

CAMERA DEI DEPUTATI

XIV Commissione – Politiche dell’Unione Europea

Audizione informale – 22 luglio 2026

Osservazioni sullo schema di decreto legislativo recante 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 penale e civile (Atto del Governo n. 418)

*Federica Paolucci – Assegnista di ricerca in Diritto costituzionale, Università Bocconi,
Centro di Ricerca Baffi*

1. Oggetto delle osservazioni

L’analisi che segue si appunta sulla disciplina introdotta dal Titolo I dello schema di decreto in oggetto e, in particolare, dall’articolo 10, che contiene disposizioni sui «sistemi di videosorveglianza dotati della tecnologia di riconoscimento facciale a posteriori, integrata dall’intelligenza artificiale, per il contrasto dei reati».

Con la presente memoria si intende segnalare alcuni profili di possibile discordanza rispetto ai parametri costituzionali interni e, per il loro tramite, al regolamento (UE) 2024/1689 (AI Act) e alla CEDU, che il parere parlamentare potrebbe contribuire a comporre con interventi puntuali. Quattro i nodi sottoposti alle Commissioni: (i) l’ambito oggettivo di applicazione della norma; (ii) l’assetto dei presupposti e delle responsabilità delineato dall’articolo 10, comma 2; (iii) la mancata individuazione dei reati che legittimano il ricorso alle tecnologie di riconoscimento facciale a posteriori; (iv) la disciplina della valutazione d’impatto sui diritti fondamentali di cui all’articolo 27 del regolamento.

2. I parametri di riferimento

Conviene muovere da una premessa sistematica. Nell’ordinamento costituzionale italiano, l’impiego di strumenti investigativi capaci di incidere in modo particolarmente penetrante sulla sfera individuale è tradizionalmente accompagnato da un sistema di garanzie rafforzate. La riserva di legge, il controllo dell’autorità giudiziaria, la tassatività dei presupposti applicativi, la motivazione del provvedimento, i limiti temporali costituiscono altrettanti presidi volti a impedire che esigenze di sicurezza, prevenzione o repressione penale si traducano in forme arbitrarie di intrusione nella vita delle persone.

Per tali atti l'ordinamento conosce un modello scandito dagli articoli 13, 14 e 15 della Costituzione e ricostruito dalla Corte costituzionale come sistema fondato sul concorso di riserva di legge e intervento dell'autorità giudiziaria. Pur non costituendo sempre il riconoscimento biometrico una relazione diretta con la restrizione della libertà personale, un'ingerenza nel domicilio o un'interferenza con la libertà e la segretezza delle comunicazioni, tali disposizioni conservano, nondimeno, un significativo rilievo sistematico, in quanto esprimono un paradigma costituzionale comune secondo il quale gli strumenti investigativi maggiormente invasivi devono essere disciplinati dalla legge mediante presupposti sufficientemente determinati e accompagnati da garanzie procedurali e da forme di controllo proporzionate all'intensità dell'ingerenza.

Quali parametri direttamente pertinenti vengono anzitutto in rilievo l'articolo 2 della Costituzione, sotto il profilo della tutela della riservatezza, dell'identità personale e dell'autodeterminazione informativa, e l'articolo 3, con riguardo alla ragionevolezza della disciplina e ai rischi di trattamenti discriminatori. A essi si affianca l'articolo 117, primo comma, della Costituzione, in relazione all'articolo 8 CEDU, che subordina le ingerenze nella vita privata alla presenza di una base legale prevedibile, al perseguimento di uno scopo legittimo e al rispetto dei requisiti di necessità e proporzionalità. Nell'ambito di applicazione del diritto dell'Unione assumono, inoltre, specifico rilievo gli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, relativi, rispettivamente, al rispetto della vita privata e alla protezione dei dati personali.

Quando i risultati prodotti dal sistema sono acquisiti o utilizzati nel procedimento penale, occorre altresì prendere in considerazione gli articoli 24 e 111 della Costituzione, in particolare sotto il profilo della possibilità per la persona interessata di conoscere, verificare e contestare l'impiego dello strumento e l'attendibilità dei risultati che ne derivano.

La Corte Costituzionale, nella sentenza n. 252 del 2020, in materia di perquisizioni operate dalla polizia giudiziaria, ha ribadito che proprio l'ampliamento dei poteri di quest'ultima esige precise garanzie costituzionali, imperniate sull'intervento del pubblico ministero e sulla convalida dei suoi atti¹. Parimenti, la giurisprudenza costituzionale sulle misure di prevenzione conferma che il riferimento alla sicurezza pubblica non neutralizza le garanzie costituzionali². Trattasi del paradigma che informa la disciplina delle intercettazioni, predisposto attorno a un catalogo tassativo dei reati presupposto selezionati per gravità edittale o per tipologia (articolo 266 c.p.p.), decreto motivato, limiti di durata, controllo del giudice.

