Procura della Repubblica presso il Tribunale di Salerno

Il Procuratore della Repubblica

Direttiva n. 3089/2026.U

Ai Procuratori Aggiunti
Ai Sostituti
Al Dirigente amministrativo
Sede

Al Questore
Ai Comandante provinciale Carabinieri
Al Comandante provinciale Guardia di Finanza
Salerno

p.c. Al Sig. Procuratore Generale
presso la Corte di Appello
Salerno

Oggetto: Prime indicazioni operative a seguito dell'emanazione del d.lgs 9 settembre 2026, n. 160 avente ad oggetto "*Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale*".

Il decreto legislativo n. 160 del 2026 (nel prosieguo, decreto), emanato a seguito della delega legislativa recata dalla l. n. 132 del 2025 ed entrato in vigore il 30 settembre u.s., rappresenta uno dei provvedimenti con cui l'ordinamento nazionale sta dando attuazione all'importante regolamento UE 2024/1689 del Parlamento e del Consiglio del 13 giugno 2024 (nel prosieguo, Regolamento UE) in materia di intelligenza artificiale (nel prosieguo, IA) e, in particolare, a quella parte di esso che riguarda il possibile utilizzo dei sistemi di IA per le attività giudiziarie e di polizia.

Va, in premessa, evidenziato che il decreto - suddiviso come si dirà in due titoli - contiene una regolamentazione che, già di per sé complessa per le peculiarità della materia trattata, appare tutt'altro che di agevole lettura sia per la tecnica di scrittura di alcune disposizioni, che hanno ripreso integralmente il contenuto della norma sovranazionale senza i necessari adattamenti all'ordinamento interno, sia perché molte norme sono infarcite di numerosi, e non sempre immediatamente comprensibili, rinvii alla superiore disciplina eurounitaria oltre che a decreti attuativi, fra l'altro ancora da emanare, della Presidenza del Consiglio o di singoli ministri.

Il presente atto, però, non ha alcuna pretesa di fornire chiavi ermeneutiche dell'intero impianto normativo recato dal decreto ma vuole limitarsi a dare indicazioni operative, "a prima lettura", utili ad orientare l'attività dei magistrati della procura e degli organi di polizia interessati, relativamente a quelle sole disposizioni che possono impattare sull'attività dell'ufficio, riservandosi eventualmente di intervenire ulteriormente, all'esito dell'emergere di orientamenti e prassi interpretative, anche giurisprudenziali, consolidate.

Per non appesantire la lettura del documento, né nel testo né nelle note saranno riportati gli articoli del decreto, ritenendo, invece, utile ed opportuno menzionare, sia pure in nota, quelle parti del Regolamento UE a cui le disposizioni del decreto in commento espressamente rinviano o a cui intendono dare attuazione.

****

Il titolo I del decreto tratta dell'"utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia" e nel suo ambito sono due gli articoli qui di interesse.

Il primo è **l'art. 8,** che si occupa dell'**identificazione biometrica "in tempo reale" per finalità di tipo preventivo.**

La norma, in particolare, dà attuazione alle previsioni dell'art. 5 del Regolamento UE che pur rubricato "pratiche di IA vietate", al par. 1, comma 1, lett. h), dopo aver previsto il divieto di uso di sistemi di identificazione biometrica "in tempo reale" in spazi accessibili al pubblico, ai punti i) e ii) - e iii) di cui si dirà più avanti -, ne ammette la possibilità per specifiche ragioni[1].

---

[1] Si riporta di seguito l'art. 5, par. 1, comma 1, lett. h), secondo cui
"*Sono vietate le pratiche di IA seguenti:*
omissis
h) l'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto a meno che, e nella misura in cui, tale uso sia strettamente necessario per uno degli obiettivi seguenti:
i) la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse;
ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico;
iii) la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'allegato II, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni.

Queste ultime - di natura chiaramente preventiva - sono espressamente menzionate nei commi 1 e 2, che regolano, in particolare, il caso che i sistemi di IA debbano essere usati dalla polizia ai fini dell'identificazione biometrica remota in tempo reale, in luoghi pubblici o aperti al pubblico, per confermare l'identità delle persone, per finalità di prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico (art. 5, par. 1, comma 1, lettera *h)*, punto *ii)*, Regolamento UE) e per la ricerca di una persona scomparsa o di persone specifiche, vittime dei reati di sequestro di persona, tratta di esseri umani o sfruttamento sessuale (art. 5, par. 1, comma 1, lettera *h)*, punto *i)*, Regolamento UE).

Per evitare, però, il rischio di una progressiva costituzione di "banche dati generali" di riconoscimento facciale, il comma 3 impone di utilizzare per il confronto biometrico una banca dati, il cui contenuto sia formato *ad hoc*, con i soli dati biometrici pertinenti alla specifica finalità, da cancellarsi al termine della validità dell'autorizzazione, in modo da garantire che il set di confronto sia specifico per ciascuna autorizzazione e non sia suscettibile di alimentazione incrementale rispetto ad autorizzazioni pregresse.

Il Regolamento UE richiede, all'art. 5 par. 3 ([2]), come necessaria per l'utilizzo dei sistemi di IA "un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente" e tale indicazione viene tradotta nel diritto nazionale, dai commi 4 e 5 dell'articolo in esame, individuando l'autorità giudiziaria competente all'autorizzazione nel procuratore distrettuale della Repubblica, in coerenza con l'attribuzione a questo ufficio di altri poteri in materia di prevenzione dei reati, quali, in particolare, l'autorizzazione a disporre le intercettazioni preventive, di cui all'art. 226 disp. att. c.p.p.

