su un diverso server e trasferita localmente per ragioni operative, la precisazione rischia di risultare superflua o comunque ambigua. Una definizione più puntuale appare necessaria per evitare incertezze applicative e garantire che il trattamento dei dati biometrici avvenga entro confini giuridici chiari e verificabili.

2. Utilizzo di sistemi di identificazione biometrica remota in tempo reale per finalità di prevenzione e ricerca di persone: criticità dell'art. 8, commi 1-5, dello schema di decreto sulle attività di polizia

Si richiede in primo luogo, di eliminare l'articolo in radice in quanto l'uso di tecnologie di identificazione biometrica da remoto in tempo reale a scopo preventivo potrebbero rappresentare una minaccia al diritto alla privacy e alla protezione dei dati, la libertà di espressione e di riunione, e il principio di non discriminazione. In subordine si richiede una profonda revisione dell'art. 8 sotto i seguenti profili:

- identificazione in modo dinamico, compresa la localizzazione;
- possibilità di incrociare l'eventuale banca dati utilizzata dalle forze dell'ordine con altre banche dati della PA;
- limitare la richiesta al solo pubblico ministero e al giudice per le indagini preliminari, come già previsto per strumenti di indagine quali intercettazioni. In subordine, ridimensionare l'elenco dei soggetti legittimati alla richiesta espungendo le forze di polizia diverse dalla polizia giudiziaria;
- introdurre un limite massimo alle proroghe per l'utilizzo dei sistemi di identificazione in tempo reale.

Appare necessario chiarire cosa debba intendersi per "*identificazione in modo dinamico, compresa la localizzazione*" (comma 2). Qualora si intenda fare riferimento a sistemi che "*seguono*" una persona attraverso l'uso di diverse telecamere, appare necessario prevedere una ulteriore e specifica disciplina (in particolare con riferimento alle misure di garanzia dei diritti fondamentali), poiché, secondo la definizione giuridica di identificazione in tempo reale, tale utilizzo costituirebbe un trattamento di dati sostanzialmente diverso e significativamente più invasivo.

Inoltre, la possibilità di incrociare l'eventuale banca dati utilizzata dalle forze dell'ordine con altre banche dati della PA (comma 3) introduce seri rischi di sorveglianza di massa ed in particolare trattamenti in violazione del principio di necessità, della proporzionalità e del principio di presunzione di innocenza. Si chiede pertanto di chiarire le modalità pratiche di tale ipotesi con particolare riferimento alle misure di salvaguardia per le libertà e i diritti fondamentali dei cittadini.

Il comma 4 prevede che: "L'utilizzo dei sistemi di IA di cui al comma 1 è subordinato a una richiesta del questore o del comandante provinciale dell'Arma dei Carabinieri e della Guardia di Finanza, ovvero dei responsabili dei Servizi centrali". Per coerenza con l'impostazione del nostro sistema costituzionale e di procedura penale, si ritiene che la possibilità di tale richiesta dovrebbe essere circoscritta al pubblico ministero e al giudice per le indagini preliminari. In subordine, si chiede di ridimensionare l'elenco dei soggetti legittimati a richiedere l'utilizzo, espungendo le forze di polizia diverse dalla polizia giudiziaria; la possibilità di avviare l'uso da parte delle forze di polizia, con il solo controllo del pubblico ministero, può aprire la strada ad utilizzi abusivi.

Prevedendo al comma 5 che: *"l'autorizzazione deve essere concessa con riguardo a uno specifico evento o per il tempo strettamente necessario, in ogni caso non superiore a quindici giorni, prorogabili dal pubblico ministero, con decreto motivato per periodi successivi di quindici giorni qualora permangano le condizioni di cui al comma 1"*, sostanzialmente si abdica al fissare un limite massimo alle proroghe. Tale disposizione appare totalmente sproporzionata; è pertanto necessario prevedere un limite massimo in tale senso.

3. Procedura d'urgenza in forma orale azionabile dal questore, ex art. 8 commi 6 e 7.

Si chiede l'espunzione della procedura d'urgenza in forma orale di cui all'art. 8, commi 6 e 7, o quanto meno il chiarimento del rapporto della disciplina richiamata con quella stabilita dalla *lex specialis* dell'art. 359-ter c.p.p.. In tal senso, si richiede la riserva dell'autorizzazione all'impiego dei sistemi di cui all'art. 8 al giudice per le indagini preliminari, secondo il modello già adottato per l'art. 359-ter c.p.p., o quantomeno la subordinazione dell'avvio alla richiesta del pubblico ministero e alla previa autorizzazione del giudice.

Costituendo l'uso in tempo reale l'ipotesi maggiormente invasiva e che può più dare origine ad abusi, appare totalmente insufficiente, quale misura di garanzia la possibilità di utilizzo previa richiesta in forma orale. Altresì appare insufficiente la successiva convalida da parte del pubblico ministero, ancor più in assenza di esplicita previsione sulla modalità con cui deve provvedere il suddetto pubblico ministero.