¹ Corte Costituzionale, sentenza n. 252 del 2020, dep. 26/11/2020.

² Corte Costituzionale, sentenza n. 291/2013, dep. 6/12/2013, e n. 24/2019, dep. 27/02/2019.

A questi parametri si affianca, sul piano dei rapporti tra ordinamenti, l'indirizzo che la Corte costituzionale ha progressivamente assestato a partire dalla sentenza n. 269 del 2017 e portato a maturazione, da ultimo, con la sentenza n. 71 del 2026³: la violazione, da parte della legge interna, di norme del diritto dell'Unione dotate di «tono costituzionale» è direttamente sindacabile in riferimento agli articoli 11 e 117, primo comma, della Costituzione, come si premetteva. Resta ferma, nel quadro del concorso dei rimedi, la possibilità di non applicare la disposizione interna incompatibile con una norma unionale direttamente efficace e di promuovere il rinvio pregiudiziale alla Corte di giustizia.

Ne discende che l'eventuale difformità del decreto rispetto all'AI Act non resterebbe questione di mero adeguamento tecnico, ma assumerebbe immediato rilievo costituzionale, cui si aggiunge, trattandosi di decreto delegato, il possibile profilo di eccesso rispetto al criterio di coerenza con il regolamento posto dall'articolo 24 della legge n. 132 del 2025, rilevante ai sensi dell'articolo 76 della Costituzione.

Prima di muovere all'analisi delle questioni attinenti al contenuto dello schema di decreto, giova rammentare che il riconoscimento facciale a posteriori, identificazione biometrica remota diversa da quella in tempo reale, ai sensi dell'articolo 3, punto 43), del regolamento, è qualificato dal legislatore europeo come sistema ad alto rischio (allegato III, punto 1, lettera a)). L'AI Act stabilisce, difatti, una *lex specialis* (Considerando 38) che disciplina il riconoscimento biometrico come utilizzo vietato per la parte in tempo reale, salvo le eccezioni nell'ambito del *law enforcement*, e come ad "alto rischio" per il secondo. Pertanto, oltre alla disciplina dell'articolo 26, paragrafo 10, dell'AI Act, su cui si tornerà, viene in rilievo la giurisprudenza della Corte di giustizia sulla terzietà dell'organo chiamato al controllo preventivo sugli strumenti d'indagine incidenti sulla vita privata e sulla necessità che sia la legge nazionale a graduare condizioni e limiti dell'ingerenza in funzione della gravità dei reati perseguiti⁴.

Sul versante convenzionale, la Corte europea dei diritti dell'uomo (Corte EDU), nella sentenza *Glukhin c. Russia* ha qualificato il riconoscimento facciale come tecnologia «altamente intrusiva», riscontrando la violazione dell'articolo 8 CEDU con riguardo a entrambe le declinazioni della tecnologia, quella differita, impiegata per identificare il ricorrente a partire da filmati pubblicati online, e quella in tempo reale, utilizzata per localizzarlo e trarlo in arresto⁵. La Corte EDU ha subordinato la legittimità convenzionale dell'impiego alla presenza di «regole dettagliate» sul perimetro applicativo e di «solide

³ Corte cost., sent. n. 269 del 2017, e progressivamente assestato dalle sentt. n. 20 del 2019, n. 181 del 2024 e, da ultimo, n. 71 del 2026, che ammette il sindacato di costituzionalità, in riferimento agli artt. 11 e 117, primo comma, Cost., delle disposizioni interne in contrasto con il diritto dell'Unione, ogniquale volta la violazione presenti un «tono costituzionale» (cfr. n. 181/2024).

⁴ CGUE (Grande Sezione), C-746/18, *H.K. c. Prokuratuur*, 2 marzo 2021; CGUE (Grande Sezione), C-548/21, *Bezirkshauptmannschaft Landeck*, 4 ottobre 2024.

⁵ Corte EDU (Sez. III), *Glukhin c. Russia*, ric. n. 11519/20, 4 luglio 2023.

garanzie» contro l'abuso e l'arbitrio: esigenze di garanzia previste per entrambe le tipologie di riconoscimento facciale⁶.