In special modo, il comma 4 subordina l'utilizzo dei sistemi di IA ad una richiesta del questore o del comandante provinciale dell'Arma dei carabinieri o della Guardia di finanza, ovvero del responsabile dei servizi centrali della Polizia di Stato, dell'Arma dei Carabinieri e del corpo della Guardia di finanza al procuratore della Repubblica presso il Tribunale del capoluogo del distretto nel quale sono emerse le esigenze di prevenzione ovvero di ricerca; la richiesta deve specificare la finalità perseguite, la durata prevista dell'utilizzo dell'IA, l'area territoriale interessata, le persone interessate e ricercate, le banche dati di riferimento utilizzate ed i sistemi e le tecnologie impiegate.

Il procuratore della Repubblica, ai sensi del comma 5, autorizza l'utilizzo richiesto con decreto motivato, con riguardo ad uno specifico evento o per il tempo strettamente necessario (in ogni caso, non superiore a quindici giorni, prorogabili, però, per periodi successivi di quindici giorni, qualora permangano le condizioni giustificatrici), con riferimento ad un'area territoriale delimitata e all'indi-

---

[2] L'art. 5, par. 3, del regolamento UE prevede:
"*Ai fini del paragrafo 1, primo comma, lettera h), e del paragrafo 2, ogni uso di un sistema di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto è subordinato a un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente, la cui decisione è vincolante, dello Stato membro in cui deve avvenire l'uso, rilasciata su richiesta motivata e in conformità delle regole dettagliate del diritto nazionale di cui al paragrafo 5. Tuttavia, in una situazione di urgenza debitamente giustificata, è possibile iniziare a usare il sistema senza autorizzazione a condizione che tale autorizzazione sia richiesta senza indebito ritardo, al più tardi entro 24 ore. Se tale autorizzazione è respinta, l'uso è interrotto con effetto immediato e tutti i dati nonché i risultati e gli output di tale uso sono immediatamente eliminati e cancellati.*"

cazione delle persone specificamente interessate e ricercate, previa effettuazione delle valutazioni di cui all'articolo 5, paragrafo 2 del regolamento UE ([3]) e cioè tenendo in debito conto sia la natura della situazione che dà luogo al possibile uso (in particolare, la gravità, la probabilità e l'entità del danno che sarebbe causato in caso di mancato uso del sistema) sia le conseguenze dell'uso del sistema per i diritti e le libertà di tutte le persone interessate (in particolare, la gravità, la probabilità e l'entità di tali conseguenze).

In conformità alle previsioni del par. 3 dell'art. 5 Regolamento UE, i commi 6 e 7 dell'articolo in esame consentono, nei casi d'urgenza, quando vi è fondato motivo di ritenere che dal ritardo possa derivare un pregiudizio grave e irreparabile per le finalità perseguite, che l'utilizzo dei sistemi di IA possa essere avviato, su disposizione dell'organo di polizia, previa comunicazione, anche in forma orale, al procuratore della Repubblica e a condizione che esso sia limitato a quanto strettamente necessario, in ogni caso con delimitazione dell'area interessata e indicazione delle persone ricercate; il provvedimento adottato dall'organo di polizia va poi trasmesso al procuratore della Repubblica senza ritardo e, comunque, entro ventiquattro ore dall'inizio delle operazioni ed il procuratore, ove ritenga sussistenti, oltre che la dedotta urgenza, anche le condizioni giustificatrici, provvede all'emissione dell'autorizzazione, nelle successive ventiquattro ore.

L'art. 8 in commento, nel suo penultimo capoverso (comma 8), prevede - anche in questo caso in conformità con le indicazioni del Regolamento UE (par. 3 dell'art. 5)([4]) - le conseguenze del mancato rispetto dei termini e delle condizioni previsti per l'utilizzo dei sistemi di IA, cioè l'obbligo dell'interruzione dell'uso dei sistemi di intelligenza artificiale oggetto dell'autorizzazione, la cancellazione di tutti i dati personali, dei risultati e degli output acquisiti e prodotti, fatti salvi gli elementi acquisiti legittimamente sotto altra base giuridica e l'inutilizzabilità dei risultati forniti dai sistemi di intelligenza artificiale.

Nell'ultimo comma, invece, l'articolo 8 si occupa opportunamente di un aspetto di cui non si fa carico il Regolamento UE e cioè di quale sia il regime di utilizzabilità, in sede processuale penale, dei risultati dell'utilizzo dei sistemi di AI; lo fa, però, attraverso non una regolamentazione esplicita ma con un discutibile rinvio ad un comma della norma delle disposizioni di attuazione del codice di rito riguardante le intercettazioni cd preventive (il comma 5 dell'art. 226 disp. att. c.p.p.); il significato

---

[3] L'art. 5, par. 2, del regolamento UE prevede:

"*L'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto per uno qualsiasi degli obiettivi di cui al paragrafo 1, primo comma, lettera h), è applicato ai fini di cui a tale lettera, solo per confermare l'identità della persona specificamente interessata e tiene conto degli elementi seguenti:*

a) la natura della situazione che dà luogo al possibile uso, in particolare la gravità, la probabilità e l'entità del danno che sarebbe causato in caso di mancato uso del sistema;

b) le conseguenze dell'uso del sistema per i diritti e le libertà di tutte le persone interessate, in particolare la gravità, la probabilità e l'entità di tali conseguenze.