Si consideri che, una disposizione del genere costituisce motivo di violazione dell'art. 52 Carta Europea diritti fondamentali nonché con i principi costituzionali.

Si segnala inoltre l'eccessiva ampiezza dei soggetti legittimati a richiedere l'autorizzazione e si suggerisce di designare unicamente un'autorità giudiziaria come soggetto legittimato ad avviare l'uso del riconoscimento facciale in tempo reale, ancor più se in forma orale.

4. Chiarire il rapporto tra art. 8 dello schema di decreto e art. 359-ter c.p.p..

Lo schema di decreto legislativo introduce un evidente cortocircuito interpretativo nel coordinamento tra l'art. 8 del decreto e il nuovo art. 359-ter c.p.p.

Le due norme sembrano riferirsi a ipotesi di reati profondamente diversi:

- L'art. 359-ter c.p.p. disciplina l'attivazione dell'identificazione in tempo reale nei casi di cui all'allegato II dell'AI Act, ma esclude la richiesta da soggetti diversi dal pubblico ministero o, per ragioni d'urgenza, dalla polizia giudiziaria; ed esclude, inoltre, qualsiasi procedura in forma orale.
- L'art. 8 dello schema di decreto per le attività di polizia, invece, si applicherebbe all'art. 5, par. 1, lett. h) punti i) e ii) dell'AI Act, con la possibilità di richiesta da parte delle forze di polizia, anche in forma orale qualora ricorrano ragioni d'urgenza.

Nonostante questa netta separazione di scopi e catalogo reati, l'art. 8 si apre con la clausola di riserva: "Fermo restando quanto previsto dall'articolo 359-ter del codice di procedura penale", lasciando presupporre che quest'ultimo prevalga sull'art.8 del Decreto.

Questo inciso crea un grave problema di coordinamento: non è chiaro se la riserva configuri un rapporto di esclusione reciproca o se determini una sovrapposizione procedurale.

Differenziare il grado di invasività delle indagini in base alla gravità dei reati è di per sé positivo. Sarebbe opportuno un definitivo chiarimento sul rapporto di sussidiarietà o specialità tra le due norme.

5. Profili di incostituzionalità emergenti dalla delega al Governo e dalla successiva delega al Ministero dell'Interno.

Considerati i profili di incostituzionalità che emergono dalla delega al Governo e dalla successiva delega al Ministero dell'Interno, si chiede che il parere contenga una richiesta di chiarimento e specificazione dei criteri della delega al Ministero.

Oltre ai profili già richiamati, il decreto relativo alle attività di polizia presenta una serie di criticità *ab origine* rispetto alla delegazione legislativa, di cui si evidenziano di seguito i principali profili di incostituzionalità.

La struttura della delega si articola su due livelli che, cumulandosi, accentuano la concentrazione della funzione normativa in capo all'esecutivo.

Al primo livello si colloca la delega di cui all'art. 24 della legge 23 settembre 2025, n. 132 (commi 1, 2, lett. h, 3 e 5), che conferisce al Governo l'adozione di una specifica disciplina dei sistemi di IA per l'attività di polizia: delega ampia, in materia direttamente incidente su diritti fondamentali, rispetto alla quale la giurisprudenza costituzionale esige principi e criteri direttivi «precisi e definiti» (Corte cost. n. 175/2022), a pena della violazione dell'art. 76 Cost. Al secondo livello, quello propriamente censurato, il decreto delegato rinvia a sua volta a decreti del Ministro dell'interno la determinazione di elementi che, benché presentati come tecnici, condizionano direttamente l'incidenza dei sistemi sui diritti: l'art. 9, comma 5, demanda a tale fonte la fissazione dei requisiti minimi di affidabilità e delle soglie operative dei sistemi in tempo reale, oltre alle modalità di monitoraggio dei bias; l'art. 10, comma 11, vi demanda le modalità del trattamento automatizzato dei dati biometrici e la costituzione della base dati di riferimento per il confronto a posteriori.

Si tratta di parametri a diretta rilevanza per i diritti fondamentali, giacché la soglia operativa determina il tasso di falsi positivi, la base dati determina il perimetro dei soggetti sottoposti a confronto, parametri che così vengono sottratti alla fonte primaria e al vaglio parlamentare e rimessi a un atto ministeriale.

Il vizio si aggrava per la coincidenza soggettiva: per il sistema a posteriori il titolare del trattamento è lo stesso Ministero dell'interno, Dipartimento della Pubblica Sicurezza (art. 10, comma 4), sì che l'amministrazione che impiega i sistemi ne fissa, con proprio decreto, i parametri di funzionamento, facendo coincidere l'autorità che pone la norma con quella che la applica.