3. L'oggetto della regolazione

L'AI Act introduce, come si premetteva, una disciplina speciale per l'uso di strumenti di «identificazione biometrica remota in tempo reale» (articolo 5, paragrafo i, lettera h) e di «identificazione biometrica remota a posteriori» (articolo 26, Allegato III, paragrafo 1, lettera a). La nozione inserita nel regolamento europeo abbraccia, anche in virtù della sua natura tecnologicamente neutra, qualsiasi identificatore biometrico automatizzato a prescindere dal fatto che il riconoscimento avvenga sulla base di dati del volto o di altre caratteristiche biometriche (ad esempio, voce, andatura, o altre caratteristiche fisiche).

Lo schema, all'articolo 10, di contro, disciplina il solo «riconoscimento facciale», seppur faccia uso sia nell'epigrafe del Capo III sia nell'articolo 8 di riconoscimento della più ampia formula di «sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale».

La differenza, tutt'altro che nominalistica, attiene all'ambito materiale di applicazione della norma nazionale, giacché i sistemi di identificazione biometrica a posteriori fondati su identificatori diversi dal volto restano privi di disciplina nazionale, pur ricadendo nel regolamento, con conseguente incertezza sul regime loro applicabile.

Inoltre, nulla è previsto per i sistemi di riconoscimento delle emozioni, che il regolamento vieta soltanto nei luoghi di lavoro e negli istituti di istruzione (articolo 5, paragrafo 1, lettera f)) e qualifica, negli altri ambiti, come sistemi ad alto rischio (allegato III, punto 1, lettera c)): il loro eventuale impiego per finalità di polizia resterebbe dunque fuori dal perimetro dello schema, in un'area di particolare delicatezza per la libertà della persona.

Sarebbe opportuno che la disciplina nazionale definisse espressamente l'ambito oggettivo della disciplina e prendesse posizione sui sistemi biometrici diversi dal riconoscimento facciale, specie su quelli di riconoscimento emotivo.

4. L'articolo 10, comma 2

Un primo punto attiene al presupposto classificatorio. Il comma 1 dell'articolo 10 individua il discrimine rispetto all'identificazione in tempo reale in un «intervallo di tempo tale da non configurare un'identificazione biometrica remota in tempo reale ai sensi del regolamento IA»: formula che rinvia alla nozione da definire, senza fissare criteri quantitativi o funzionali di demarcazione. Il punto è definitorio e dirimente poiché dalla qualificazione dipende l'individuazione del regime applicabile: da un lato, difatti, opera

⁶ § 82, *id.*

l'autorizzazione del procuratore della Repubblica (articolo 8) o del giudice per le indagini preliminari (articolo 359-ter c.p.p.), dall'altro la sola responsabilità interna all'amministrazione che intende utilizzare gli strumenti di IA in esame.

In tal senso, il considerando 17 del regolamento avverte che la nozione di «tempo reale» ricomprende anche l'uso con limitati ritardi di breve durata, proprio al fine di prevenire elusioni⁷; lasciare l'«intervallo» indeterminato, e di fatto rimesso alla configurazione operativa del sistema, significa consegnare all'utilizzatore la scelta del regime di garanzia applicabile. Sarebbe opportuno che il decreto, o, quantomeno, il decreto ministeriale attuativo, definisse criteri oggettivi di demarcazione, anche alla luce degli effettivi strumenti che si intenderanno utilizzare.

Il rilievo centrale che si intende qui sottoporre all'attenzione delle Commissioni attiene però all'architettura del comma 2. La disposizione affida l'utilizzo delle tecnologie di riconoscimento facciale a posteriori alla «diretta ed esclusiva responsabilità» dell'ufficiale di pubblica sicurezza designato dal questore ovvero, fuori da tale ipotesi, dell'ufficiale di polizia giudiziaria che procede in relazione al fatto di reato. Il comma 2 non fa riferimento, né esplicito né implicito, ad un'altra tipologia di intervento autorizzativo o di convalida da parte di un'autorità esterna.

Oltre ai profili di costituzionalità che si presentano nelle osservazioni svolte *infra*, si richiama la disciplina prevista dall'AI Act, al menzionato articolo 26, paragrafo 10, che, come peraltro anche richiamato dal Dossier n. 728 predisposto dal Servizio Studi,⁸ nel quadro di un'indagine per la ricerca mirata di una persona sospettata o condannata per un reato, subordina l'uso del sistema all'autorizzazione, richiesta *ex ante* o comunque entro quarantotto ore, di un'autorità giudiziaria o di un'autorità amministrativa la cui decisione sia vincolante e soggetta a sindacato giurisdizionale, con la sola eccezione dell'identificazione *iniziale* di un potenziale sospetto fondata su «fatti oggettivi e verificabili direttamente connessi al reato».