L'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto per uno qualsiasi degli obiettivi di cui al paragrafo 1, primo comma, lettera h), del presente articolo rispetta inoltre le tutele e le condizioni necessarie e proporzionate in relazione all'uso, conformemente al diritto nazionale che autorizza tale uso, in particolare per quanto riguarda le limitazioni temporali, geografiche e personali. L'uso del sistema di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico è autorizzato solo se l'autorità di contrasto ha completato una valutazione d'impatto sui diritti fondamentali come previsto all'articolo 27 e ha registrato il sistema nella banca dati UE conformemente all'articolo 49. Tuttavia, in situazioni di urgenza debitamente giustificate, è possibile iniziare a usare tali sistemi senza la registrazione nella banca dati dell'UE, a condizione che tale registrazione sia completata senza indebito ritardo."

[4] Il testo della norma è stato già riportato sopra alla nota n. 2

che sembra potersi ricavare dal rinvio è che sono processualmente inutilizzabili i risultati conseguiti attraverso l'utilizzo dei sistemi di IA in un eventuale processo penale, fatti salvi i fini investigativi, con il divieto, comunque, anche di sola menzione di tali risultati in atti di indagine e di poter essi costituire oggetto di una deposizione.

Riportato sinteticamente il contenuto della norma del decreto, possono essere date le indicazioni operative sia per l'autorità di polizia che per i magistrati dell'ufficio; in particolare:

- le autorità di polizia, specificamente sopra indicate, quando ritengono necessario utilizzare i sistemi di AI per le specifiche finalità preventive, devono depositare una richiesta motivata, indicando con precisione i presupposti che la giustificano, le finalità che intendono perseguire e le modalità concrete che intendono utilizzare, secondo quanto espressamente previsto nei commi 1, 2 e 3 dell'articolo in esame;
- la richiesta viene depositata presso la Procura della Repubblica ed il sostituto di turno, in base a quanto previsto dal vigente progetto organizzativo, dispone che essa sia iscritta a mod 45, autoassegnandosi il relativo procedimento, e in tempi più brevi possibili (ragionevolmente individuabili, in relazione alla tipologia di attività preventiva che deve essere svolta, in non oltre 48 ore dal momento del deposito), decide sull'istanza con decreto motivato, valutando la configurabilità dei presupposti, previsti dal comma 5 dell'articolo in esame;
- qualora consideri la richiesta di autorizzazione carente in ordine ai presupposti, alle finalità o alle modalità indicate, può richiedere, sempre con la necessaria tempestività, con atto scritto chiarimenti e/o integrazioni all'autorità di polizia che ha avanzato l'istanza;
- qualora l'autorità di polizia intenda autorizzare in via di urgenza l'utilizzo dei sistemi di AI, comunica oralmente tale suo intendimento al sostituto di turno, indicando sommariamente ed oralmente le ragioni dell'urgenza e trasmette poi il proprio provvedimento entro 24 ore dalla sua adozione;
- il sostituto di turno, ritenute eventualmente sussistenti le ragioni di urgenza e i presupposti a sostegno, convalida con provvedimento motivato, entro le successive 24 ore l'autorizzazione già data, indicando le modalità con cui i sistemi di AI debbano essere utilizzati;
- qualora il p.m. ritenga non configurabili i presupposti per la convalida, emette provvedimento motivato con cui specifica le ragioni per le quali non ha autorizzato l'attività e dispone l'immediata interruzione dell'utilizzo del sistema di IA, dandone immediata comunicazione all'organo di polizia istante;
- qualora la polizia ritenga necessaria la proroga dell'utilizzo del sistema di IA, almeno quarantotto ore prima della scadenza deposita richiesta motivata di proroga, indicando il periodo in cui è necessario proseguire l'attività;
- la richiesta di proroga viene valutata dal p.m. assegnatario del procedimento a mod 45 o, in caso di sua assenza, dal sostituto di turno;

- i provvedimenti disposti dal sostituto di turno di autorizzazione, di convalida o di proroga sono trasmessi in copia al Procuratore della Repubblica, che li raccoglierà in un apposito registro, per ragioni statistiche;
- l'organo di polizia, che ha richiesto l'autorizzazione o che l'ha disposta in via urgenza ed essa sia stata poi convalidata, comunica la cessazione dell'attività, indicando i risultati eventualmente ottenuti e dando atto dell'avvenuta cancellazione dei dati biometrici utilizzati per effettuare il confronto;
- qualora all'esito dell'attività svolta dovessero emergere elementi suscettibili di approfondimento investigativo, l'organo di polizia predispone un'autonoma annotazione, senza che siano menzionate le attività svolte attraverso il sistema di AI, secondo quanto stabilito dal secondo alinea del comma 5 dell'art 226 disp. att. c.p.p.;
- l'annotazione da ultimo indicata viene iscritta a mod 45 ed il procedimento viene assegnato *ratione materiae*, secondo i criteri previsti dal progetto organizzativo vigente, per svolgere gli eventuali accertamenti investigativi;
- il procedimento mod. 45, nel quale sono contenute la richiesta degli organi di polizia di utilizzo dei sistemi di IA, i provvedimenti adottati dal p.m. e le comunicazioni conclusive della p.g., viene definito con trasmissione del fascicolo all'archivio, con provvedimento sinteticamente motivato, nel quale deve darsi atto dell'avvenuta comunicazione da parte della polizia della cancellazione dei dati.