Ne risulta portata alle estreme conseguenze quella forza centripeta verso l'esecutivo che percorre l'intero provvedimento. Si chiede pertanto che gli elementi a diretta incidenza sui diritti fondamentali, in particolare le soglie operative e i criteri di costituzione e alimentazione delle basi dati, siano fissati nella fonte primaria ovvero nel decreto delegato entro criteri predeterminati, e non rimessi a decreti ministeriali, in assenza di precisi parametri di riferimento.

6. Relazione annuale che monitori gli utilizzi di sistemi di identificazione biometrica in tempo reale e a posteriori e il relativo impatto sui diritti umani.

Il parere dovrebbe richiedere che lo schema di decreto preveda la presentazione al Parlamento di un'unica relazione annuale che monitori gli utilizzi di sistemi di identificazione biometrica in tempo reale e a posteriori, e il relativo impatto sui diritti umani.

Tale richiesta è finalizzata a rendere effettive le prerogative di vigilanza del Parlamento in materia di rispetto dei diritti umani e intelligenza artificiale, prevedendo la presentazione alle Camere, da parte del Garante per la Protezione dei Dati Personali, di un'unica relazione annuale sull'utilizzo dei sistemi di riconoscimento biometrico, corredata da una valutazione di impatto sui diritti umani.

La relazione dovrà presentare i dati nella maniera più accessibile e disaggregata possibile, riportando la percentuale di errori riscontrati e le statistiche relative al tipo di reato per cui è stato richiesto e

autorizzato l'utilizzo, sia nelle ipotesi di identificazione biometrica «in tempo reale», sia nelle ipotesi di identificazione biometrica «ex-post», descrivendo le possibili implicazioni negative relative all'utilizzo del riconoscimento biometrico in una valutazione d'impatto sui diritti umani.

Perché ciò si realizzi, occorre assegnare al Garante per la protezione dei dati personali i poteri di accesso per il reperimento delle predette informazioni, considerato che tali dati sono comunque elaborati da AGID e ACN per le relazioni di cui agli artt.5, par. 5 e 26, par. 10 dell'AI Act, indirizzate alle istituzioni europee.

7. Inserimento della valutazione d'impatto sui diritti fondamentali, ex Art. 27, AI Act, e coordinamento con la valutazione d'impatto sui dati personali, ex Art. 37, Law Enforcement Directive. Richiesta: correzione e chiarimento

L'impianto dello schema ancora l'utilizzo dei sistemi biometrici a due distinti strumenti di valutazione d'impatto, assegnati però in modo asimmetrico e su piani normativi non sovrapponibili. Per l'identificazione in tempo reale (artt. 8 dello schema e 359-ter c.p.p.) l'art. 9, comma 1, prescrive la sola valutazione d'impatto sui diritti fondamentali di cui all'art. 27 del regolamento IA, da completare «in via preventiva»; per il riconoscimento a posteriori l'art. 10, comma 5, prescrive invece la valutazione d'impatto sulla protezione dei dati e la consultazione preventiva del Garante ai sensi degli artt. 23 e 24 del d.lgs. n. 51/2018.

Da tale ripartizione discendono tre criticità.

In primo luogo, la valutazione sui diritti fondamentali è circoscritta alla sola identificazione in tempo reale e non è estesa agli altri sistemi ad alto rischio impiegati nell'attività di polizia ai sensi del Capo II, in contrasto con la vocazione dell'art. 27 del regolamento IA.

In secondo luogo, essa è configurata come adempimento esaurito nel momento anteriore all'attivazione del sistema, senza previsione di riesame iterativo lungo il ciclo di vita, in tensione con la logica di gestione continuativa del rischio propria, ancora una volta, dell'art. 27 del regolamento IA. Peraltro, sebbene l'art. 10 stabilisce che *“è possibile effettuare un'unica valutazione d'impatto sulla protezione dei dati valida per tutti i sistemi analoghi”*, la disposizione pare differente rispetto a quanto disposto dall'AI Act. Difatti, l'art. 27, par. 2, ammette che *“in similar cases”* il *deployer* possa fare affidamento su valutazioni d'impatto già svolte. Dunque questa possibilità non equivale affatto a una certificazione estendibile automaticamente per analogia, essendo, in ogni modo, soggetta a una valutazione di compatibilità della DPIA svolta con la FRIA, come postulato dall'art. 27, par. 4

In terzo luogo, ed è il profilo di maggiore gravità, l'assegnazione incrociata dei due strumenti fa sì che il riconoscimento a posteriori, che è l'ipotesi di impiego più estesa e sistematica, poiché coinvolge la generalità dei soggetti che accedono a luoghi ed eventi, sia presidiato dalla sola valutazione sulla protezione dei dati e resti privo della valutazione d'impatto sui diritti fondamentali.