Lo schema in analisi riprende in parte la lettera dell'eccezione, il riferimento agli «elementi oggettivi e verificabili», ma se ne discosta in due punti: non riproduce il requisito della connessione diretta di tali elementi con il reato e non circoscrive l'esenzione dall'autorizzazione alla sola identificazione iniziale, sì che l'esenzione, congegnata dal legislatore europeo come valvola per la fase germinale dell'accertamento, finisce per assumere portata generale. In virtù dell'indirizzo richiamato al §2 della

⁷ Cfr. considerando 17 del regolamento (UE) 2024/1689, secondo cui la nozione di identificazione «in tempo reale» comprende anche l'uso con «limitati ritardi di breve durata», al fine di evitare elusioni, mentre l'identificazione «a posteriori» presuppone un ritardo «significativo».

⁸ Servizio Studi, *Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità penale e civile*, Dossier n. 728, 6 luglio 2026. In particolare, si veda pag. 46 per l'analisi relativa al comma 2 dell'articolo 10 dello schema di decreto.

presente relazione, il profilo assume rilievo ai sensi degli articoli 11 e 117, primo comma, della Costituzione, oltre che dell'articolo 76, in relazione al criterio di coerenza con il regolamento posto dalla legge di delegazione, giacché la funzione di garanzia risulta nella formula attuale interamente internalizzata nella struttura del *deployer*, ossia l'utilizzatore del sistema.

Misurato sul parametro interno, l'assetto suscita perplessità dal punto di vista costituzionale. Con specifico riferimento alle perquisizioni personali e domiciliari, la Corte costituzionale, nella sentenza n. 252 del 2020, cit., ha ritenuto che l'ampliamento dei poteri attribuiti alla polizia giudiziaria dovesse essere accompagnato da un «plus di garanzie», individuato, nella fattispecie esaminata, nell'intervento del pubblico ministero e nella successiva convalida motivata. Sebbene tale pronuncia si sia formata nel distinto ambito applicativo degli articoli 13 e 14 Cost., la sua *ratio* offre un argomento sistematico utile anche per la disciplina in esame: all'accrescimento della capacità invasiva degli strumenti investigativi deve corrispondere un adeguato rafforzamento delle garanzie procedurali e delle forme di controllo.

Merita, altresì, distinta considerazione il doppio binario delineato dal comma 2, che affianca all'ufficiale di polizia giudiziaria l'ufficiale di pubblica sicurezza designato dal questore per la gestione dell'ordine e della sicurezza pubblica. Poiché l'articolo 26, paragrafo 10, colloca l'impiego del riconoscimento a posteriori «nel quadro di un'indagine», l'attivazione in un contesto amministrativo, ancorché occasionata dalla commissione di un reato, rischia di collocarsi ai margini del perimetro funzionale tracciato dal regolamento, o quantomeno di renderne incerti i confini, in un ambito nel quale la prevedibilità della base legale costituisce, tanto per la giurisprudenza costituzionale quanto per quella convenzionale, requisito di legittimità dell'ingerenza. Andrebbe chiarito che anche in tale ipotesi l'impiego resta funzionale all'identificazione di persone indiziate di uno specifico reato ed è ricondotto al medesimo regime di controllo.

L'assenza del presidio esterno determina, infine, una significativa asimmetria interna allo schema: per l'identificazione in tempo reale, anche nella variante urgente, è sempre previsto l'intervento, quantomeno in convalida, dell'autorità giudiziaria; per quella a posteriori, alcun intervento è contemplato. Una simile divaricazione appare di dubbia ragionevolezza, ex articolo 3 della Costituzione, anche alla luce della sentenza *Glukhin*, sopra richiamata, che conferma il carattere significativamente invasivo dell'identificazione differita e l'esigenza che anche tale impiego sia accompagnato da regole dettagliate e solide garanzie contro ogni arbitrio.

Quanto ai correttivi, il modello più coerente con il regolamento europeo e il paradigma interno è l'autorizzazione dell'autorità giudiziaria secondo lo schema previsto

dall'articolo 359-ter c.p.p., pure introdotto dallo schema in esame, che allo stato è esclusivamente applicabile al riconoscimento biometrico in tempo reale.