****

La seconda norma del titolo I che è opportuno trattare è l'**art. 10** del decreto che disciplina il **riconoscimento facciale a posteriori, effettuato dopo la commissione di un reato, ai fini di una ricerca mirata ovvero dell'identificazione della persona**.

La norma del decreto dà attuazione alla previsione del comma 1 del par. 10 dell'art. 26 del Regolamento UE ([5]).

Il riconoscimento facciale a posteriori, secondo quanto stabilito dal comma 1 dell'art. 10, è possibile nei soli casi in cui siano stati installati, in base a specifiche disposizioni di legge, sistemi di videosorveglianza integrati con componenti di IA.

Le componenti di IA, presenti nell'impianto di video registrazione, però, potranno essere attivate solo in due situazioni che presuppongono, in entrambi i casi, la commissione di un reato.

---

[5] L'art. 26 del Regolamento UE è rubricata "obblighi dei disployer dei sistema di IA ad alto rischio", il par.10, comma 1 prevede: "*Fatta salva la direttiva (UE) 2016/680, nel quadro di un'indagine per la ricerca mirata di una persona sospettata o condannata per aver commesso un reato, il deployer di un sistema di IA ad alto rischio per l'identificazione biometrica remota a posteriori chiede un'autorizzazione, ex ante o senza indebito ritardo ed entro 48 ore, da parte di un'autorità giudiziaria o amministrativa la cui decisione è vincolante e soggetta a controllo giurisdizionale, per l'uso di tale sistema, tranne quando è utilizzato per l'identificazione iniziale di un potenziale sospetto sulla base di fatti oggettivi e verificabili direttamente connessi al reato. Ogni uso è limitato a quanto strettamente necessario per le indagini su uno specifico reato.*"

La prima ipotesi, regolata nel comma 2 dell'articolo in esame del decreto, ha ad oggetto la possibilità di procedere al riconoscimento facciale a posteriori di una persona oggetto di ricerca mirata, in quanto indiziata della commissione di un reato.

Secondo il comma 1 del par. 10 dell'art. 26 del Regolamento UE, per attivare in questo caso l'utilizzo dei sistemi di IA sarebbe necessaria un'autorizzazione "da parte di un'autorità giudiziaria o amministrativa la cui decisione è vincolante e soggetta a controllo giurisdizionale".

Il decreto, con il comma 2 in esame, però, ha tradotto l'indicazione eurounitaria - la cui formulazione è analoga a quella dell'art. 5 (sopra già riportata) - in modo diverso da quanto aveva fatto con l'art. 8 sopra esaminato, non accontentandosi di un'autorizzazione del solo procuratore della Repubblica, ma richiedendo, presumibilmente in una logica di maggiore garanzia collegata alla delicatezza dell'attività da compiersi e nella prospettiva di un utilizzo dei risultati dell'attività in sede processuale, l'intervento del giudice.

Il capoverso stabilisce, infatti, che il p.m., su istanza degli ufficiali di polizia giudiziaria che hanno avviato i sistemi di IA, può chiedere al giudice per le indagini preliminari l'autorizzazione all'utilizzo dei predetti sistemi senza ritardo e comunque entro 48 ore dall'avvio degli stessi; il giudice, ricorrendo i presupposti, autorizza l'utilizzo con decreto motivato entro le successive 48 ore.

Nel caso di inosservanza dei termini o di mancata autorizzazione da parte del giudice, in conformità con quanto stabilito dal comma 2 del par. 10 dell'art. 26 del Regolamento UE ([6]), l'uso della tecnologia di riconoscimento facciale è immediatamente interrotto e tutti i dati personali, i risultati e gli output acquisti e prodotti sono cancellati, salvo che costituiscano corpo del reato.

Il capoverso in esame, essendo stato costruito sulla falsariga della disposizione europea, sembra individuare la polizia come l'unico soggetto che può dare avvio alla procedura autorizzatoria per effettuare il riconoscimento facciale a posteriori.

Il testo, però, non può non essere letto nel contesto del sistema dei rapporti fra p.g e p.m., così come delineato non solo nel codice di procedura penale (art. 55 e ss) ma anche nella Costituzione, con l'art. 109 e, quindi, alla luce del principio di subordinazione funzionale della prima al secondo.

Si deve di conseguenza ritenere che il p.m., anche di propria iniziativa, possa delegare alla p.g. l'utilizzo dei sistemi di IA, senza attendere alcun input da parte di essa, fermo restando che, una volta avviata l'attività delegata, debba poi richiedere l'autorizzazione entro 48 ore dall'avvio.

La seconda ipotesi, invece, regolata nel comma 3 del medesimo art. 10, si riferisce ad un'attività che la polizia giudiziaria può svolgere senza alcuna autorizzazione, in conformità pure a quanto previsto dall'art. 26, par. 10, comma 1, del regolamento UE; l'attività è consentita, in particolare, quando le tecnologie di riconoscimento facciale, integrate con componenti di IA, sono utilizzate esclusivamente dopo la commissione di un reato, al solo fine dell'identificazione iniziale di una persona potenzialmente indiziata della commissione del reato, sulla base di elementi oggettivi e verificabili,

[6] L'art. 26, par. 10, comma 2 del regolamento UE prevede che:
Se l'autorizzazione richiesta a norma del primo comma è respinta, l'uso del sistema di identificazione biometrica remota a posteriori collegato a tale autorizzazione richiesta è interrotto con effetto immediato e i dati personali connessi all'uso del sistema di IA ad alto rischio per il quale è stata richiesta l'autorizzazione sono cancellati

direttamente connessi al fatto di reato; in questo caso, l'utilizzo delle tecnologie è effettuato sotto la diretta ed esclusiva responsabilità dell'ufficiale di pubblica sicurezza, designato dal questore per la gestione dell'ordine e della sicurezza pubblica, ovvero, fuori da tale ipotesi, dell'ufficiale di polizia giudiziaria di cui all'art. 57, comma 1, lett. a) e b), c.p.p. che procede in relazione al reato; l'inosservanza delle previsioni riportate, comporta l'inutilizzabilità dei risultati ottenuti e l'obbligo della loro cancellazione, salvo che costituiscano corpo del reato.