Poiché l'incidenza sui diritti fondamentali opera su un piano autonomo e non riducibile a quello della protezione dei dati, esigendo un giudizio di proporzionalità ai sensi dell'art. 52, paragrafo 1, della Carta, che la valutazione sulla protezione dei dati non è deputata a svolgere, quest'ultima non è idonea ad assorbirne la funzione, con la conseguenza che il sistema più invasivo sfugge per intero al vaglio di proporzionalità sui diritti fondamentali.

A ciò si aggiunge una speculare asimmetria nel coinvolgimento dell'autorità indipendente: per il tempo reale è prevista la sola notifica successiva al Garante (art. 9, comma 4), mentre la consultazione preventiva è riservata al solo sistema a posteriori (art. 10, comma 5), sì che il controllo esterno è più tenue proprio dove l'ingerenza è attuale e meno reversibile.

Alla luce di quanto precede, chiediamo, pertanto, che il comma 5 dell'art. 10 del decreto in oggetto venga riformulato in conformità all'AI Act. In subordine, qualora si intendesse mantenere la possibilità di ricorrere a una DPIA unica, tale facoltà dovrebbe essere espressamente subordinata a una valutazione formale, preventiva e documentata sulla persistente attualità e adeguatezza della DPIA originaria rispetto al nuovo sistema considerato. In assenza di tale verifica, il rischio è che la valutazione d'impatto si riduca a un mero adempimento formale, replicato per analogia senza un effettivo esame del contesto, delle finalità, delle caratteristiche tecniche e dei rischi specifici del sistema impiegato.

Si chiede infine di estendere, secondo le previsioni normative di cui all'AI Act, la valutazione d'impatto sui diritti fondamentali a tutti i sistemi ad alto rischio impiegati nell'attività di polizia, di prevederne lo svolgimento lungo l'intero ciclo di vita del sistema e di imporre, per entrambe le tipologie di impiego, il cumulo dei due strumenti, valutazione sui diritti fondamentali e valutazione sulla protezione dei dati con consultazione preventiva del Garante, così da sottoporre anche il riconoscimento a posteriori al vaglio sui diritti fondamentali e da anticipare, per il tempo reale, il coinvolgimento del Garante alla fase autorizzatoria.

8. Esclusione della fattispecie di *Traffico illecito di stupefacenti e sostanze psicotrope* dall'ambito di applicazione dell'art. 359-ter, per i quali è ammesso l'utilizzo del riconoscimento biometrico «in tempo reale».

Il parere dovrebbe pretendere una differenziazione di disciplina tra le varie fattispecie di reato per le quali l'AI Act consente l'utilizzo di strumenti di identificazione biometrica, chiedendo di escludere la fattispecie di *Traffico illecito di stupefacenti e sostanze psicotrope*

Tale richiesta trova giustificazione nella mancanza di proporzionalità tra la lesione dei diritti fondamentali implicita nell'utilizzo della sorveglianza in tempo reale e l'interesse pubblico a reprimere il traffico di stupefacenti e sostanze psicotrope. Includere la fattispecie in oggetto appare tanto più manifestamente sproporzionato laddove si vada a comparare la gravità del reato di traffico illecito di sostanze stupefacenti alle altre contenute nell'elenco di cui all'allegato II, alle quali non si capisce come possa essere ragionevolmente accostata: terrorismo; tratta di esseri umani; sfruttamento sessuale di minori e materiale pedopornografico; traffico illecito di armi, munizioni ed esplosivi; omicidio volontario; lesioni personali gravi; traffico illecito di organi e tessuti umani; traffico illecito di materie nucleari e radioattive, rapimento, sequestro e presa di ostaggi; reati che rientrano nella competenza giurisdizionale della Corte penale internazionale; dirottamento di un aeromobile o una nave; stupro; reati ambientali; furto organizzato o rapina a mano armata; sabotaggio, partecipazione a un'organizzazione criminale coinvolta in uno o più dei reati qui elencati sopra. Temiamo che il traffico di sostanze stupefacenti possa costituire la porta di ingresso per possibili abusi diretti nei confronti di persone che si vuole controllare, anche estendendo il controllo ad altri soggetti, quali, ad esempio, attivisti e giornalisti, giacché il pretesto di un'accusa di questo tipo è facilmente azionabile nei confronti di chiunque senza particolari artificiosità.

Peraltro, risulta preoccupante la mancanza di un riferimento, quanto meno editale, ai reati per cui sarebbero impiegabili strumenti di identificazione biometrica post remota, che, allo stato, non sono oggetto di alcuna limitazione per quanto ai reati. Questo aspetto, unito alle criticità già evidenziate e che si esporranno, presenta un chiaro elemento di criticità e trasparenza rispetto all'impiego di strumenti di sorveglianza, sproporzionato rispetto ad altri e simili supporti tecnici come nel campo delle intercettazioni.