5. La mancata individuazione dei reati presupposto

Il comma 2 consente l'attivazione delle tecnologie di riconoscimento facciale a posteriori «dopo la commissione di un fatto di reato, anche nell'ipotesi tentata». La formulazione attuale non fa riferimento ad alcuna fattispecie specifica, né a selezione tipologica né a soglia edittale. Per apprezzare la portata della scelta conviene ricostruire il riparto operato dal regolamento.

Per l'identificazione in tempo reale è il legislatore europeo stesso a selezionare i reati: l'articolo 5 ne consente l'impiego, tra l'altro, per la localizzazione o l'identificazione di persone sospettate dei reati di cui all'allegato II, puniti con una pena detentiva non inferiore nel massimo a quattro anni, e rimette agli Stati membri la facoltà di delimitare ulteriormente, o di non introdurre affatto, la relativa disciplina: facoltà che lo schema esercita, recependo catalogo e soglia nell'articolo 359-ter c.p.p.

Per l'identificazione a posteriori, viceversa, l'articolo 26, paragrafo 10, non contiene alcun elenco di reati: esige che ciascun uso sia strettamente necessario all'indagine su uno specifico reato e autorizza espressamente, all'ultimo capoverso del paragrafo 10, l'adozione di norme nazionali più restrittive. La selezione dei reati presupposto è, in altri termini, uno spazio che il regolamento lascia deliberatamente al legislatore nazionale, e lo schema, in quello spazio, sceglie di non operare alcuna selezione.

È qui che il paradigma interno torna a offrire un *tertium comparationis* utile per assicurare, tra le altre cose, coerenza interna nell'ordinamento. Per le intercettazioni, lo strumento cui la riflessione costituzionalistica ha da sempre commisurato gli atti d'indagine tecnologicamente intrusivi, l'articolo 266 c.p.p. individua i reati presupposto attraverso il duplice criterio della soglia edittale e della selezione per tipologia, calibrando così l'intrusività dello strumento sulla gravità del fatto.

L'assenza di qualunque filtro nell'articolo 10 si espone pertanto a un triplice ordine di rilievi: di proporzionalità, di determinatezza e prevedibilità della base legale, secondo il canone fatto proprio dalla sentenza n. 24 del 2019⁹, e di ragionevolezza intrinseca, ex articolo 3 della Costituzione, rispetto al ben più selettivo regime riservato all'identificazione in tempo reale.

Si suggerisce, pertanto, di introdurre anche per gli strumenti di IA disciplinati dall'articolo 10 un catalogo di reati presupposto o, quanto meno, l'individuazione di una

⁹ Corte Costituzionale, n. 24/2019, dep. 27/02/2019, cit.

soglia di pena edittale, secondo la tecnica normativa già collaudata dall'articolo 266 c.p.p. e ripresa dall'articolo 359-ter c.p.p.

6. La valutazione d'impatto sui diritti fondamentali

L'articolo 27 del regolamento impone ai *deployer* che siano organismi di diritto pubblico di effettuare, prima del primo utilizzo di un sistema ad alto rischio di cui all'allegato III, categoria cui l'identificazione biometrica remota a posteriori appartiene, una valutazione d'impatto sui diritti fondamentali (FRIA), con notifica dei risultati all'autorità di vigilanza del mercato. Lo schema, tuttavia, richiama espressamente la FRIA soltanto per l'identificazione in tempo reale (articolo 9, comma 1), mentre per i sistemi di IA di cui all'articolo 10 il comma 5 prevede unicamente la valutazione d'impatto sulla protezione dei dati e la consultazione del Garante ai sensi degli articoli 23 e 24 del decreto legislativo n. 51 del 2018.

I due istituti, è opportuno ribadirlo, non sono fungibili: la valutazione d'impatto sulla protezione dei dati opera sul piano del trattamento e dei rischi per gli interessati in quanto tali; la FRIA investe il processo in cui il sistema è destinato a inserirsi, le categorie di persone e i gruppi verosimilmente incisi, i danni specifici che possono derivarne, le misure di sorveglianza umana e i meccanismi di governo interno e di reclamo.

Le due valutazioni possono integrarsi, come peraltro previsto dallo stesso articolo 27 dell'AI Act, ma non sono sostitutive in special modo in assenza di un'effettiva complementarità da doversi valutare caso per caso. Quanto alla DPIA, la possibilità di una valutazione comune dovrebbe restare subordinata all'effettiva omogeneità dei trattamenti, dei contesti operativi, delle categorie di interessati e dei rischi. Distintamente, la FRIA deve essere aggiornata quando cambiano o non sono più attuali gli elementi indicati dall'articolo 27, paragrafo 1, del regolamento.