Gli altri commi dell'articolo in esame riguardano soprattutto le modalità di conservazione dei dati e l'individuazione del titolare del trattamento degli stessi e possono essere tralasciate in questa sede, meritando, invece, solo due di essi una specifica menzione.
In particolare, va evidenziato il comma 4 che consente l'utilizzo dei sistemi di videosorveglianza, integrati da componenti di IA per luoghi ed eventi a rischio (quali possono essere gli impianti sportivi, i concerti e più in generale i grandi eventi anche se i criteri per individuare tali luoghi, ai sensi del comma 10 devono essere indicati con un decreto del ministro dell'interno, sentito il Garante); in questi casi, è ammesso il trattamento automatizzato delle immagini del volto e dei dati anagrafici delle persone che accedono ai luoghi in cui si tengono gli eventi in questione, senza però che vi sia elaborazione dei dati biometrici; solo nel caso di commissione di un reato, sarà possibile l'attivazione delle tecnologie di riconoscimento facciale. Non prevedendo il capoverso alcuna indicazione sulle modalità di attivazione delle tecnologie di riconoscimento facciale, deve ritenersi che l'attivazione potrà avvenire secondo quanto previsto dai già riportati commi 2 e 3, ricorrendone i rispettivi presupposti.
Il comma 10, invece, stabilisce che nessuna decisione produttiva di effetti giuridici negativi sulla persona cui si riferiscono i dati oggetto del trattamento può essere basata esclusivamente su di essi; la disposizione, per riprendere quasi pedissequamente il contenuto del comma 3, del par. 10 dell'art. 26 del Regolamento UE ([7]), appare *prima facie* non di agevole comprensione; essa, a ben vedere, sembra recare, invece, un importante principio, dettando il criterio di valutazione dei risultati forniti dall'applicazione di riconoscimento facciale in un eventuale processo penale, non solo nella fase del processo di merito, ma anche in sede di eventuali richieste cautelari; stabilisce cioè che i risultati in questione non possono essere considerati una prova autosufficiente nei confronti del soggetto interessato dall'attività di riconoscimento facciale, ma richiedono sempre elementi di necessario riscontro.

Come si evince dalla sintetica ricostruzione del contenuto dell'art. 10, la distinzione fra le due ipotesi di attivazione dei sistemi di IA è basata sull'essere quella del comma 2, che richiede l'intervento del

---

[7] L'art. 26, par. 10, comma 3 del regolamento UE prevede che:
In nessun caso tale sistema di IA ad alto rischio per l'identificazione biometrica remota a posteriori è utilizzato a fini di contrasto in modo non mirato, senza alcun collegamento con un reato, un procedimento penale, una minaccia reale e attuale o reale e prevedibile di un reato o la ricerca di una determinata persona scomparsa. Occorre garantire che nessuna decisione che produce effetti negativi su una persona possa essere presa dalle autorità di contrasto unicamente sulla base dell'output di sistemi di identificazione biometrica remota a posteriori.

giudice, una ricerca mirata di un soggetto già individuato quella, invece, del comma 3, attribuita all'esclusiva competenza della polizia, finalizzata all'identificazione iniziale di un soggetto ancora ignoto.

Il legislatore nazionale, però, riprendendo sul punto quanto stabilito dal Regolamento UE, individua per l'attivazione del sistema di IA da parte della polizia presupposti descritti in modo generico – e cioè che l'identificazione iniziale della persona potenzialmente indiziata della commissione del reato sia compiuta "*sulla base di fatti oggettivi e verificabili direttamente connessi al reato*" – circostanza, quest'ultima, che impone grande cautela da parte degli organi di polizia nell'utilizzare lo strumento in esame, quantomeno in una prima fase di attuazione della normativa e fino a quando la giurisprudenza non si sarà pronuncia in modo dirimente sul punto, attese le conseguenze che potrebbero derivare nel caso in cui si ritenessero insussistenti le condizioni legittimanti e cioè l'inutilizzabilità assoluta dei risultati conseguiti.

