RICONOSCIMENTO FACCIALE TRA PRIVATO E PUBBLICO: GDPR, AI ACT E NUOVE REGOLE NAZIONALI

Artificial Intelligence & Data protection

AUTORI

Aurora Agostini
Partner

Alessandro Carlini
Associate

*I sistemi di riconoscimento facciale comportano il trattamento di dati personali biometrici e, in genere, l'impiego anche di un sistema di intelligenza artificiale: il Regolamento (UE) 2016/679 ("**GDPR**") e il Regolamento (UE) 2024/1689 ("**AI Act**"), con i relativi decreti e regolamenti attuativi, trovano dunque applicazione congiunta.*

*Il 2026 ha profondamente ridisegnato il quadro regolatorio: la moratoria nazionale nei luoghi pubblici o aperti al pubblico è stata prorogata al 31 dicembre 2027; il nuovo D. Lgs. 9 settembre 2026, n. 160 ha dettato la disciplina dell'uso da parte delle Forze di polizia; il successivo D. Lgs. 7 ottobre 2026, n. 179 lo ha completato sul versante dei poteri di vigilanza e sanzionatori; il Regolamento (UE) 2026/1744 ("**Digital Omnibus**") ha rinviato al 2 dicembre 2027 gli obblighi per i sistemi ad alto rischio dell'Allegato III, compresi quelli biometrici, lasciando fermi i divieti già applicabili.*

A che punto siamo, dunque? Aziende e datori di lavoro possono ricorrere a sistemi di riconoscimento biometrico facciale? Ed entro quali limiti le Autorità di contrasto possono servirsi di queste tecnologie?

▼ ▼ ▼

DATO BIOMETRICO E RICONOSCIMENTO FACCIALE

Prima di entrare nel merito del quadro regolatorio, è opportuna una premessa: non tutti i sistemi di videosorveglianza comportano un trattamento di dati biometrici, né ogni trattamento di dati biometrici dà luogo, di per sé, a un sistema di riconoscimento facciale.

Ai sensi dell'**art. 4, n. 14) del GDPR**, costituiscono **dati biometrici** i dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona, che ne consentono o confermano l'identificazione univoca, come l'immagine facciale. Le riprese video o la fotografia di una persona non sono quindi, di per sé, dati biometrici, trattandosi di dati "grezzi": lo diventano soltanto a seguito di un trattamento tecnico specifico funzionale all'identificazione univoca dell'individuo (*cfr.* Considerando 51 del GDPR). In altri termini, si è in presenza di dati biometrici quando concorrono tre

elementi: (i) la particolare **natura** dei dati personali (dati relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica); (ii) i **mezzi e le modalità** del trattamento applicati a tali dati grezzi ("trattamento tecnico specifico") e (iii) la **finalità** del trattamento (i dati devono essere utilizzati al fine di identificare in modo univoco una persona fisica).

Proprio in ragione della loro delicatezza e dell'incidenza sui diritti fondamentali, i dati biometrici rientrano tra le **categorie particolari di dati personali di cui all'art. 9 del GDPR**, il cui trattamento è di regola vietato, salvo che ricorra una delle condizioni del par. 2; il par. 4 dello stesso articolo consente poi agli Stati membri di introdurre condizioni ulteriori, previste in Italia dall'**art. 2-*septies* del Codice Privacy**.

Possono dunque costituire dati biometrici, ad esempio, la scansione dell'iride o i dati dattiloscopici e, per quanto qui rileva, i dati facciali trattati ai fini dell'identificazione univoca di una persona: è in quest'ultima ipotesi che si parla di sistemi di riconoscimento facciale basati su dati biometrici.

Va inoltre precisato che, nei sistemi di riconoscimento facciale, il trattamento biometrico si realizza sia (i) nella fase di registrazione (*enrolment*), che consiste nell'acquisizione delle caratteristiche biometriche dell'interessato (es. caratteristiche del volto), sia (ii) nella fase di riconoscimento vero e proprio, ossia al momento della rilevazione del volto. Ne consegue che anche la sola estrazione del modello matematico del volto (*template*) integra un trattamento di dati biometrici.

Occorre poi distinguere tre diverse funzioni dei sistemi di riconoscimento facciale, ciascuna definita dall'art. 3 dell'AI Act e soggetta a un regime proprio:

- **la verifica biometrica (1:1)**, con cui si accerta che una persona sia effettivamente chi dichiara di essere, confrontandone il volto con un unico *template* fornito in precedenza;
- **l'identificazione biometrica (1:N),** che confronta il volto con quelli contenuti in una banca dati di più persone e che, se effettuata a distanza, può avvenire "in tempo reale" o "a posteriori";
- **la categorizzazione biometrica**, che assegna la persona a categorie specifiche sulla base dei suoi dati biometrici.

I rischi connessi al riconoscimento facciale sono numerosi e peculiari: a differenza di una *password*, il dato biometrico non può essere sostituito; gli algoritmi di intelligenza artificiale su cui il sistema si fonda possono generare falsi positivi e falsi negativi con possibili *bias* tra gruppi di popolazione e conseguenze significative sui diritti e libertà dell'interessato; l'impiego in spazi pubblici, infine, rischia di scoraggiare l'esercizio delle libertà di riunione ed espressione.

IL CONTESTO PRIVATO: BASI GIURIDICHE, LAVORO E LUOGHI PUBBLICI E APERTI AL PUBBLICO

Per trattare categorie particolari di dati personali, il titolare del trattamento (es. l'azienda che intende installare un sistema di riconoscimento facciale) dovrà individuare una base giuridica ai sensi dell'art. 6 del GDPR e, cumulativamente, una delle condizioni di cui all'art. 9, par. 2 del GDPR.

Nel contesto d'impresa, la condizione legittimante è di regola il **consenso esplicito** dell'interessato (lett. a), manifestato in modo libero, specifico, informato e inequivocabile (artt. 4, n. 11, e 7 del GDPR), il che presuppone, tra l'altro, che all'interessato sia offerta un'alternativa non biometrica effettiva e priva di svantaggi.

Sul punto è essenziale la distinzione, tracciata dall'EDPB nelle Linee Guida 3/2019, tra l'uso di sistemi di riconoscimento facciale in ambienti non controllati e in ambienti controllati. Nel primo caso, il dispositivo biometrico è collocato in uno spazio pubblico o aperto al pubblico ed è in grado di funzionare su chiunque entri nel cono di ripresa della videocamera; nel secondo, invece, il sistema opera soltanto con la partecipazione attiva di una persona consenziente.

Negli ambienti non controllati, il sistema acquisisce in tempo reale il volto di chiunque entri nell'area di ripresa della telecamera, comprese le persone che non hanno acconsentito all'uso del dispositivo biometrico, e ne genera i relativi modelli biometrici. Tali modelli vengono poi confrontati con quelli creati dagli interessati che hanno prestato il previo consenso durante un processo di registrazione, al fine di consentire al titolare del trattamento di riconoscere se la persona utilizzi o meno il dispositivo biometrico. Anche in questi casi occorre fare ricorso a una delle deroghe di cui all'art. 9, par. 2, del GDPR che, come anticipato, nel contesto privato coincide di regola con il consenso.

Per i luoghi pubblici o aperti al pubblico, inoltre, opera l'**art. 9, co. 9, D.L. 8 ottobre 2021, n. 139** (conv. L. 3 dicembre 2021, n. 205), che sospende l'installazione e l'utilizzo di impianti di videosorveglianza con sistemi di riconoscimento facciale basati su dati biometrici, da parte di autorità pubbliche e soggetti privati, fino a una disciplina legislativa della materia. Il termine è stato da ultimo esteso al **31 dicembre 2027** dall'art. 2, co. 6-quater, D.L. 31 dicembre 2025, n. 200, inserito in sede di conversione dalla L. 27 febbraio 2026, n. 26. Se nel contesto pubblico tale disciplina potrebbe essere rinvenuta, come si vedrà *infra*, nelle disposizioni nazionali di attuazione e, in particolare, nel D. Lgs. 160/2026, appare invece difficile ipotizzare, allo stato, un impiego lecito dei sistemi di riconoscimento facciale in ambienti non controllati di natura privata, come in negozi, centri commerciali, cinema ed eventi privati, qualunque sia la base giuridica applicata.

Quanto ai **rapporti di lavoro**, il quadro è ancora più stringente: l'art. 4 della L. 300/1970 ammette l'installazione e l'impiego di impianti da cui derivi la possibilità di controllo a distanza dei lavoratori solo per esigenze organizzative e produttive, di sicurezza del lavoro e di tutela del patrimonio, previo accordo sindacale o autorizzazione dell'Ispettorato. In ambito lavorativo, dunque, l'installazione e l'impiego di sistemi di videosorveglianza sono già di per sé presidiati dalle garanzie giuslavoristiche dell'art. 4 della L. 300/1970, oltre che dalla normativa sulla protezione dei dati personali (obblighi informativi, DPIA sul sistema, ecc.). Il Garante per la protezione dei dati personali, del resto, si è già pronunciato sui sistemi di riconoscimento facciale impiegati per la rilevazione delle presenze (*cfr.* Provvedimento n. 108/2024), vietando il trattamento di dati biometrici dei dipendenti per la rilevazione delle presenze e precisando che nemmeno il consenso costituisce, di regola, una base valida, attesa l'asimmetria tra datore di lavoro e lavoratore.

A nostro avviso, in ambito privato, restano dunque ipotizzabili soltanto usi di verifica 1:1 in ambienti controllati (non aperti al pubblico), come l'accesso ad aree riservate, e sempre che ricorra: un consenso esplicito, un'alternativa reale, una DPIA formalizzata e, preferibilmente, *template* sotto il controllo dell'interessato, fermo restando quanto osservato per i rapporti datore di lavoro-dipendente.

AI ACT E NORMATIVA ITALIANA: LE REGOLE PER LE IMPRESE

L'AI Act, come anticipato, si affianca al GDPR e si rivolge tanto ai soggetti privati quanto a quelli pubblici nel disciplinare i sistemi biometrici che fanno uso di tecnologie di intelligenza artificiale.

I **divieti di sviluppare e mettere in opera determinati sistemi di intelligenza artificiale previsti dall'art. 5, par. 1 dell'AI Act**, valgono anche per le imprese: creazione o ampliamento di banche dati di riconoscimento facciale mediante *scraping* non mirato di immagini da internet o da filmati di videosorveglianza; inferenza delle emozioni sul luogo di lavoro e negli istituti di istruzione, salvo motivi medici o di sicurezza; categorizzazione biometrica per dedurre razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale.

Sotto il cappello dei sistemi di intelligenza artificiale classificati come ad alto rischio dall'**allegato III, punto 1, dell'AI Act**, e quindi meritevoli di particolari precauzioni, troviamo: (a) i sistemi di identificazione biometrica remota, (b) la categorizzazione basata su attributi sensibili e (c) il riconoscimento delle emozioni, escludendo invece espressamente la sola verifica 1:1. Ne discende che un sistema di controllo accessi basato sulla verifica facciale non è ad alto rischio, pur restando pienamente

soggetto all'art. 9 del GDPR, alla disciplina in materia di protezione dei dati personali nel suo complesso e ai limiti di utilizzo del pertinente diritto dell'Unione o nazionale.

L'utilizzatore (*deployer*) di un sistema ad alto rischio è tenuto, tra l'altro, a utilizzarlo conformemente alle istruzioni d'uso, ad assicurare una sorveglianza umana competente, a conservare i *log* e a informare lavoratori e rappresentanti prima della messa in servizio sul luogo di lavoro. Per effetto del Digital Omnibus molti di questi obblighi decorreranno, tuttavia, soltanto dal **2 dicembre 2027**.

IL CONTESTO PUBBLICO: CONTRASTO DEI REATI E D.LGS. 160/2026

L'**art. 5, par. 1 dell'AI Act** vieta, tra le altre cose, l'identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di contrasto, salvo che sia strettamente necessaria per la ricerca mirata di vittime di sottrazione, tratta o sfruttamento sessuale e di persone scomparse, per prevenire una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone o una minaccia reale e attuale, o reale e prevedibile, di attacco terroristico, o per localizzare o identificare sospettati dei reati dell'Allegato II dell'AI Act punibili con una pena o una misura di sicurezza privative della libertà della durata massima di almeno quattro anni.

Anche in tali ipotesi sono comunque necessarie una FRIA, la registrazione del sistema nella banca dati UE, l'autorizzazione preventiva di un'autorità giudiziaria o amministrativa indipendente, la notifica all'autorità di vigilanza del mercato e al Garante e una legge nazionale abilitante. L'identificazione **"a posteriori"** in indagini mirate richiede invece un'autorizzazione, da chiedere entro 48 ore, salvo l'identificazione iniziale di un potenziale indagato basata su fatti oggettivi e verificabili direttamente connessi al reato; la **FRIA** di cui all'art. 27 dell'AI Act grava, dal canto suo sugli organismi di diritto pubblico e sugli enti privati che forniscono servizi pubblici, e può integrare la DPIA già svolta sul sistema biometrico.

Sul piano nazionale attuativo, la base legale è oggi rappresentata dal **D. Lgs. 9 settembre 2026, n. 160**, adottato in esecuzione della L. 23 settembre 2025, n. 132, che articola la disciplina dei sistemi di riconoscimento facciale, in sintesi, come segue:

- **tempo reale per prevenzione e ricerca di vittime o scomparsi**: autorizzazione del procuratore della Repubblica del capoluogo del distretto, su richiesta del questore o dei comandanti provinciali di Carabinieri e Guardia di finanza, per massimo 15 giorni prorogabili, in un'area delimitata; convalida entro 24 ore nell'urgenza; banca dati formata per il singolo impiego e poi cancellata, senza *scraping*; FRIA e DPIA preventive e *log* conservati per cinque anni;

- tempo reale a fini di indagine (mediante introduzione del nuovo art. 359-*ter* c.p.p.): autorizzazione del GIP su richiesta del PM (nei casi di urgenza, decreto motivato del PM soggetto a convalida), per i delitti dell'Allegato II dell'AI Act puniti con la reclusione non inferiore nel massimo a quattro anni e per la ricerca di latitanti e vittime;
- a posteriori: per la ricerca mirata di un indiziato, autorizzazione del GIP, che il PM deve richiedere entro 48 ore e sulla quale il giudice si pronuncia nelle successive 48 ore; senza autorizzazione, la sola identificazione iniziale *ex* art. 26, par. 10 dell'AI Act; in luoghi ed eventi con esigenze di ordine pubblico, immagini trattate senza elaborazione biometrica, conservate sette giorni e confrontate solo dopo un reato; vietato l'uso non mirato o generalizzato;
- in caso di violazione: inutilizzabilità dei risultati e cancellazione dei dati.

A nostro avviso, il decreto può essere letto come la disciplina legislativa della materia idonea a superare la moratoria sui sistemi di riconoscimento facciale, ma soltanto per le attività di polizia: per i privati nulla sembrerebbe cambiato.

CONCLUSIONI

In sintesi, il riconoscimento facciale non è retto da regimi alternativi – uno per il privato, uno per il pubblico – ma da più livelli normativi che si sommano. Per le imprese il quadro resta decisamente restrittivo: nel rapporto di lavoro manca una ver norma abilitante, nei luoghi pubblici o aperti al pubblico vige la moratoria fino al 31 dicembre 2027 e alcuni usi sono vietati in modo assoluto.

Per le Forze di polizia il D.Lgs. 160/2026 introduce autorizzazioni, limiti e garanzie la cui applicazione concreta andrà seguita con attenzione.

Il rinvio al 2027 degli obblighi per i sistemi ad alto rischio non deve indurre a rimandare l'adeguamento: DPIA, divieti, obblighi di trasparenza e regole nazionali sono già pienamente operativi.

Il *team* Data & Technology Innovation di LEXIA resta a disposizione per ogni approfondimento e per affiancare imprese ed enti nella valutazione dei progetti di riconoscimento facciale e nei relativi percorsi di adeguamento.

AUTORI



Aurora Agostini

Partner



Giulietta Minucci

Partner



Marco Grechi

Senior Associate



Giovanni Lombardi

Associate



Alessandro Carlini

Associate



Francesca Costarelli

Associate

Questo documento è fornito a scopo informativo generale e non intende fornire consulenza legale sui temi trattati. I destinatari di questo documento non possono fare affidamento sui suoi contenuti. LEXIA e/o i professionisti dello studio non possono essere ritenuti responsabili in alcun modo per i contenuti di questo documento, né sulla base di un incarico professionale né per qualsiasi altra ragione.