Il silenzio dello schema non esonera, beninteso, le amministrazioni dall'obbligo, che discende direttamente dal regolamento; ma alimenta l'equivoco per cui l'adempimento *privacy* esaurirebbe la fase valutativa preventiva, e priva la FRIA di ogni aggancio procedimentale interno.

Desta perplessità, inoltre, la previsione del comma 5 dell'articolo 10 dello schema in esame secondo cui è possibile effettuare «un'unica valutazione d'impatto sulla protezione dei dati valida per tutti i sistemi analoghi»: questa ipotesi non dovrebbe tradursi in un'automatica estensione della valutazione a contesti operativi non del tutto analoghi. Occorrerebbe pertanto precisare che il *deployer* deve verificare l'effettiva analogia del caso concreto e aggiornare la valutazione ogniqualvolta mutino o non siano più attuali gli elementi indicati dall'articolo 27, paragrafo 1.

Una diversa logica mal si concilierebbe con la natura contestuale della valutazione, chiamata a misurarsi con i luoghi, gli eventi e le platee di interessati di volta in volta

coinvolti, nel pieno rispetto dei principi di diritto nazionale e dell'Unione europea, alla base dell'analisi relativa a violazioni e interferenze sui diritti fondamentali.

7. Ulteriori profili di analisi

Per completezza, si dà conto in forma sintetica di ulteriori profili che meriterebbero un autonomo approfondimento e che, per economia della presente relazione, ci si limita a segnalare.

a) La base di dati di riferimento (articolo 10, commi 3 e 4). Il comma 3 comporta il trattamento automatizzato dei dati biometrici estratti dalle immagini del volto di tutte le persone che accedono ai luoghi o agli eventi considerati, con memorizzazione nella base di dati di riferimento: un trattamento che prescinde da qualunque collegamento individuale con un reato e investe una platea indeterminata di soggetti estranei. La sua compatibilità con il principio di minimizzazione e con la giurisprudenza europea in materia di raccolta e conservazione generalizzate di dati richiederebbe un'autonoma verifica, anche in punto di informazione degli interessati.

b) Il rinvio al decreto del Ministro dell'interno (articolo 10, comma 11). Modalità del trattamento biometrico, misure di sicurezza e adempimenti del titolare sono rimessi a un decreto del Ministro dell'interno, sentito il Garante: una fonte secondaria adottata dalla medesima amministrazione titolare del trattamento, per profili che concorrono a definire il perimetro dell'ingerenza e che, secondo il canone della qualità della legge, dovrebbero trovare nella fonte primaria quantomeno i propri contenuti essenziali.

c) Il raccordo tra articolo 8 e articolo 359-ter c.p.p. Le due discipline dell'identificazione in tempo reale insistono su perimetri distinti: l'articolo 8 sulle finalità di cui all'articolo 5, paragrafo 1, lettera h), punti i) e ii), del regolamento (ricerca di persone scomparse e di vittime di specifici reati, prevenzione di minacce); l'articolo 359-ter sui delitti di cui all'allegato II, in attuazione del punto iii). I criteri di confine tra il canale preventivo-amministrativo e quello processuale non risultano però compiutamente definiti, con possibili incertezze applicative nelle ipotesi, tutt'altro che marginali, in cui l'esigenza preventiva emerga nel corso di un procedimento penale già pendente.

8. Conclusioni

Quattro le condizioni o osservazioni che si sottopongono alle Commissioni.

Prima: definire l'ambito di applicazione oggettivo della disciplina nella parte in cui l'articolo 10 parrebbe applicarsi ai soli strumenti di riconoscimento facciale, e non alla categoria più ampia di «sistemi di identificazione biometrica remota».

Seconda: introdurre all'articolo 10 un presidio autorizzativo esterno, l'autorizzazione dell'autorità e definire criteri oggettivi di demarcazione rispetto all'identificazione in tempo reale.

Terza: individuare i reati presupposto mediante catalogo e soglia di pena edittale, secondo la tecnica dell'articolo 266 c.p.p.

Quarta: richiamare espressamente la valutazione d'impatto sui diritti fondamentali di cui all'articolo 27 del regolamento anche per i sistemi dell'articolo 10, specificandone le modalità di svolgimento, notifica e aggiornamento.

Si ritiene che nessuno dei quattro interventi incida sulle scelte di fondo dello schema.