Con riferimento, invece, all'ipotesi in cui si debba procedere al riconoscimento facciale a posteriori ai sensi del comma 2, possono essere date le seguenti indicazioni operative:

- la p.g. inoltra la richiesta di autorizzazione al p.m. immediatamente dopo l'avvio dell'utilizzo dei sistemi integrati dall'IA; non prevedendo la norma un termine entro il quale va inoltrata l'istanza di autorizzazione - essendo stabilito, in ossequio a quanto stabilito dalla disposizione sovranazionale, soltanto che il p.m. debba chiedere al gip la relativa autorizzazione senza ritardo e comunque entro 48 ore dall'avvio degli stessi - si richiede che tale adempimento debba avvenire con massima tempestività e comunque non oltre le 24 ore;
- nella richiesta la polizia giudiziaria deve indicare con precisione l'orario in cui è stato avviato l'utilizzo dei sistemi di riconoscimento facciale, specificando gli elementi investigativi raccolti che consentono di ritenere la persona oggetto della ricerca mirata indiziata di uno specifico reato;
- il p.m. competente ad avanzare richiesta di autorizzazione è il titolare del procedimento nel quale l'utilizzo dei sistemi di IA deve essere effettuato, se un procedimento è stato già iscritto;
- nel caso, invece, non sia stato ancora iscritto un procedimento penale, la richiesta sarà avanzata dal sostituto di turno, previa iscrizione del procedimento a mod 21; il procedimento sarà poi assegnato al medesimo sostituto di turno o al sostituto di un gruppo specialistico, secondo i criteri previsti dal progetto organizzativo vigente;
- il p.m. di turno avanza richiesta motivata al Gip di autorizzazione all'utilizzo dei sistemi di IA per procedere al riconoscimento facciale, inderogabilmente entro 48 ore dal momento in cui è stata avviato l'utilizzo del sistema;
- nel caso in cui sia stato il p.m. a delegare alla p.g. l'attività di riconoscimento facciale, nella delega prevede che la p.g. comunichi con precisione il momento dell'attivazione dei sistemi di IA, in modo da poter richiedere entro 48 l'autorizzazione al Giudice.

****.

Il titolo II del decreto contiene "disposizioni penali, sostanziali e processuali, in materia di realizzazione e impiego illeciti dei sistemi di intelligenza artificiale e disposizioni processuali civili in materia di risarcimento dei danni cagionati dall'utilizzo dei sistemi medesimi".

La prima disposizione del titolo che necessita di essere menzionata è **l'art. 12** che innesta nel codice penale **una nuova fattispecie di reato, l'art. 437 bis,** la cui rubrica recita "**Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi**".
Il delitto è stato introdotto a seguito della delega recata dall'art. 24, comma 5, lett. b) della l. n. 132/2025 che richiedeva al Governo la "introduzione di autonome fattispecie di reato, punite a titolo di dolo o di colpa, incentrate sull'omessa adozione o sull'omesso adeguamento di misure di sicurezza per la produzione, la messa in circolazione e l'utilizzo professionale di sistemi di intelligenza artificiale, quando da tali omissioni deriva pericolo concreto per la vita o l'incolumità pubblica o individuale o per la sicurezza dello Stato".
Non può essere questa la sede per approfondire tutti gli aspetti della fattispecie, alquanto complessa nella sua struttura, bastando invece alcune limitate considerazioni, funzionali ad individuare quale articolazione dell'ufficio debba occuparsi delle eventuali notizie di reato relative.

Il legislatore, pur in presenza di una delega che consentiva di poter introdurre più ipotesi di reato, ha ritenuto di prevederne uno solo, che ha ad oggetto il compimento azioni o omissioni illecite di vario tipo sui sistemi di IA e che ha inserito nel Titolo VI dei delitti contro l'incolumità pubblica, nel Capo I, dei delitti di comune pericolo mediante violenza.
Nel delitto sono, però, contenute più fattispecie, costruite sul modello dei delitti di comune pericolo mediante omissione di cautele che sanzionano, in particolare, l'omissione dolosa delle misure di sicurezza previste per sistemi ad alto rischio, l'omissione colposa connotata da colpa grave, l'omissione intenzionale da parte dell'utilizzatore professionale ma anche l'alterazione dolosa degli stessi sistemi.
Tutte le fattispecie appaiono qualificabili come reati di pericolo concreto, in quanto per la loro punibilità dello stesso è richiesto che dal fatto derivi un pericolo per la vita o l'incolumità pubblica o individuale ovvero per la sicurezza dello Stato.
Sotto il profilo sanzionatorio, l'ipotesi delittuosa dalla quale derivi un pericolo per la vita o l'incolumità pubblica o individuale è meno grave di quella dalla quale derivi un pericolo per la sicurezza dello Stato.
La già evidenziata struttura a più fattispecie, la pluralità e la trasversalità dei beni giuridici tutelati (la vita, l'incolumità pubblica o individuale, la sicurezza dello Stato) sono elementi che non consentono di ascriverla agevolmente ad una delle sezioni o dei gruppi di lavoro previsti dal progetto organizzativo.

Quantomeno in questa prima fase, quindi, anche in attesa di verificare quale saranno gli spazi della sua effettiva applicazione, si ritiene di farla rientrare nella categoria residuale dei reati non riconducibili ad una sezione o ad un gruppo specialistico e cioè la cd area cd generica.

****

La seconda norma del titolo II da prendere in considerazione è l'**art. 13** che innesta una nuova disposizione nel codice di procedura penale, l'art. 359-*ter*, rubricato "**identificazione e localizzazione mediante sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale**".

In tal modo si è dato attuazione all'art. 5, par. 1, lett. h), punto iii) del Regolamento UE ([8]), sostanzialmente replicando nel procedimento penale il medesimo meccanismo già previsto, sia pure con non poche differenze connesse alla diversità delle finalità perseguite, dall'art. 8 del decreto, di cui si è già detto sopra.

In particolare, l'utilizzo di sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale è consentito in varie situazioni connesse ad un procedimento penale, e cioè per confermare l'identificazione di una persona, quando nei confronti della stessa sussistono sufficienti indizi di uno dei delitti indicati nell'allegato II al regolamento UE[9], puniti con la pena della reclusione non inferiore nel massimo a quattro anni; per la ricerca mirata, ivi compresa la localizzazione, di una persona indiziata dei medesimi delitti; per la ricerca, mediante localizzazione, di un latitante ai fini dell'esecuzione di un'ordinanza cautelare coercitiva ovvero di un ordine di carcerazione non sospeso sempre per i medesimi delitti; per la ricerca mirata, mediante localizzazione, nell'ambito di un procedimento penale, di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani.

In modo analogo a quanto già previsto nell'art. 8, il confronto biometrico anche in questo caso deve avvenire esclusivamente con una banca dati di riferimento, creata *ad hoc* per ciascun utilizzo, adeguata per ciascuna delle finalità di cui ai medesimi commi, contenente i dati biometrici e le relative informazioni identificative, ove disponibili, riferiti alle persone, anche non identificate; la banca dati può essere derivata da dati contenuti in banche dati in uso alla polizia giudiziaria o tenute da altre pubbliche amministrazioni e accessibili alla stessa o all'autorità giudiziaria, ovvero da immagini, filmati o altri elementi biometrici acquisiti legalmente nell'ambito delle indagini; i dati biometrici sono cancellati al termine della validità dell'autorizzazione, in modo da garantire che il set di

---

[8]. L'art. 5, par 1, lett. h) è riportato integralmente già sopra nella nota 1.

[9] I reati riportati nell'allegato II al regolamento UE sono i seguenti: terrorismo, tratta di esseri umani, sfruttamento sessuale di minori e pornografia minorile, traffico illecito di stupefacenti o sostanze psicotrope, traffico illecito di ami, munizioni ed esplosivi, omicidio volontario, lesioni gravi, traffico illecito di organi e tessuti umani, traffico illecito di materie nucleari e radioattive, sequestro, detenzione illegale e presa di ostaggi, reati che rientrano nella competenza giurisdizionale della Corte penale internazionale, illecita cattura di aeromobile o nave, violenza sessuale, reato ambientale, rapina organizzata o a mano armata, sabotaggio, partecipazione a un'organizzazione criminale coinvolta in uno o più dei reati in precedenza elencati.

confronto sia specifico per ciascuna autorizzazione e non sia suscettibile di alimentazione incrementale rispetto alle autorizzazioni pregresse

Per quanto riguarda, la procedura per l'utilizzo del sistema di IA per l'identificazione biometrica remota in tempo reale, il nuovo articolo del codice di rito, ai commi 4, 5, 6 e 7, traspone nell'ordinamento nazionale la norma del Regolamento UE (art. 5, par. 3) sulle modalità dell'autorizzazione ("autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente") in modo analogo a quanto ha già fatto nell'ipotesi dell'art. 10, ritenendo cioè indispensabile l'intervento del giudice e non sufficiente la mera autorizzazione del p.m.; si tratta di una scelta che appare coerente con l'impianto del codice di rito, in quanto l'attività da compiersi appare molto simile ad una intercettazione di immagini e, di conseguenza, opportunamente ricalca il procedimento acquisitivo di quest'ultima tipologia probatoria.

Quindi, in via ordinaria, l'utilizzo del sistema di IA è autorizzato preventivamente dal giudice per le indagini preliminari su richiesta motivata del p.m., con la delimitazione dell'area geografica di applicazione, l'indicazione delle persone specificamente da ricercare e la determinazione del tempo strettamente necessario, che non può superare i quindici giorni, prorogabili dal giudice per periodi di ulteriori quindici giorni nel caso in cui permangono le condizioni; il giudice può concedere l'autorizzazione previa effettuazione delle valutazioni di cui all'articolo 5, paragrafo 2 del regolamento UE ([10]) e cioè tenendo in debito conto sia la natura della situazione che dà luogo al possibile uso, in particolare la gravità, la probabilità e l'entità del danno che sarebbe causato in caso di mancato uso del sistema sia le conseguenze dell'uso del sistema per i diritti e le libertà di tutte le persone interessate, in particolare la gravità, la probabilità e l'entità di tali conseguenze

Nel caso di urgenza, l'utilizzo dei sistemi di IA può essere disposto dal p.m., con decreto motivato, che delimiti l'area, indichi le persone da ricercare e determini il tempo necessario; il decreto va trasmesso al Gip entro ventiquattro ore dal momento della sua adozione ed il giudice, se ricorrono i presupposti, lo convalida nelle successive quarantotto ore.

Nel caso di assoluta urgenza, tale da non consentire di attendere neppure il provvedimento del pubblico ministero, il sistema è attivato da un ufficiale di polizia giudiziaria, con successiva richiesta di autorizzazione entro dodici ore al pubblico ministero, che ne richiede la convalida al giudice per le indagini preliminari entro ventiquattro ore dall'avvio del sistema.

L'ultimo comma dell'articolo (il comma 8), prevede - anche in questo caso in conformità con le indicazioni del Regolamento UE - le conseguenze del mancato rispetto dei termini e delle condizioni previsti per l'utilizzo dei sistemi di IA e, in particolare, l'obbligo dell'interruzione dell'uso dei sistemi di intelligenza artificiale oggetto dell'autorizzazione, la cancellazione di tutti i dati personali, dei risultati e degli output acquisiti e prodotti, fatti salvi gli elementi acquisiti legittimamente sotto altra base giuridica e l'inutilizzabilità dei risultati forniti dai sistemi di intelligenza artificiale

---

[10] L'art. 5, par. 2, Regolamento UE è già riportato *supra*, nella nota n. 3

La disamina, sia pure molto rapida della disposizione, evidenzia un'incongruenza in ordine al giudice competente ad autorizzare o convalidare l'utilizzo dei sistemi di IA; l'art. 359-*ter* c.p.p. fa riferimento, esplicitamente o indirettamente, sempre al giudice per le indagini preliminari, anche nel caso in cui l'impiego dei sistemi di I.A. può servire per la ricerca di un latitante ai fini dell'esecuzione di una misura cautelare coercitiva ovvero di un ordine di carcerazione non sospeso, seppure la misura cautelare sia stata applicata da un giudice diverso dal GIP (ad esempio, il giudice del dibattimento di primo grado o quello di appello) e l'emissione di un ordine di carcerazione, presupponendo una sentenza di condanna definitiva, comporti, su tutte le questioni esecutive, la competenza del giudice dell'esecuzione *ex* art. 665 c.p.p..
L'indicazione testuale nella norma, per quanto non coerente con i principi del codice di rito, appare difficilmente superabile in via interpretativa per cui, quantomeno fino a quando non si pronuncerà la giurisprudenza, è opportuno comunque avanzare la richiesta di autorizzazione o richiedere la convalida al GIP.

Introducendo la norma del decreto un nuovo mezzo di ricerca della prova, la cui applicazione dipende dalle scelte investigative del p.m. designato per il procedimento, sono sufficienti alcune limitate indicazioni operative; in via ordinaria la richiesta di autorizzazione o di proroga spetta al p.m. titolare del procedimento e sempre a quest'ultimo compete eventualmente l'adozione del provvedimento di urgenza cui seguirà la richiesta di "convalida".
Nel caso, invece, in cui sia la polizia a disporre in via di urgenza l'avvio dei sistemi di IA, è opportuno che essa si coordini con il sostituto titolare del procedimento, avvisandolo immediatamente oralmente dell'inizio dell'attività; la polizia curerà di trasmettere in tempi più brevi possibili il provvedimento motivato con cui ha dato inizio l'attività e comunque non oltre le dodici ore, dando atto in esso dell'orario preciso di avvio; al p.m. titolare del procedimento (o in caso di sua assenza al sostituto di turno) spetterà richiedere la convalida, rispettando il termine complessivo di ventiquattro ore dall'avvio del sistema.
In caso di mancata convalida dei provvedimenti di urgenza, il p.m. dà disposizioni immediate alla p.g. di interrompere immediatamente il sistema di IA.

****

Delle altre disposizioni contenute nel titolo II è opportuno richiamare l'attenzione dei magistrati dell'ufficio su due di esse, in quanto di particolare rilevanza.

In primo luogo, **l'art. 14** che, in attuazione della delega recata dall'art. 24, comma 5, lett. *a)*, della l. n. 132/2025, ha **modificato l'articolo 104, comma 1, disp. att. c.p.p.**, sostituendo alla lettera e-*bis*) (introdotta dal recente decreto-legge n. 23/2026, conv. in l. n. 54/2026), le parole: "del profilo personale" con le seguenti: "generati anche con sistemi di intelligenza artificiale", consentendo in tal

modo il sequestro preventivo dei contenuti *online*, anche se generati con sistemi di intelligenza artificiale.

Nessuna modifica, invece, è stata introdotta sulle modalità di esecuzione del sequestro di cui alla citata lett. *e-bis)*, per cui essa va eseguito mediante un ordine di rimozione dei contenuti e dei dati o un ordine di inabilitazione dell'accesso al profilo rivolto ai prestatori di servizi di *hosting*, ai fornitori di piattaforme online o di motori di ricerca o ai prestatori di servizi intermediari della società dell'informazione, individuati sulla base della definizione di servizio di cui all'art. 1, par. 1, lett. b), della direttiva UE 2015/1535[11], garantendo, ove tecnicamente possibile, la fruizione dei contenuti estranei alle condotte illecite.

La seconda norma di interesse è l'**art. 15** che, in attuazione della delega recata dall'art. 24, comma 5, lett. *c)*, della l. n. 132/2025, ha **innestato nel d.lgs n. 231/2001 l'articolo 25-*vicies*** (rubricato *Reati commessi con l'uso di sistemi di intelligenza artificiale*), consentendo, in particolare, di procedere nei confronti degli enti per i delitti di cui agli artt. 437-*bis* e 612-*quater* c.p.

Si segnala che la nuova disposizione, al suo terzo comma, individua le sanzioni applicabili agli enti nel caso di commissione dei suddetti reati, escludendo, però, la più grave delle sanzioni interdittive, cioè quella di cui all'art. 9, comma 2, *lett. a)*, del d.lgs. n. 231/2001 e cioè l'interdizione dall'esercizio dell'attività.

****

La presente direttiva viene trasmessa al sig. Procuratore Generale presso la Corte di Appello di Salerno ai sensi dell'art. 14 della Circolare del CSM sull'organizzazione degli uffici di procura e va pubblicata sul sito dell'ufficio sia fra le *news* nell'home page che nella partizione relativa alle direttive e ai provvedimenti organizzativi.

Salerno, 4 novembre 2026

Il Procuratore della Repubblica
Raffaele Cantone

[11] L'art. 1, par. 1 lett. della direttiva UE 2015/1535 del Parlamento europeo e del Consiglio del 9 settembre 2015, così stabilisce:
Ai fini della presente direttiva si applicano le seguenti definizioni:
a) omissis;
b) «servizio»: qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi.