SED QUIS CUSTODIET IPSOS CUSTODES?[*] L'IDENTIFICAZIONE BIOMETRICA REMOTA A FINI DI POLIZIA IN ITALIA, FRANCIA E SPAGNA, E I SUOI TERMINI DI CONFRONTO NEGLI STATI UNITI D'AMERICA E NELLA REPUBBLICA POPOLARE CINESE.

di Damiano Fuschi[**]

Sommario. 1. Il problema e il metodo. – 2. L'ordinamento italiano. – 3. L'ordinamento francese. – 4. L'ordinamento spagnolo. – 5. Il modello europeo per induzione. – 6. Il termine intermedio di confronto: gli Stati Uniti d'America. – 7. Il termine esterno di controllo: la Repubblica popolare cinese. – 8. La variabile discriminante.

1. Il problema e il metodo. Il presente contributo muove da una distinzione tecnica che il diritto, europeo e nazionale, ha reso giuridicamente rilevante. Occorre tenere separate quattro operazioni: l'identificazione biometrica remota in tempo reale, che ricorre quando la cattura del dato biometrico, il confronto e l'identificazione avvengono istantaneamente o comunque senza ritardo significativo; l'identificazione *a posteriori*, in cui il dato è già stato acquisito e il confronto interviene solo successivamente, su materiale generato prima dell'uso del sistema rispetto alle persone interessate[1]; il confronto con dati liberamente accessibili in rete, ottenuti mediante *scraping* non mirato; la videosorveglianza algoritmica non biometrica, che rileva *pattern* comportamentali senza identificare la persona. La distinzione fra tempo reale e *a posteriori* non è cronometrica ma funzionale, e su di essa il regolamento (UE) 2024/1689 ha costruito l'intera architettura dei divieti e delle eccezioni: mentre la prima è vietata come regola generale e ammessa solo in ipotesi tassative, la seconda è ricondotta fra i sistemi ad alto rischio, subordinata alla ricerca mirata di un soggetto sospettato o condannato in relazione a un caso concreto[2]. È anche per questo che il tema appartiene al diritto pubblico europeo, e non soltanto al diritto interno di ciascuno Stato. L'art. 5, par. 5, del regolamento rimette agli Stati membri la scelta se ammettere, in tutto o in parte, l'identificazione in tempo reale, e impone loro di dettarne la disciplina di dettaglio; il par. 3 subordina ogni impiego all'autorizzazione preventiva di un'autorità giudiziaria o di un'autorità amministrativa indipendente la cui decisione sia vincolante. Il diritto dell'Unione fissa così il pavimento e il tipo di controllo, ma lascia agli ordinamenti nazionali l'individuazione dell'autorità e del

[*] *Sottoposto a referaggio.*

[**] Research Fellow in Diritto pubblico comparato – Università dell'Insubria.

[1] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce norme armonizzate sull'intelligenza artificiale, Considerando 17 e art. 3, punti 41-43.

[2] Reg. UE 2024/1689, art. 5, par. 1, lett. *h*), e art. 26, par. 10.

procedimento: è in questo spazio che la comparazione diventa necessaria[3].
Alla distinzione fra tempo reale e *a posteriori* se ne accompagna una seconda, spesso trascurata nel dibattito pubblico ma decisiva sul piano tecnico-giuridico: quella fra verificazione e identificazione biometrica. La prima è un confronto uno-a-uno, che conferma o smentisce che una persona sia chi dichiara di essere, misurando il suo dato biometrico contro un unico *template* già associato alla sua identità dichiarata; la seconda è un confronto uno-a-molti, che cerca una corrispondenza fra il dato rilevato e un intero archivio di riferimento, senza che la persona abbia dichiarato alcunché. È solo la seconda operazione – l'identificazione in senso stretto – a porre il problema che qui interessa, perché è la sola in cui l'iniziativa del confronto appartiene interamente all'autorità e non alla persona controllata; la prima, impiegata ad esempio per l'accesso a un dispositivo o a un varco doganale automatizzato, non richiede l'apparato di garanzie di cui si discorrerà, proprio perché la persona vi si sottopone volontariamente per un proprio scopo. Le pagine che seguono si occupano dunque, salvo diversa indicazione, della sola identificazione uno-a-molti.

Da questa premessa discende il *tertium comparationis* che regge l'intero impianto: non il contenuto delle tecnologie impiegate, sostanzialmente omogeneo negli ordinamenti esaminati, ma quale organismo autorizza l'identificazione biometrica di una persona a fini di polizia, su quale archivio di confronto, e con quali rimedi esperibili dall'interessato. È un criterio che consente di misurare, su basi comuni, esperienze che si presentano sotto forme testuali diverse – decreto legislativo delegato, *loi* sperimentale, legge organica – e che permette, allo stadio successivo, di includere nella comparazione un ordinamento estraneo alla famiglia romanistica senza che il confronto scada nell'accostamento meramente descrittivo.
La selezione dei casi risponde a una logica differenziata, che conviene dichiarare. Italia, Francia e Spagna sono esaminate come casi omogenei: soggette al medesimo regolamento (UE) 2024/1689 e alla medesima direttiva (UE) 2016/680, consentono di isolare per induzione ciò che resta costante al variare della scelta nazionale (*infra*, §§ 2-5). La Germania non è un quarto caso, ma una prova di tenuta delle invarianti così indotte fuori dal loro veicolo legislativo e dalla sottofamiglia cui i tre ordinamenti appartengono (*infra*, § 5). Gli Stati Uniti e la Repubblica popolare cinese sono invece termini di confronto in senso proprio, non casi da ricostruire con la medesima estensione: i primi servono a verificare se la separazione fra chi impiega la tecnologia e chi ne controlla l'uso basti da sola a qualificare il modello (*infra*, § 6), la seconda a verificare che cosa accada quando quella separazione manchi (*infra*, § 7). La diversa profondità dell'analisi è dunque una scelta di metodo, non un difetto di simmetria.
Va dichiarato, infine, il diverso statuto delle fonti. Per l'Italia l'analisi verte sul d.lgs. n. 160/2026, ma ne ricostruisce anche l'*iter*, perché è proprio nello scarto fra lo schema e il testo pubblicato che si misura l'incidenza dei controlli esterni. Per la Spagna l'oggetto è un *proyecto de ley orgánica* ancora all'esame delle Cortes; per la Francia, una disciplina sperimentale più volte prorogata. Per gli Stati Uniti si è privilegiato il livello statale e municipale, l'unico nel quale una disciplina esista; e dove il diritto positivo tace, come nelle vicende di elusione dei divieti municipali, si è fatto ricorso a inchieste giornalistiche, impiegate come indizio di prassi e non come fonte di regole. Per la Cina le fonti normative sono citate per provvedimento e articolo, in modo da consentirne il riscontro sul testo ufficiale.
Resta da giustificare, a questo punto del ragionamento, la scelta di introdurre la Repubblica popolare cinese come termine esterno di controllo, anziché limitare l'indagine ai tre

[3] Reg. UE 2024/1689, art. 5, parr. 3 e 5; per il trattamento dei dati biometrici a fini di polizia, dir. UE 2016/680, art. 10.

ordinamenti dell'Unione. La giustificazione richiede tre passaggi.

Primo. Le tassonomie successive al 1989 hanno registrato, con sostanziale concordia, la dissoluzione della famiglia giuridica socialista come categoria autonoma: collassata in Russia e nell'Europa orientale insieme al sistema politico che la sorreggeva, essa non ha più, nella comparatistica successiva, statuto di famiglia a sé stante[4]. Ciò che rimane problematico è la collocazione della Repubblica popolare cinese, che quel collasso non ha conosciuto e che la dottrina comparatistica riconduce, a seconda dei criteri prescelti, a un residuo socialista riformato dall'economia di mercato, a un ordinamento *sui generis* non riconducibile alle famiglie tradizionali, o a un più ampio modello dell'Asia orientale accomunato da tratti di derivazione confuciana e dalla ricezione selettiva di istituti romanistici[5]. Quell'ipotesi, del resto, non è una costruzione dottrinale astratta: poggia su un'opera di collaborazione scientifica trentennale, che a questo lavoro offre la verifica più netta della distinzione fra formante legislativo e formante politico[6].

Il rilievo che qui interessa è però di segno diverso da quello che larga parte di quella letteratura è incline a trarne. Dove il trapianto del diritto romano in Cina è comunemente letto come indice di un avvicinamento alla tradizione giuridica occidentale, esso mostra piuttosto l'esatta misura di ciò che un trapianto può e non può trasferire. Il formante legislativo ha viaggiato con successo storico – categorie, sistematica, apparato concettuale, financo i testi giustinianei in lingua cinese – mentre il formante politico non si è spostato di un passo: il medesimo ordinamento che nel 2020 adotta un codice civile di impianto romanistico colloca, cinque anni dopo, l'adesione alla direzione del Partito nel dispositivo del regolamento sulla

---

[4] K. Zweigert, H. Kötz, *An Introduction to Comparative Law*, Oxford, 1998; G. Ajani, *Il modello post-socialista*, Torino, 2008. Per l'inquadramento dell'ordinamento cinese nella comparatistica di lingua italiana resta fondamentale G. Ajani, A. Serafino, M. Timoteo, *Diritto dell'Asia orientale*, nel Trattato di diritto comparato diretto da R. Sacco, Torino, 2007; e già R. Sacco, (voce) *Cina*, in *Dig. disc. priv.*, Sez. civ., II, Torino, 1988, 360 ss. Nella tradizione continentale il riferimento classico è J. Escarra, *Le droit chinois*, Pékin-Paris, 1936.

[5] L. Moccia, *Il diritto in Cina. Tra ritualismo e modernizzazione*, Torino, 2009; Id., *Il sistema giuridico cinese: caratteri tradizionali e lineamenti attuali*, in *Rivista trimestrale di diritto e procedura civile*, LIV, 4, 2000, 1251 ss.; F.R. Antonelli, *Il diritto cinese. Dall'antica alla nuova Via della Seta*, Padova, 2021. Va peraltro segnalato che, con la promulgazione del Codice civile del 2020, una parte autorevole della dottrina ha ritenuto che il diritto cinese segnali marcatamente la propria presenza nella famiglia romanistica: v. R. Cardilli, *Diritto cinese e tradizione romanistica alla luce del nuovo Codice civile della RPC*, in *Mondo Cinese*, 167, 2020, 25 ss.; M. Timoteo, *Il Codice civile in Cina: oltre i* legal transplants*?*, ivi, 13 ss.; e, quanto al formante linguistico, Ead., *Il diritto nelle parole: aspetti linguistici del diritto cinese contemporaneo*, in E. Calzolaio, R. Torino, L. Vagni (a cura di), *Liber Amicorum Luigi Moccia*, Roma, 2021, 643 ss. Se questa lettura è corretta – e la scelta di riferirsi al tratto strutturale anziché alla collocazione genealogica ne risulta rafforzata, non indebolita – l'appartenenza alla famiglia romanistica cessa di poter spiegare la differenza che questo lavoro intende isolare.

[6] Nel febbraio 1989, in occasione di una visita a Roma, Jiang Ping, allora rettore dell'Università di Scienze politiche e Giurisprudenza della Cina, sottoscrisse con l'Università di Roma «Tor Vergata» un accordo di collaborazione in forza del quale la parte cinese avrebbe inviato giovani ricercatori a studiare il diritto romano in Italia e a tradurre in cinese frammenti scelti del *Corpus Iuris Civilis*; il coordinamento delle traduzioni dei *Digesta* fu assunto da Sandro Schipani. Da quel programma sono passati, fra gli altri, Xu Guodong, Fei Anling, Zhang Lihong, Huang Feng, Mi Jian, Ding Mei e Liu Jiaan, cioè una parte non marginale della civilistica che avrebbe poi preso parte all'elaborazione dei progetti di codice. All'accordo hanno fatto seguito quattro congressi internazionali di Pechino su *Diritto romano, diritto cinese e codificazione del diritto civile* (1994, 1999, 2005 e 2009), l'istituzione presso «Tor Vergata» di un Osservatorio sulla codificazione e formazione del giurista in Cina nel quadro del sistema giuridico romanistico, e la collana *Diritto cinese e sistema giuridico romanistico. Leggi tradotte della Repubblica popolare cinese*, diretta da S. Schipani e G. Terracina. Sull'esito, v. S. Schipani, *Il nuovo codice civile cinese: dai fondamenti romanistici al diritto vigente. Osservazioni introduttive*, in *Bullettino dell'Istituto di diritto romano «Vittorio Scialoja»*, s. IV, X (CXIV), 2020, 35 ss.; e, dal versante cinese, Xu Guodong, *La base romanistica della parte generale del codice civile cinese*, in *Bullettino dell'Istituto di diritto romano «Vittorio Scialoja»*, s. IV, VI (CX), 2016; per l'inquadramento storico del processo, M. Timoteo, *La lunga marcia della codificazione civile nella Cina contemporanea*, ivi, 35 ss.

videosorveglianza di pubblica sicurezza (*infra*, punto secondo) e affida il controllo sull'osservanza di quella disciplina all'organo di pubblica sicurezza gerarchicamente superiore (*infra*, § 7). Il contenuto delle categorie civilistiche si trasferisce; l'architettura del controllo sull'esecutivo no. È precisamente per questo che l'appartenenza a una famiglia giuridica, quand'anche la si ritenga acquisita, non può reggere da sola il peso della comparazione qui tentata.

Secondo. Di fronte a questa incertezza, il presente contributo non intende sciogliere la questione della collocazione storico-genealogica della Cina, bensì aggirarla: il modello viene qui definito per il tratto strutturale, non per l'appartenenza a una famiglia. Si assume come modello di riferimento quello nel quale la disciplina della tecnologia di sorveglianza promana dallo stesso apparato che la impiega, e il controllo sulla sua osservanza resta interno alla gerarchia di quell'apparato. Si tratta di un tratto verificabile sul testo positivo, non di un'inferenza sociologica: l'art. 3 del regolamento del Consiglio di Stato n. 799/2025 colloca l'adesione alla direzione del Partito comunista cinese nel dispositivo della disciplina sulla videosorveglianza di pubblica sicurezza, e non nel preambolo – il formante politico, per usare la nota terminologia di Rodolfo Sacco, non opera qui in modo criptico, ma risulta esplicitato nel formante legislativo stesso[7]. La scelta di privilegiare il tratto strutturale sulla collocazione genealogica trova riscontro in una tendenza della comparatistica successiva alle classificazioni per famiglie, che ripartisce i sistemi secondo il tipo di autorità cui spetta l'ultima parola sulle regole di condotta[8]. Nel diritto di tipo professionale quell'ultima parola appartiene a un corpo di giuristi che ne rivendica l'autonomia rispetto alla politica. Nel diritto di tipo politico spetta a chi detiene il potere esecutivo o l'apparato di partito, e la regola resta strumento di governo più che limite a esso. Nel diritto di tipo tradizionale, infine, risiede in una tradizione religiosa o consuetudinaria che precede la stessa distinzione fra diritto e politica. Applicata al presente oggetto, questa tripartizione offre più di un'etichetta: consente di formulare l'ipotesi di lavoro in termini verificabili. Se il tratto che qualifica il modello europeo è la separazione fra chi impiega la tecnologia e chi ne controlla l'osservanza, ci si attende che tale separazione sia tenuta in piedi da un ceto professionale – magistratura, autorità indipendenti, avvocatura – la cui legittimazione a intervenire non dipende dal consenso dell'esecutivo che la tecnologia impiega. L'ipotesi, come si vedrà, andrà in parte corretta: nella vicenda italiana uno dei correttivi decisivi è venuto da un organo politico, e ciò che la verifica confermerà è meno la natura professionale del controllore che la struttura del procedimento nel quale il controllo si inserisce (*infra*, § 8). Se, per converso, il controllo resta interno alla medesima gerarchia che applica la regola, ci si trova di fronte a un diritto del secondo tipo, quale che sia l'etichetta storico-genealogica che gli si voglia attribuire. È questa verifica, e non la collocazione in una famiglia, l'oggetto dei paragrafi che seguono (*infra*, §§ 2-7).

Terzo. Resta un'obiezione da affrontare, ed è la più insidiosa: Italia, Francia e Spagna appartengono tutte alla sottofamiglia romanistica, sicché il modello indotto (*infra*, §§ 2-5) rischia di essere il modello romanistico, e non un modello propriamente europeo. La corroborazione che consente di superare l'obiezione viene dall'esperienza tedesca, che alla sottofamiglia romanistica non appartiene, collocandosi nella famiglia germanica pur entro la comune tradizione di *civil law*, e il cui vincolo sull'esecutivo proviene per giunta da una fonte diversa da quella degli ordinamenti esaminati: non un atto legislativo che disciplini *ex ante* l'identificazione biometrica remota, ma la giurisprudenza costituzionale interna

[7] Regolamento sull'amministrazione dei sistemi di videosorveglianza di pubblica sicurezza, ordinanza del Consiglio di Stato (RPC) n. 799, art. 3; sulla teoria dei formanti, R. Sacco, *Legal Formants: A Dynamic Approach to Comparative Law*, in *The American Journal of Comparative Law*, 39, 1991, I, 1 ss., II, 343 ss.

[8] U. Mattei, *Three Patterns of Law: Taxonomy and Change in the World's Legal Systems*, in *The American Journal of Comparative Law*, 45, 1, 1997, 5 ss., spec. 21 ss.

Issn 2421-0528

sull'autodeterminazione informativa. Il Bundesverfassungsgericht, dichiarando incostituzionali le norme di Assia e di Amburgo sull'analisi automatizzata dei dati di polizia per violazione dell'art. 2, c. 1, in combinato disposto con l'art. 1, c. 1, della Legge fondamentale, ha fissato standard di proporzionalità che la prassi amministrativa tedesca sconta anche fuori dal perimetro del giudizio deciso[9]; ed è coerente con questo standard che le forze di polizia federali, dopo la sperimentazione del riconoscimento facciale in tempo reale alla stazione di Berlino Südkreuz nel 2017-2018, non abbiano più fatto ricorso al dispositivo in tempo reale, collocandosi la Germania così al di sotto della soglia che il regolamento (UE) 2024/1689 pure consentirebbe. Se l'invariante – separazione fra chi autorizza e chi impiega la tecnologia – si mantiene anche fuori dalla sottofamiglia romanistica, e anche dove la fonte del vincolo muta radicalmente, da delega legislativa a giurisprudenza costituzionale, essa è allora un tratto del modello, e non un prodotto della sottofamiglia cui i tre ordinamenti esaminati appartengono.

2. L'ordinamento italiano. La disciplina italiana dell'identificazione biometrica remota a fini di polizia nasce da una delega legislativa già esercitata solo in parte. L'art. 24, c. 2, lett. *h*), della l.n. 132/2025 ha delegato il Governo ad adeguare l'ordinamento interno al regolamento (UE) 2024/1689 anche quanto all'utilizzo dei sistemi di intelligenza artificiale nell'attività di polizia, fissando il termine del 10 ottobre 2026 per l'esercizio della delega[10]. In attuazione di essa il Consiglio dei ministri ha approvato in via preliminare, il 10 giugno 2026, due schemi di decreto legislativo gemelli: l'Atto del Governo n. 418, relativo all'impiego dei sistemi di IA nell'attività di polizia e alla responsabilità civile e penale, che è quello qui esaminato, e l'Atto del Governo n. 421, relativo alle autorità nazionali e alla formazione, che resta estraneo al presente oggetto. Il primo è divenuto il d.lgs. n. 160/2026, in vigore dal 30 settembre 2026[11].

---

[9] Bundesverfassungsgericht, *Urteil des Ersten Senats* del 16 febbraio 2023, 1 BvR 1547/19 e 1 BvR 2634/20. Il Primo Senato ha dichiarato incostituzionali, per violazione del diritto all'autodeterminazione informativa (art. 2, c. 1, in combinato disposto con l'art. 1, c. 1, della Legge fondamentale), le norme di Assia (§ 25a HSOG) e di Amburgo (§ 49 HmbPolDVG) che consentivano alla polizia l'elaborazione automatizzata di dati già acquisiti a fini di prevenzione. La pronuncia non riguarda specificamente l'identificazione biometrica: ha ad oggetto, più in generale, i sistemi di analisi automatizzata di banche dati di polizia (il *software* impiegato, di matrice Palantir, era condiviso dai due *Länder*). Ma proprio per questo la sua rilevanza ai fini del presente lavoro è indiretta e, si ritiene, più significativa: il Bundesverfassungsgericht vi ha fissato uno standard di proporzionalità stringente – necessità di indizi concreti riferiti a un fatto specifico, esclusione della mera raccolta preventiva indifferenziata – che vale come parametro generale per qualunque trattamento automatizzato di dati personali da parte della polizia, e dunque anche per un'eventuale identificazione biometrica remota, pur in assenza di una legge federale che la disciplini *ad hoc*. È in questo quadro che si colloca la scelta, empiricamente rilevabile, della polizia federale di non riattivare il riconoscimento facciale in tempo reale sperimentato nel 2017-2018 alla stazione di Berlino Südkreuz: non un divieto legislativo puntuale, ma l'effetto dissuasivo di uno standard costituzionale che eccede, nella sua severità, il pavimento fissato dall'art. 5, par. 1, lett. *h*), del regolamento (UE) 2024/1689. La Germania resta, cioè, sotto la soglia europea non per una scelta del legislatore ordinario paragonabile a quella francese (esclusione espressa della biometria dal perimetro della *loi* sperimentale), bensì per un vincolo di fonte giurisprudenziale-costituzionale che opera a monte di qualsiasi intervento legislativo – a riprova che la separazione strutturale fra chi impiega la tecnologia e chi ne controlla l'osservanza, quando è la variabile che si sta isolando, tollera mutamenti anche radicali nella fonte del vincolo senza perdere la propria identità di modello.

[10] L.n. 132/2025, *Disposizioni e deleghe al Governo in materia di intelligenza artificiale*, in G.U. n. 223 del 25 settembre 2025, art. 24, c. 2, lett. *h*).

[11] D.lgs. n. 160/2026, *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*, in G.U. n. 214 del 15 settembre 2026. Lo schema corrispondente è l'Atto del Governo n. 418, trasmesso alle Camere il 24 giugno 2026. La numerazione degli articoli è rimasta invariata nel passaggio dallo schema al decreto, mentre all'interno dell'art. 10 i commi risultano rinumerati: il c. 3 dello schema corrisponde al c. 4 del testo pubblicato, il c. 6 al c.

Il raffronto fra lo schema trasmesso alle Camere il 24 giugno e il testo pubblicato non è un'operazione di mero aggiornamento: è il terreno sul quale, come si vedrà, si misura l'incidenza dei controlli esterni sul procedimento normativo.

Il d.lgs. n. 160/2026 non prevede un'unica procedura di autorizzazione, ma tre, corrispondenti a tre distinte finalità dell'identificazione biometrica, e la loro sovrapposizione è la caratteristica più rilevante del testo. Per l'identificazione in tempo reale a fini di prevenzione, nonché di ricerca di persone scomparse o di vittime di specifici reati, l'art. 8 attribuisce l'autorizzazione al Procuratore della Repubblica presso il tribunale del capoluogo del distretto, su richiesta del questore, dei comandanti provinciali dell'Arma dei carabinieri e della Guardia di finanza o dei responsabili dei Servizi centrali, per non più di quindici giorni, prorogabili con decreto motivato. Nei casi di urgenza l'impiego può essere avviato previa comunicazione, anche orale, al Procuratore, con richiesta da trasmettere entro ventiquattro ore e decisione nelle ventiquattro successive[12]. Per l'identificazione in tempo reale a fini investigativi, l'art. 13 introduce nel codice di procedura penale l'art. 359-*ter*, che affida l'autorizzazione al giudice per le indagini preliminari, su richiesta del pubblico ministero, con un meccanismo di convalida in urgenza modellato su quello delle intercettazioni. Il decreto del pubblico ministero è comunicato al giudice entro ventiquattro ore e convalidato nelle quarantotto successive; se neppure il provvedimento del pubblico ministero può essere atteso, il sistema è attivato dalla polizia giudiziaria, che trasmette la richiesta al pubblico ministero entro dodici ore, e la convalida va chiesta entro ventiquattro ore dall'avvio[13]. Per il riconoscimento facciale a posteriori sulle immagini della videosorveglianza, infine, l'art. 10 distingue due ipotesi. La ricerca mirata di una persona indiziata di un reato richiede l'autorizzazione del giudice per le indagini preliminari, che il pubblico ministero chiede entro quarantotto ore dall'avvio dei sistemi e il giudice concede con decreto motivato nelle quarantotto ore successive. L'identificazione iniziale di una persona potenzialmente indiziata, dopo la commissione del reato e sulla base di elementi oggettivi e verificabili, non richiede invece alcuna autorizzazione, conformemente all'art. 26, par. 10, del regolamento, ed è condotta sotto la responsabilità dell'ufficiale di pubblica sicurezza designato dal questore o dell'ufficiale di polizia giudiziaria che procede. Titolare del trattamento è il Ministero dell'interno – Dipartimento della pubblica sicurezza[14]. Rispetto allo schema, che per il riconoscimento a posteriori non prevedeva alcun intervento del giudice, il testo pubblicato ha dunque esteso la riserva di giurisdizione a una parte del terzo canale.

È su quest'ultima disposizione che si è concentrato il rilievo critico del Garante per la protezione dei dati personali. Nel parere reso il 14 luglio 2026 sui titoli I e III dello schema di decreto, il Garante ha segnalato una tensione interna all'art. 10: il c. 3 dello schema consente la costituzione anticipata, in luoghi o in occasione di eventi che presentino esigenze di ordine e sicurezza pubblica, di un archivio biometrico esteso a chiunque vi acceda, mentre il c. 10 dello schema vieta l'identificazione biometrica generalizzata e non mirata. La soluzione indicata dall'Autorità è stata di spostare l'estrazione del dato biometrico a valle della registrazione, così che la banca dati resti costituita da immagini non ancora elaborate fino a quando non insorga una necessità investigativa concreta[15]. Pochi giorni dopo il Presidente dell'Autorità, in sede di audizione presso le Commissioni riunite Giustizia e Affari

7, il c. 9 al c. 10 e il c. 10 al c. 11. Salvo diversa indicazione, gli articoli sono citati nel testo pubblicato; i rinvii allo «schema» si riferiscono al testo del 24 giugno 2026.

[12] D.lgs. n. 160/2026, art. 8, cc. 4, 5, 6 e 7.

[13] D.lgs. n. 160/2026, art. 13, che introduce l'art. 359-*ter* c.p.p.; per i termini dell'urgenza, c. 7 del nuovo articolo.

[14] D.lgs. n. 160/2026, art. 10, cc. 2, 3 e 5.

[15] Garante per la protezione dei dati personali, parere sui Titoli I e III dello schema di decreto legislativo di adeguamento al reg. UE 2024/1689, provv. n. 531 del 14 luglio 2026.

costituzionali del Senato, ha depositato una memoria che isola il medesimo punto critico, mentre il 30 luglio 2026 un portavoce della Commissione europea ha pubblicamente ricordato che, nell'impianto del regolamento (UE) 2024/1689, il riconoscimento facciale negli spazi accessibili al pubblico costituisce, come regola, una pratica vietata – un monito esterno che si è inserito nel dibattito parlamentare proprio nei giorni in cui questo si avviava alla conclusione[16].

L'*iter* parlamentare merita, per la sua stessa cronologia, di essere ricostruito. Assegnato alle Commissioni riunite I (Affari costituzionali) e II di Camera e Senato il 26 giugno 2026, con termine per il parere fissato al 25 agosto, lo schema è stato oggetto di una serie di audizioni informali – fra gli altri Fernanda Faini, Federica Paolucci, Francesco Paolo Micozzi, oltre a rappresentanti della Polizia di Stato, della Guardia di Finanza e della Rete diritti umani digitali – prima di ricevere, il 30 luglio 2026, il parere favorevole delle Commissioni del Senato[17]. Le Commissioni della Camera hanno approvato, nella stessa giornata, un parere diverso da quello del Senato e, su tre punti, più garantista: la richiesta di affidare al giudice, anziché al Procuratore della Repubblica, l'autorizzazione all'identificazione in tempo reale nel canale dell'art. 8, «in coerenza con l'articolo 5, paragrafo 3, del regolamento (UE) 2024/1689»; la verifica dell'esito del sistema «da almeno due operatori fisici»; la qualificazione degli *output* dei sistemi di IA come «meri elementi di orientamento investigativo», privi di autonoma efficacia probatoria[18]. Merita di essere segnalato, per la sua rilevanza rispetto alla tesi del presente lavoro, che il relatore per la I Commissione, nel presentare il parere, ha giudicato «non corretta» l'interpretazione delle finalità del provvedimento offerta dagli articoli di stampa nei quali si faceva riferimento a «schedature di massa», al «Grande Fratello» e a «modelli cinesi»[19]: è un dato di cronaca parlamentare, non una fonte normativa, ma segnala come il termine di paragone impiegato in questo lavoro – il modello cinese, per l'appunto – non sia un artificio dell'analisi comparatistica, bensì un riferimento già presente, sia pure allo stato di formula polemica, nel dibattito pubblico sul provvedimento.

Un secondo dato emerso in sede parlamentare conferma, con maggiore precisione tecnica, i rilievi già mossi dal Garante. Nel parere del 30 luglio le Commissioni della Camera hanno formulato, già nella proposta dei relatori di maggioranza, osservazioni che intercettano proprio i due profili critici individuati da questo lavoro: la «non incrementalità del *set* di confronto» – cioè la necessità che la banca dati costituita per una singola autorizzazione non si sommi a quelle già esistenti – e l'«autonomia tra il momento di mera acquisizione delle immagini, rispetto a quello successivo di attivazione» delle tecnologie di riconoscimento facciale[20]. Si tratta, riformulata in sede parlamentare, della stessa separazione temporale fra

[16] Garante per la protezione dei dati personali, memoria del Presidente Pasquale Stanzione su AG 418, Senato della Repubblica, Commissioni riunite Giustizia e Affari costituzionali, luglio 2026; dichiarazione di un portavoce della Commissione europea, Bruxelles, 30 luglio 2026.

[17] Camera dei deputati – Senato della Repubblica, *Atti del Governo sottoposti a parere*, scheda relativa all'Atto n. 418 (assegnazione 26 giugno 2026, termine 25 agosto 2026); Camera dei deputati, Commissioni riunite I (Affari costituzionali) e II (Giustizia), seduta del 30 luglio 2026, in *Bollettino delle Giunte e delle Commissioni parlamentari*, 30 luglio 2026, ove si dà conto (intervento dell'on. Serracchiani) del parere votato nella stessa giornata dalle Commissioni riunite 1ª e 2ª del Senato.

[18] Camera dei deputati, Commissioni riunite I e II, seduta del 30 luglio 2026, parere favorevole con osservazioni sull'Atto del Governo n. 418, in *Bollettino delle Giunte e delle Commissioni parlamentari*, 30 luglio 2026, allegato 1, lett. *e*), *l*) e *v*). Il parere è stato approvato con il voto contrario del gruppo PD; il gruppo M5S ha dichiarato di sostenere soltanto la propria proposta alternativa.

[19] Camera dei deputati, Commissioni riunite I e II, seduta del 30 luglio 2026, intervento del relatore per la I Commissione, on. Paolo Emilio Russo (FI-PPE), in *Bollettino delle Giunte e delle Commissioni parlamentari*, 30 luglio 2026.

[20] Camera dei deputati, Commissioni riunite I e II, parere del 30 luglio 2026 sull'Atto del Governo n. 418, cit., allegato 1, lett. *f*) e *i*).

registrazione ed elaborazione già indicata dal Garante per l'art. 10. Il punto è stato colto trasversalmente, e non soltanto dall'opposizione, e il testo pubblicato lo ha recepito: segno che non si trattava di un rilievo isolato, ma di una criticità strutturale dello schema, riconosciuta dagli stessi soggetti istituzionali chiamati a valutarlo.

Il decreto non si limita alla disciplina amministrativa e processuale dell'identificazione biometrica: introduce anche, sul piano del diritto penale sostanziale, una fattispecie di reato autonoma. L'art. 12 inserisce nel codice penale l'art. 437-*bis*, che punisce con la reclusione da uno a cinque anni chiunque ometta di adottare le misure tecniche di sicurezza previste per la progettazione, l'addestramento, la produzione o l'immissione sul mercato di sistemi di intelligenza artificiale ad alto rischio, idonee a prevenirne malfunzionamenti o alterazioni, ovvero ometta di adottare misure di sorveglianza umana, quando ne derivi pericolo per la vita o per l'incolumità pubblica o individuale; la pena è della reclusione da due a otto anni se dal fatto deriva pericolo per la sicurezza dello Stato. Il secondo comma punisce, salvo che il fatto costituisca più grave reato, chi altera sistemi di IA ad alto rischio. Il terzo prevede la forma colposa, limitata alla colpa grave e ai soli fatti del primo comma, con pena ridotta da un terzo a un sesto. Il quarto estende le pene del primo comma all'utilizzatore professionale che ometta intenzionalmente di adottare misure di sorveglianza umana[21]. L'art. 15 introduce inoltre nel d.lgs. n. 231/2001 l'art. 25-*vicies*, che include fra i reati presupposto sia l'art. 437-*bis* c.p. sia l'art. 612-*quater* c.p., già introdotto dalla legge delega, e vi aggiunge le sanzioni interdittive: la responsabilità dell'ente si affianca così, in questa materia, a quella della persona fisica[22]. La scelta di configurare fattispecie autonome, anziché rinviare alle norme generali su colpa e dolo, risponde a un modello già sperimentato in materia di infortuni sul lavoro, e postula in capo al giudice una valutazione discrezionale sull'idoneità preventiva delle misure tecniche omesse, da riferire a eventi-tipo di alterazione o malfunzionamento piuttosto che alla singola occorrenza concreta[23].

Non sono mancate, nella fase di esame parlamentare, critiche di segno opposto a quelle qui esposte, provenienti dal versante delle garanzie individuali. Un'organizzazione non governativa attiva sui temi della giustizia penale ha chiesto, in sede di audizione, che il nuovo reato di cui all'art. 437-*bis* definisse con maggiore chiarezza le condotte tipiche riferibili a ciascun soggetto della catena – dai progettisti fino ai vertici delle forze di polizia – per evitare che la responsabilità penale ricada soltanto sugli operatori di livello più basso; la stessa organizzazione ha inoltre segnalato un errore di coordinamento testuale: nello schema l'art. 8, c. 1, indicava come introdotto «dall'articolo 14 del presente decreto» l'art. 359-*ter* c.p.p., che è invece introdotto dall'art. 13. Il testo pubblicato ha corretto il rinvio[24]. L'episodio è minore, ma non irrilevante per un decreto che affida alla precisione dei rinvii interni la tenuta del sistema delle tre autorizzazioni distinte, e mostra in piccolo la stessa dinamica che si osserva per i rilievi di maggior peso: la correzione del testo a valle di un rilievo esterno formulato in corso di procedimento.

Il Consiglio dei ministri ha approvato in via definitiva il decreto nella seduta del 4 agosto 2026[25], e il raffronto con lo schema consente di verificare quali rilievi abbiano trovato accoglimento. Ne hanno trovato tre. L'art. 10, c. 4, accoglie la soluzione indicata dal Garante:

[21] D.lgs. n. 160/2026, art. 12, che introduce l'art. 437-*bis* c.p. Il secondo comma punisce l'alterazione con la reclusione da due a sei anni, ovvero da tre a dieci anni se ne deriva pericolo per la sicurezza dello Stato.

[22] D.lgs. n. 160/2026, art. 15, che introduce l'art. 25-*vicies* nel d.lgs. n. 231/2001: sanzione pecuniaria da seicento a mille quote per il delitto di cui all'art. 437-*bis* c.p. e da duecento a settecento quote per quello di cui all'art. 612-*quater* c.p., oltre alle sanzioni interdittive dell'art. 9, c. 2, lett. *b*), *c*), *d*) ed *e*).

[23] *AI, è reato l'omessa adozione di misure di sicurezza*, in *Il Sole 24 Ore*, giugno 2026.

[24] Antigone, *IA e Forze di Polizia. Antigone boccia il decreto governativo*, luglio 2026; d.lgs. n. 160/2026, art. 8, c. 1.

[25] Presidenza del Consiglio dei ministri, comunicato stampa n. 185 del 4 agosto 2026.

le immagini del volto delle persone che accedono ai luoghi o agli eventi a rischio sono trattate e memorizzate localmente «senza elaborazione dei relativi dati biometrici», e l'elaborazione biometrica è attivata solo «successivamente alla commissione di un fatto di reato». L'art. 10, c. 10, recepisce il richiamo espresso alle garanzie e ai limiti dell'art. 8 del d.lgs. n. 51/2018, chiesto dal medesimo Garante. L'art. 8, c. 3, e l'art. 359-*ter*, c. 3, c.p.p. accolgono l'osservazione parlamentare sulla non incrementalità: la banca dati di confronto è «formata appositamente per ciascun utilizzo» e i dati sono cancellati alla scadenza dell'autorizzazione, «in modo da garantire che il *set* di confronto sia specifico per ciascuna autorizzazione e non sia suscettibile di alimentazione incrementale rispetto alle autorizzazioni pregresse»[26]. Non ha trovato accoglimento, invece, la richiesta della Camera di affidare al giudice anche l'autorizzazione prevista dall'art. 8, che resta al Procuratore della Repubblica. Il punto non è di mera opportunità. L'art. 5, par. 3, del regolamento (UE) 2024/1689 richiede che l'autorizzazione promani da un'autorità giudiziaria o da un'autorità amministrativa indipendente la cui decisione sia vincolante, e la Corte di giustizia ha escluso che il pubblico ministero che dirige le indagini e sostiene l'accusa possieda la terzietà necessaria per autorizzare l'accesso a dati di traffico e di ubicazione[27]. La trasposizione di quel principio al canale dell'art. 8 non è automatica: l'autorizzazione vi è resa a fini di prevenzione, al di fuori di un procedimento penale nel quale il Procuratore sia parte, e l'appartenenza del pubblico ministero all'ordine giudiziario distingue l'assetto italiano da quello esaminato dalla Corte. Resta però che il canale preventivo è quello nel quale il soggetto autorizzante è più prossimo all'apparato che impiega la tecnologia, e che la richiesta della Camera, respinta in sede di approvazione definitiva, avrebbe sciolto alla radice il dubbio di compatibilità.

La disciplina si inserisce in un quadro previgente segnato da una moratoria di più lunga durata di quanto il solo dato letterale della sua origine potrebbe suggerire: introdotta dall'art. 9, c. 9, del d.l. n. 139/2021, conv. l.n. 205/2021, per i sistemi di riconoscimento facciale mediante dati biometrici installati in luoghi pubblici o aperti al pubblico, essa è stata dapprima prorogata al 31 dicembre 2025 dall'art. 8-*ter* del d.l. n. 51/2023, conv. l.n. 87/2023, e poi ulteriormente estesa al 31 dicembre 2027 in sede di conversione del decreto Milleproroghe 2026[28]. Il d.lgs. n. 160/2026, in vigore dal 30 settembre 2026, deve ora coordinarsi con questo termine, che resta più esteso della delega stessa.

Due rilievi critici restano, invece, anche a fronte del testo pubblicato. Il primo attiene alla clausola di salvezza dell'art. 8, c. 8. La disposizione sanziona l'impiego non autorizzato imponendo l'immediata interruzione del sistema e la cancellazione di tutti i dati personali, dei risultati e degli *output*, ma fa salvi «gli elementi acquisiti legittimamente sotto altra base giuridica conforme al decreto legislativo n. 51 del 2018». Rispetto allo schema, il testo pubblicato ancora la clausola alla disciplina del trattamento dei dati per finalità di polizia, e risponde così in parte al rilievo del Garante, che ne aveva chiesto la tipizzazione normativa; non individua però il titolo alternativo, né affida l'accertamento della sua sussistenza a un soggetto diverso dall'amministrazione procedente[29]. Il secondo riguarda il reimpiego dei dati.

[26] D.lgs. n. 160/2026, art. 10, cc. 4 e 10; art. 8, c. 3; art. 13, che introduce l'art. 359-*ter* c.p.p., c. 3. Le formule riportate sono quelle del testo pubblicato in G.U.; sull'art. 8 del d.lgs. n. 51/2018, v. anche il parere del Garante cit. (v. *supra*, § 2, nota 15).

[27] Corte Giust., sent. 2 marzo 2021, causa C-746/18, *H.K. c. Prokuratuur*; sulle garanzie del pubblico ministero nell'ordinamento italiano, artt. 104 e 107, c. 4, Cost.

[28] D.l. n. 139/2021, conv. l.n. 205/2021, art. 9, c. 9; d.l. n. 51/2023, conv. l.n. 87/2023, art. 8-*ter*; l. di conversione del d.l. Milleproroghe 2026, in G.U. 28 febbraio 2026.

[29] L'art. 8, c. 8, del d.lgs. n. 160/2026 dispone che, ove non siano osservate le condizioni e i termini di cui ai commi da 4 a 7 ovvero in caso di mancata autorizzazione, «l'uso del sistema di intelligenza artificiale oggetto dell'autorizzazione è immediatamente interrotto e tutti i dati personali, i risultati e gli *output* acquisiti e prodotti sono cancellati, fatti salvi gli elementi acquisiti legittimamente sotto altra base giuridica conforme al decreto

Issn 2421-0528

L'art. 7, c. 1, lett. *d*), impone al titolare del trattamento, per l'etichettatura, il filtraggio e la categorizzazione di dati biometrici, misure idonee a prevenire «il reimpiego dei dati e dei risultati per finalità incompatibili con quelle per cui sono stati raccolti»; un obbligo corrispondente non compare negli artt. 8 e 10, che disciplinano operazioni più intrusive. La cancellazione del *set* di confronto alla scadenza dell'autorizzazione, introdotta dall'art. 8, c. 3, riduce ma non elimina l'asimmetria, perché presidia l'archivio di riferimento e non i risultati dell'identificazione.

3. L'ordinamento francese. La sperimentazione francese della videosorveglianza algoritmica nasce con un tratto che la distingue nettamente dagli altri due ordinamenti esaminati: l'esclusione espressa, fin dall'origine, di ogni trattamento biometrico. L'art. 10 della *loi* n. 2023-380 del 19 maggio 2023 ha autorizzato, a titolo sperimentale e in vista dei Giochi olimpici e paralimpici del 2024, l'impiego di sistemi di videosorveglianza algoritmica capaci

legislativo n. 51 del 2018», soggiungendo che «i risultati forniti dai sistemi di intelligenza artificiale in violazione delle disposizioni del presente articolo non possono essere utilizzati». Nello schema trasmesso alle Camere mancava il riferimento al d.lgs. n. 51/2018. La struttura del comma merita attenzione, perché la deroga non investe entrambi i periodi: l'inutilizzabilità sancita dal secondo è formulata senza eccezioni, mentre la clausola di salvezza incide sul solo obbligo di cancellazione previsto dal primo. Ne discende che elementi acquisiti in violazione delle condizioni autorizzatorie, pur restando processualmente inutilizzabili, possono nondimeno essere conservati ove l'amministrazione invochi una diversa base giuridica, che il testo pubblicato riconduce al d.lgs. n. 51/2018 ma non individua né tipizza. È esattamente il rilievo mosso dal Garante nel parere n. 531 del 14 luglio 2026, che ha giudicato eccessivamente ampia la deroga, vi ha ravvisato un sostanziale depotenziamento delle tutele già assicurate dal d.lgs. n. 51/2018, e ha chiesto di tipizzarne normativamente i presupposti, assicurando la cancellazione effettiva ove questi non ricorrano. L'integrazione apportata in sede di approvazione definitiva risponde al rilievo solo in parte: il richiamo al d.lgs. n. 51/2018 delimita l'ambito dei titoli invocabili, ma non li tipizza, né prevede che la loro sussistenza sia accertata da un soggetto diverso dall'amministrazione procedente. Il rilievo può essere precisato sul piano dogmatico. Perché la clausola non si risolva in un'autovalutazione dell'amministrazione procedente sulla legittimità della propria conservazione, occorrerebbe che la sussistenza della «altra base giuridica» fosse accertata dallo stesso organo giurisdizionale cui il decreto affida l'autorizzazione – il giudice per le indagini preliminari, nel canale dell'art. 13 – con un provvedimento autonomo e motivato, anziché essere rimessa alla valutazione interna della polizia procedente. Il modello di riferimento è quello dell'art. 191 c.p.p., ove l'inutilizzabilità è rilevabile d'ufficio in ogni stato e grado e la sua estensione agli elementi derivati è oggetto di accertamento giudiziale, non amministrativo. A ciò si aggiunge il vincolo eurounitario: l'art. 10 della direttiva (UE) 2016/680 subordina il trattamento dei dati biometrici alla stretta necessità, oltre che a garanzie adeguate e a una base normativa espressa, e l'art. 4, par. 2, della medesima direttiva assoggetta il trattamento ulteriore per finalità diverse alla verifica della sua necessità e proporzionalità; nella lettura che ne ha dato la Corte di giustizia, l'art. 10 osta a una normativa nazionale che preveda la raccolta sistematica di dati biometrici senza imporre all'autorità competente di verificare, e di dimostrare, che essa sia strettamente necessaria al conseguimento delle finalità specifiche perseguite; si tratta di una verifica che spetta all'autorità stessa e che il giudice successivamente adito non può surrogare (Corte Giust., sent. 26 gennaio 2023, causa C-205/21, *Ministerstvo na vatreshnite raboti*; Corte Giust., sent. 28 novembre 2024, causa C-80/23). Una clausola che consenta la conservazione sulla base di un titolo non tipizzato, senza convalida giurisdizionale né verifica di stretta necessità, si colloca in tensione con entrambi i parametri. Nella direzione opposta, e in senso restrittivo, opera invece il successivo c. 9, che estende all'impiego preventivo dei sistemi biometrici il regime dell'art. 226, c. 5, del d.lgs. n. 271/1989, dettato per le intercettazioni preventive e caratterizzato dall'inutilizzabilità processuale dei risultati. A quanto precede si aggiunge un'asimmetria interna al Capo III che pare sfuggita al dibattito: l'art. 7, c. 1, lett. *d*), impone al titolare del trattamento, per le attività di etichettatura, filtraggio e categorizzazione di dati biometrici, di adottare «misure idonee a prevenire il reimpiego dei dati e dei risultati per finalità incompatibili con quelle per cui sono stati raccolti»; un obbligo di contenuto corrispondente non compare né nell'art. 8 né nell'art. 10, che disciplinano operazioni di intrusività manifestamente superiore. La cancellazione del *set* di confronto alla scadenza dell'autorizzazione, prevista dal testo pubblicato all'art. 8, c. 3, attenua l'asimmetria quanto all'archivio di riferimento, non quanto ai risultati. Il presidio positivo contro la ri-finalizzazione è dunque previsto per l'operazione meno invasiva del Capo e omesso per le due più invasive, senza che la relazione illustrativa offra ragione della differenza. Il rilievo, formulato sullo schema, è stato riscontrato sul testo pubblicato in G.U. n. 214 del 15 settembre 2026.

di rilevare eventi predeterminati a partire da immagini captate da dispositivi già installati – ma ha escluso in termini non equivoci qualsiasi utilizzazione di un sistema di identificazione biometrica, sia in tempo reale sia a posteriori[30]. Il legislatore francese ha così tenuto fuori dal proprio perimetro sperimentale l'oggetto specifico di questo lavoro, regolando un fenomeno adiacente – la rilevazione comportamentale, non l'identificazione della persona.
Il termine della sperimentazione, fissato al 31 marzo 2025, è stato oggetto di un primo, fallito tentativo di proroga per via di emendamento a una proposta di legge sul rafforzamento della sicurezza nei trasporti: il Conseil constitutionnel, con la décision n. 2025-878 DC del 24 aprile 2025, ne ha dichiarato l'illegittimità non nel merito, ma per violazione dell'art. 45, c. 1, della Costituzione, qualificandolo *cavalier législatif* – disposizione priva di legame anche indiretto con il testo cui era stata innestata[31]. La proroga è stata poi validamente reiterata nella *loi* relativa all'organizzazione dei Giochi olimpici e paralimpici invernali del 2030, dichiarata conforme a Costituzione dalla décision n. 2026-902 DC del 19 marzo 2026: qui va segnalata una precisazione che il solo dato letterale delle fonti secondarie può indurre a confondere, l'estensione della sperimentazione corre fino al 31 dicembre 2027, mentre il 30 settembre 2027 è il termine, distinto e anteriore, fissato per il deposito della relazione di valutazione[32]. Quella relazione, per il periodo già trascorso, è stata resa dal comitato presieduto da Christian Vigouroux il 24 gennaio 2025, con un esito che la stampa giuridica ha correttamente descritto come un *bilan contrasté*: non una bocciatura dello strumento, ma il riconoscimento che le condizioni ristrette della sperimentazione non ne hanno consentito una valutazione conclusiva quanto alla reale utilità operativa[33]. Sul fronte giurisdizionale, il TA di Grenoble ha annullato, con sentenza del 24 gennaio 2025, la decisione con cui il comune di Moirans aveva disposto l'impiego del *software* Briefcam per assenza di una finalità determinata e di garanzie sufficienti[34] – un precedente che riguarda l'iniziativa di un ente locale e che va tenuto distinto dalle rivelazioni giornalistiche del 2023 sull'uso dello stesso *software* da parte della *police nationale*, appartenenti a un piano diverso della vicenda francese.
Il modello che se ne ricava è un modello di qualificazione giuridica come strumento di politica del diritto: la sperimentazione a termine, per sua natura provvisoria e valutabile, resta sottoposta a un controllo di costituzionalità che colpisce non il contenuto della proroga, ma il veicolo normativo prescelto per introdurla – un controllo, dunque, sulla procedura con cui l'esecutivo ottiene l'estensione dei propri poteri, più che sul merito dell'estensione stessa.

4. L'ordinamento spagnolo. Il passaggio dall'ordinamento francese a quello spagnolo va compiuto tenendo presente un'ambivalenza che l'apparente somiglianza dei due esiti tende a occultare. In entrambi manca, allo stato, un procedimento nazionale autonomo di

[30] *Loi n. 2023-380 du 19 mai 2023 relative aux Jeux olympiques et paralympiques de 2024 et portant diverses autres dispositions*, art. 10.
[31] Cons. const., décision n. 2025-878 DC du 24 avril 2025; *loi n. 2025-379 du 28 avril 2025 relative au renforcement de la sûreté dans les transports*, art. 15.
[32] Cons. const., décision n. 2026-902 DC du 19 mars 2026; *loi relative à l'organisation des jeux Olympiques et Paralympiques d'hiver de 2030*, in JORF du 21 mars 2026, art. 47.
[33] Comité d'évaluation des traitements algorithmiques d'images légalement collectées au moyen de systèmes de vidéoprotection, *Rapport*, janvier 2025 (président Ch. Vigouroux). Il rapporto è stato consegnato al Ministro dell'interno a metà gennaio 2025 e trasmesso al Parlamento e alla CNIL il 24 gennaio 2025; la pubblicazione da parte del Ministero è intervenuta il 7 febbraio successivo.
[34] TA Grenoble, 24 janvier 2025, n. 2105328, Le Querrec e La Quadrature du Net c. Commune de Moirans, con intervento della Ligue des droits de l'Homme, del Syndicat de la magistrature e del Syndicat des avocats de France. La coincidenza della data con quella di trasmissione al Parlamento della relazione del comitato di valutazione (v. *supra*, nota precedente) è fortuita e riguarda atti di natura diversa: la sentenza è stata deliberata all'udienza del 20 dicembre 2024 e resa pubblica mediante deposito in cancelleria il 24 gennaio 2025.

Issn 2421-0528

autorizzazione dell'identificazione biometrica remota; ma le due lacune hanno segno opposto. In Francia si tratta di un limite materiale, deliberatamente posto dal legislatore, che ha escluso la biometria dal perimetro della sperimentazione e non ha dunque alcun procedimento da disciplinare. In Spagna si tratta invece dell'esito di una destrutturazione successiva, che ha ritirato un procedimento già scritto per rinviare alla sola fonte europea, presupponendo l'esercizio della facoltà derogatoria senza governarne le modalità interne. La medesima lacuna testuale segnala, nei due casi, l'una il massimo e l'altra il minimo di autolimitazione del legislatore nazionale. Ciò posto, la scelta spagnola si segnala anzitutto per il rango della fonte: l'adeguamento al regolamento (UE) 2024/1689 procede per legge organica, ai sensi dell'art. 81 della Costituzione, in quanto la disciplina incide su diritti fondamentali – fra cui, per quanto qui rileva, la libertà personale e la protezione dei dati[35]. È una qualificazione che vale come dichiarazione di rango del bene giuridico ancor prima che come opzione procedurale, e che consente un primo confronto diretto con la delega legislativa ordinaria italiana.

Il confronto fra il testo originario e quello attualmente all'esame delle Cortes rivela però una destrutturazione che merita di essere segnalata con precisione, perché incide proprio sul profilo di garanzia che ci si attenderebbe da una legge organica. L'*anteproyecto*, approvato dal Consiglio dei ministri l'11 marzo 2025, prevedeva un Capitolo III interamente dedicato al procedimento di autorizzazione dell'identificazione biometrica remota, che attribuiva ai *juzgados de lo contencioso-administrativo* la competenza a concederla[36]. Il *proyecto* definitivo, trasmesso al Congresso il 12 giugno 2026, ha eliminato quel capitolo: gli obblighi in materia di biometria sono confluiti, senza sviluppo procedurale autonomo, nel catalogo generale delle infrazioni gravi dell'art. 21.3, che si limita a rinviare all'art. 5.3 del regolamento europeo[37]. La conseguenza è che il testo attualmente in discussione non individua più l'ordine giurisdizionale competente: non per una lacuna involontaria, ma per l'effetto di una scelta di *drafting* che ha preferito il rinvio secco alla fonte europea alla costruzione di un procedimento nazionale autonomo. È un dato da trattare, nell'economia del presente lavoro, come acquisito e non come questione ancora aperta: la variabile «natura del terzo autorizzante», per la Spagna, è essa stessa indeterminata, e l'indeterminazione è il risultato, non un difetto di reperimento della fonte.

A compensare, almeno in parte, questa destrutturazione procedurale interviene un'architettura di vigilanza multi-autorità di notevole ampiezza, il cui funzionamento merita una descrizione più analitica di quella offerta finora. L'Agencia Española de Supervisión de la Inteligencia Artificial (AESIA), con sede in A Coruña, è chiamata a operare come autorità principale di vigilanza del mercato, punto di contatto unico verso la Commissione europea e gestore dello spazio controllato di prova (*sandbox*) che il regolamento europeo impone a ciascuno Stato membro di istituire; la Dirección General de Inteligencia Artificial, incardinata nella Secretaría de Estado de Digitalización e Inteligencia Artificial, assume invece il ruolo di autorità notificante per i sistemi elencati nell'Allegato III del regolamento[38]. L'Agencia Española de Protección de Datos (AEPD) mantiene competenza specifica su biometria, identificazione, categorizzazione biometrica, migrazione, asilo e controllo di frontiera; il Consejo General del Poder Judicial (CGPJ) vigila sui sistemi destinati all'amministrazione

[35] Constitución Española, art. 81.

[36] *Anteproyecto de Ley para el Buen Uso y la Gobernanza de la Inteligencia Artificial*, aprobado por el Consejo de Ministros el 11 de marzo de 2025, cap. III, art. 11.

[37] *Proyecto de Ley Orgánica para el buen uso y la gobernanza de la inteligencia artificial*, BOCG, Congreso de los Diputados, XV Legislatura, Serie A, núm. 97-1, de 12 de junio de 2026 (expediente 121/000096), art. 21.3, lett. *a*)-*f*).

[38] Congreso de los Diputados, *Proyecto de Ley Orgánica*, art. 5; Ministerio para la Transformación Digital y de la Función Pública, comunicato del 26 maggio 2026 sull'approvazione del *proyecto*.

della giustizia; la Banca di Spagna e la CNMV intervengono, rispettivamente, sui sistemi impiegati per la valutazione del merito creditizio e della solvibilità[39].

Questa architettura presenta però un'asimmetria interna che il presente lavoro ritiene di segnalare, perché tocca direttamente la terza invariante che si isolerà *infra*, § 5 – l'esistenza di un'autorità indipendente di vigilanza. L'AEPD è autorità indipendente per obbligo di fonte sovraordinata, discendente dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea e dall'art. 52 della legge organica spagnola sulla protezione dei dati; l'AESIA, che pure riveste il ruolo di autorità di riferimento e punto di contatto unico per l'intera disciplina, non gode del medesimo statuto, essendo incardinata – «*adscrita*», secondo la formula impiegata dal testo – in un ministero[40]. Ne risulta un'architettura a doppio statuto: indipendente l'autorità competente specificamente per la biometria (l'AEPD), non indipendente l'autorità generale cui la legge affida il coordinamento dell'intero sistema. È un'ambiguità che il solo elenco delle competenze, quale offerto in dottrina secondaria, non rende visibile, e che diventa invece rilevante non appena si chieda, come fa questo lavoro, se il controllo sull'osservanza della disciplina sia realmente esterno alla catena di comando dell'esecutivo o vi resti, in parte, interno.

Il regime sanzionatorio, per completare il quadro, ripartisce le infrazioni in lievi, gravi e molto gravi, con sanzioni pecuniarie che, per le violazioni più gravi, possono raggiungere i trentacinque milioni di euro o il sette per cento del fatturato dell'impresa responsabile[41]: un livello sanzionatorio comparabile, nell'ordine di grandezza, a quello previsto dal regolamento europeo stesso, e che colloca la Spagna fra gli ordinamenti che hanno scelto di replicare a livello nazionale la severità del regime sanzionatorio unionale, piuttosto che ridurla in sede di trasposizione.

La tesi che se ne trae, e che anticipa il passaggio induttivo del paragrafo successivo, è che la scelta della fonte – legge organica – resta una qualificazione del bene giuridico giuridicamente significativa anche a fronte della destrutturazione procedurale: la garanzia non scompare, ma si sposta dal procedimento nazionale specifico, che l'*anteproyecto* delineava e il *proyecto* ha ritirato, al rinvio diretto alla disciplina europea, la cui applicazione resta però affidata a un'architettura di controllo interno frammentata fra cinque autorità distinte, e non uniformemente indipendente al proprio interno.

5. Il modello europeo per induzione. I tre ordinamenti esaminati condividono quattro invarianti, quando si assuma come *tertium comparationis* non il contenuto delle garanzie ma la struttura del controllo. La prima invariante è una riserva di legge, sia pure di rango diverso: delega legislativa ordinaria in Italia[42], legge sperimentale a termine in Francia[43], legge organica in Spagna[44]. In nessuno dei tre casi l'esecutivo dispone di una fonte regolamentare autonoma per introdurre l'identificazione biometrica remota nel proprio armamentario; ma il rango della riserva non è uniforme, ed è proprio nella misura di questa differenza – delega ordinaria, sperimentazione a termine, legge organica – che si misura quanto ciascun ordinamento consideri la materia sottratta alla libera disponibilità del legislatore ordinario.

---

[39] BOCG, Serie A, núm. 97-1, art. 5, §§ 2-9.

[40] Il rilievo, con riferimento all'art. 16 del Trattato sul funzionamento dell'Unione europea, all'art. 8 della Carta dei diritti fondamentali dell'Unione europea e all'art. 52 della *Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales*, è sviluppato in LAW21, *Gobernanza de la IA en España: autoridades competentes, régimen sancionador y los límites de legislar sobre un reglamento directamente aplicable*, giugno 2026.

[41] *Supervisión humana, protección de derechos y nuevas garantías frente a los riesgos de la IA*, in *Infocop*, giugno 2026.

[42] L.n. 132/2025, art. 24, c. 2, lett. *h)* (v. *supra*, § 2, nota 10).

[43] *Loi* n. 2023-380 du 19 mai 2023, art. 10 (v. *supra*, § 3, nota 30).

[44] Constitución Española, art. 81 (v. *supra*, § 4, nota 35).

La seconda invariante è l'autorizzazione preventiva di un soggetto terzo rispetto a chi impiega la tecnologia, quando l'identificazione in tempo reale è comunque ammessa: il Procuratore della Repubblica o, a seconda della finalità, il giudice per le indagini preliminari in Italia, cui il testo pubblicato ha affidato anche la ricerca mirata a posteriori[45]; nessun terzo in Francia, per la semplice ragione che il legislatore ha escluso la biometria dal proprio perimetro sperimentale anziché disciplinarne l'autorizzazione[46]; un terzo non più identificato nel testo, ma presupposto dal rinvio alla disciplina europea, in Spagna[47]. Anche qui l'apparente uniformità nasconde una differenza di grado: l'Italia è l'unico dei tre ordinamenti che disciplina compiutamente due canali autorizzatori distinti per la stessa operazione tecnica, a seconda della finalità perseguita, e proprio questa duplicazione – si è visto *supra*, § 2 – è stata oggetto di una specifica richiesta parlamentare di unificazione verso l'alto, nel senso di sottoporre entrambi i canali all'autorizzazione del giudice anziché del pubblico ministero. La richiesta, del resto, non era soltanto di opportunità: è nel canale preventivo, affidato al Procuratore, che la terzietà dell'autorizzante risulta meno certa alla luce dell'art. 5, par. 3, del regolamento (*supra*, § 2).

La terza invariante è un'autorità indipendente di vigilanza dotata del potere di incidere sul procedimento normativo prima della sua conclusione, non soltanto *ex post*: il Garante per la protezione dei dati personali in Italia, il cui parere ha modificato la struttura dell'art. 10 prima dell'approvazione definitiva, come documenta il raffronto fra lo schema e il testo pubblicato (art. 10, cc. 4 e 10)[48]; il comitato di valutazione presieduto da Vigouroux in Francia, la cui relazione condiziona la sorte della proroga sperimentale[49]; l'architettura multi-autorità spagnola, frammentata fra AESIA, AEPD, CGPJ, Banca di Spagna e CNMV[50]. È qui che il caso spagnolo introduce, però, la complicazione più istruttiva dell'intero quadro comparato: si è visto *supra*, § 4, che l'autorità di riferimento generale, l'AESIA, non è indipendente nel senso tecnico dell'espressione, essendo incardinata in un ministero, mentre lo è l'AEPD, competente sulla sola biometria. La terza invariante, dunque, non richiede che *ogni* autorità coinvolta nella vigilanza sia indipendente, ma che lo sia *almeno quella* la cui competenza include la materia specifica dell'identificazione biometrica: un requisito che la Spagna soddisfa, sia pure per il tramite di un'autorità – l'AEPD – la cui competenza generale sulla protezione dei dati precede e trascende la disciplina sull'intelligenza artificiale, piuttosto che esserne un prodotto.

Occorre però riconoscere che la terza invariante, così formulata, è documentata con pienezza soltanto per l'Italia, dove il parere del Garante ha inciso sul testo prima della sua adozione. Il comitato francese valuta una sperimentazione già in corso e ne condiziona la proroga, non la prima adozione; per la Spagna, il *proyecto* è ancora all'esame delle Cortes e un intervento dell'AEPD sul testo non è, allo stato, documentabile. Il dato che consente di non ridurre la terza invariante a una contingenza della vicenda italiana è di diritto positivo dell'Unione: l'art. 28, par. 2, della direttiva (UE) 2016/680 impone agli Stati membri di prevedere la consultazione dell'autorità di controllo durante l'elaborazione di ogni proposta di misura legislativa relativa ai trattamenti a fini di polizia, e l'art. 36, par. 4, del regolamento (UE) 2016/679 dispone altrettanto per i trattamenti da esso disciplinati[51]. Il parere del Garante

[45] D.lgs. n. 160/2026, artt. 8, 10 e 13 (v. *supra*, § 2, note 12-14).
[46] V. *supra*, § 3, nota 30.
[47] V. *supra*, § 4, nota 37.
[48] Garante per la protezione dei dati personali, provv. n. 531 del 14 luglio 2026 (v. *supra*, § 2, nota 15); d.lgs. n. 160/2026, art. 10, cc. 4 e 10.
[49] Comité d'évaluation, *Rapport*, cit. (v. *supra*, § 3, nota 33).
[50] BOCG, Serie A, núm. 97-1, art. 5, §§ 2-9 (v. *supra*, § 4, nota 39).
[51] Dir. UE 2016/680, art. 28, par. 2; reg. UE 2016/679, art. 36, par. 4.

sull'Atto del Governo n. 418 non è dunque un accidente procedurale, ma l'esercizio di una funzione che il diritto dell'Unione impone in termini identici ai tre ordinamenti: l'anticipazione del controllo è un tratto del pavimento comune, e la vicenda italiana ne è la manifestazione meglio documentata, non l'unica possibile.

La quarta invariante è il sindacato giurisdizionale sull'atto che dispone o autorizza l'identificazione, esercitato per ora, nei tre ordinamenti, più sul veicolo normativo e sulla sua legittimità procedurale che sul merito della singola autorizzazione – la sentenza del Conseil constitutionnel sul *cavalier législatif* ne è l'esempio più netto[52]. In Italia il sindacato è assicurato, sul canale investigativo, dalla stessa struttura dell'autorizzazione giudiziale e, sugli esiti, dall'inutilizzabilità dei risultati acquisiti in violazione dell'art. 8 del d.lgs. n. 160/2026; in Spagna, in assenza di un procedimento nazionale, resta affidato ai rimedi generali contro gli atti dell'amministrazione. È, fra le quattro, l'invariante meno sviluppata, e conviene dichiararlo. Le variabili che distinguono i tre ordinamenti fra loro sono altrettanto significative: il rango della fonte; la natura del terzo autorizzante, che in Spagna cessa di essere una variabile determinata per diventare essa stessa oggetto di uno scarto; e l'ampiezza della deroga che ciascun ordinamento si è concesso, massima in Italia, che ammette l'identificazione in tempo reale su due canali distinti, nulla in Francia, che la esclude in radice dal proprio perimetro sperimentale, intermedia in Spagna, dove la deroga sussiste ma il suo esercizio concreto è rinviato al regolamento europeo.

È a questo punto che la corroborazione tedesca acquista rilievo, non come quarto ordinamento da ricostruire per esteso, ma come prova di tenuta delle quattro invarianti fuori dal loro contesto di origine. La Germania non appartiene alla sottofamiglia romanistica di Italia, Francia e Spagna, e il vincolo che vi limita l'esecutivo non proviene da nessuna delle quattro fonti appena censite. Non da una riserva di legge specifica sulla biometria, che manca; non da un'autorizzazione preventiva legislativamente strutturata; non da un'autorità indipendente che incida sul procedimento normativo, giacché per l'identificazione biometrica remota non vi è un procedimento normativo da correggere. Il vincolo proviene dalla giurisprudenza costituzionale sull'autodeterminazione informativa, che il Bundesverfassungsgericht ha applicato all'analisi automatizzata di dati di polizia in generale e che la prassi amministrativa sconta anche in assenza di una legge federale sulla biometria[53]. Il limite opera, va precisato, sul tempo reale: l'identificazione a posteriori è da tempo in uso presso il Bundeskriminalamt, e proprio su di essa si è registrato l'episodio che meglio documenta l'esteriorità del controllo. Dopo il vertice del G20 di Amburgo del 2017 la polizia cittadina costituì, a partire dalle immagini raccolte, una banca dati biometrica per l'identificazione a posteriori dei partecipanti ai disordini; il 18 dicembre 2018 il Commissario amburghese per la protezione dei dati ne ordinò la cancellazione, e il provvedimento fu annullato dal Tribunale amministrativo di Amburgo con sentenza del 23 ottobre 2019[54]. Quale che sia il giudizio sull'esito, la sequenza – un'autorità indipendente che interviene sull'operato della polizia, un giudice che ne sindaca l'intervento – è quella che il modello qui

[52] Cons. const., décision n. 2025-878 DC du 24 avril 2025 (v. *supra*, § 3, nota 31).

[53] BVerfG, *Urteil des Ersten Senats* del 16 febbraio 2023, 1 BvR 1547/19 e 1 BvR 2634/20 (v. *supra*, § 1, nota 9).

[54] Il sistema di riconoscimento facciale del Bundeskriminalamt (*Gesichtserkennungssystem*, GES) è in uso dal 2008 per l'identificazione di autori ignoti di reati, mediante confronto con le immagini segnaletiche registrate nel sistema informativo della polizia (INPOL). Sulla vicenda amburghese, Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit, *Anordnung* del 18 dicembre 2018, che disponeva la cancellazione della banca dati di riferimento costituita dalla *Sonderkommission* «Schwarzer Block» per le indagini sul G20; VG Hamburg, sent. 23 ottobre 2019, 17 K 203/19, che ha annullato l'ordine. Secondo il Tribunale, il Commissario non aveva accertato una violazione concreta nel trattamento in atto, il § 48 BDSG offriva una base giuridica sufficiente e non spettava all'autorità di controllo sindacare, con un proprio provvedimento, la legittimità costituzionale di una legge federale.

ricostruito descrive. La corroborazione tedesca, dunque, non riguarda le quattro invarianti come tali, nessuna delle quali si ritrova nella forma assunta negli ordinamenti esaminati, ma il tratto che le accomuna: la collocazione del vincolo all'esterno della catena di comando che impiega la tecnologia. Se questo tratto persiste anche dove la fonte del vincolo muta così radicalmente – da riserva di legge a precedente costituzionale, da autorizzazione legislativa a effetto dissuasivo di uno standard giurisprudenziale – esso non è un prodotto della sottofamiglia giuridica di appartenenza, ma qualcosa di più strutturale, che il confronto con un termine esterno alla famiglia romanistica permetterà ora di isolare con maggiore precisione.

6. Il termine intermedio di confronto: gli Stati Uniti d'America. Prima di procedere al confronto con l'ordinamento cinese conviene introdurre un termine intermedio, che la comparazione europea da sola non consente di isolare. Gli Stati Uniti presentano infatti una separazione strutturale piena – le corti sono indipendenti dall'esecutivo in una misura che nessuna autorità amministrativa europea può vantare – e nondimeno un livello di tutela che, sul terreno qui esaminato, risulta in più punti inferiore a quello europeo. È precisamente questa combinazione a rendere l'esperienza americana utile: essa consente di verificare se la separazione, isolata dalle altre due variabili che si sono viste operare in Europa, basti da sola a qualificare il modello.

Due luoghi comuni vanno preliminarmente rimossi. Il primo è che il Quarto Emendamento costituisca il presidio operativo in materia. Il criterio della *reasonable expectation of privacy* incorpora un limite che incide direttamente sul riconoscimento facciale, poiché quanto una persona espone consapevolmente al pubblico non è protetto, e il volto in strada è il caso paradigmatico dell'esposizione pubblica; la breccia aperta da *Carpenter* per i dati di localizzazione cellulare è stata dalla stessa Corte suprema qualificata come circoscritta[55]. Il secondo luogo comune è che il controllo americano operi esclusivamente *ex post*, nelle aule di giustizia. Anche questo è inesatto, e la sua rimozione è la premessa dell'argomento che segue.

Sul piano federale, per vero, il quadro è di sostanziale assenza: proposte di legge volte a disciplinare l'impiego della tecnologia da parte delle forze dell'ordine sono state presentate in legislature successive senza mai essere approvate[56]. È al livello degli Stati federati che la disciplina esiste, e quattro di essi prevedono forme di autorizzazione preventiva. Lo Stato di Washington, con legge in vigore dal 1° luglio 2021, vieta agli enti statali e locali l'impiego della tecnologia per sorveglianza continuativa, identificazione in tempo reale o quasi reale e tracciamento persistente, salvo che sia ottenuto un mandato giudiziario, ricorrano circostanze di urgenza o un ordine giurisdizionale ne autorizzi l'uso per la ricerca di persone scomparse o l'identificazione di persone decedute; la stessa legge impone ai giudici un obbligo di rendicontazione annuale sui mandati concessi e negati[57].

Il Montana è andato oltre nel 2023, affiancando al requisito del mandato un divieto assoluto di *continuous facial surveillance* – definita in modo da comprendere la scansione in tempo reale di flussi video confrontati con un elenco precostituito – un limite di gravità del reato, l'obbligo di revisione umana significativa e il dovere di informare l'imputato dell'avvenuto

[55] *Carpenter v. United States*, 585 U.S. 296 (2018). Nessuna corte federale ha finora stabilito che l'identificazione biometrica in tempo reale in spazi pubblici integri una *search* ai sensi del Quarto Emendamento.

[56] H.R. 4695, *Facial Recognition Act of 2025*, 119° Congresso, presentata nel luglio 2025; versioni precedenti erano state presentate nel 2022 e nel 2023. Nessuna è stata approvata.

[57] Wash. Rev. Code §§ 43.386.080 e 43.386.090, introdotti da ESSB 6280, Laws of 2020, ch. 257, in vigore dal 1° luglio 2021.

impiego della tecnologia[58]. Lo Utah ha seguito nel 2024, vietando agli enti pubblici di acquisire informazioni di sorveglianza biometrica senza mandato, in aggiunta al limite di gravità del reato già introdotto nel 2021[59]. Il Maine si colloca su un piano in parte diverso: vieta a ogni ente statale, di contea o municipale il possesso e l'uso della tecnologia, salva una eccezione ristretta che consente richieste al *Federal Bureau of Investigation* e all'ufficio statale della motorizzazione in presenza di *probable cause* relativa a un reato grave; stabilisce che la corrispondenza biometrica da sola non integra né *probable cause* né presupposto di arresto o perquisizione; sanziona con l'inammissibilità i dati acquisiti in violazione; e riconosce un'azione a tutela inibitoria e dichiarativa[60]. Va però segnalato che lo standard del Maine è sostanziale e non procedurale: la *probable cause* è valutata dall'ufficiale richiedente e non da un magistrato, sicché il rigore del Maine quanto all'ambito non è accompagnato da una garanzia strutturale equivalente quanto all'autorizzazione.

Quanti siano gli Stati dotati di restrizioni è domanda cui non è possibile rispondere con la precisione che la comparazione richiederebbe, e la ragione di ciò è essa stessa parte dell'argomento. Non esiste un registro federale di tali misure, né un obbligo di comunicazione verso l'alto, né un'autorità incaricata di mantenerne il quadro consolidato. Le rilevazioni disponibili, tutte di fonte privata, divergono fra loro – quindici Stati secondo alcune, prossime alle ventiquattro secondo altre – a seconda che si computino anche le leggi limitate all'impiego congiunto con le videocamere indossate dagli agenti, ovvero quelle relative al solo uso commerciale[61]. L'assenza di un dato aggregato attendibile non è una lacuna della letteratura: è la conseguenza strutturale di un sistema nel quale nulla, al di sopra degli Stati, è incaricato di sapere che cosa gli Stati abbiano fatto.

La Virginia illustra un fenomeno che nessuno degli ordinamenti europei esaminati presenta: l'oscillazione fra divieto e riautorizzazione, e poi fra riautorizzazione e restrizione condizionata. Una legge in vigore dal 1° luglio 2021 aveva introdotto quello che il proponente descrisse come un divieto di fatto, precludendo alla polizia locale e a quella universitaria l'acquisto e l'impiego della tecnologia in assenza di espressa autorizzazione legislativa. Meno di un anno dopo quel divieto è stato sostituito da un quadro autorizzatorio in vigore dal 1° luglio 2022. Un terzo regime è entrato in vigore il 1° luglio 2026. Esso subordina l'uso da parte della polizia locale all'approvazione preventiva della tecnologia da parte della *Division of Purchases and Supply*, che può approvare soltanto sistemi sottoposti al *Face Recognition Vendor Test* del National Institute of Standards and Technology, con almeno il novantotto per cento di veri positivi e una variazione minima delle prestazioni per razza, tono della pelle, etnia e genere. Vieta poi il tracciamento in tempo reale di un individuo identificato in spazi pubblici, la costituzione di una banca dati a partire da un flusso video dal vivo e l'inserimento delle immagini di confronto in archivi commerciali. Impone, infine, un preavviso scritto di trenta giorni all'organo di governo locale prima dell'acquisto, e commina una responsabilità penale di tipo contravvenzionale agli operatori che eccedano gli usi consentiti, con destituzione obbligatoria alla seconda violazione[62].

Una disposizione del regime virginiano del 2026 merita segnalazione autonoma, perché non

[58] Mont. Code Ann. § 44-15-106, introdotto da SB 397, sessione 2023; il divieto di sorveglianza facciale continuativa è contenuto nel medesimo capo.

[59] Utah Code § 77-23d-106, introdotto da SB 231, Laws of Utah 2024, ch. 216; le restrizioni anteriori sono nel capo 77-23e, introdotto da Laws of Utah 2021, ch. 200.

[60] 25 M.R.S. § 6001, introdotto da LD 1585, PL 2021 ch. 394, in vigore dal 1° ottobre 2021.

[61] Le rilevazioni curate da organizzazioni non governative e associazioni di categoria divergono a seconda della classificazione adottata. L'assenza di una fonte consolidata di carattere autoritativo è discussa nel testo.

[62] Va. HB 2031, sessione 2021, in vigore dal 1° luglio 2021; Va. SB 741, promulgata il 27 aprile 2022, in vigore dal 1° luglio 2022; Va. Code § 15.2-1723.2 e § 23.1-815.1, in vigore dal 1° luglio 2026.

ha corrispondente europeo e risolve con eleganza un problema che i testi europei lasciano aperto. La corrispondenza biometrica non può essere inserita nell'atto che fonda la *probable cause* per un mandato di perquisizione o di arresto, ma è ammissibile come prova a discarico[63]. La tecnologia è dunque abilitata a scagionare e inibita a incriminare: un'asimmetria calibrata sul profilo di errore noto di questi sistemi, che il d.lgs. n. 160/2026, il quale affronta solo obliquamente il valore probatorio della corrispondenza, avrebbe potuto utilmente mutuare. Sul piano del contenuto delle garanzie, in altri termini, l'esperienza americana è in taluni punti più avanzata di quella europea. È precisamente per questo che il contenuto non può essere la variabile discriminante.

L'Illinois espone una lacuna di natura diversa, e per la tesi qui sostenuta è la più istruttiva. Il *Biometric Information Privacy Act* è per comune riconoscimento la legge biometrica più esigente degli Stati Uniti, e l'unica che conferisca un'azione privata autonoma: è per questa via che è stata condotta la *litigation* che ha piegato Clearview AI. Eppure la definizione di soggetto obbligato esclude espressamente le agenzie statali e locali e gli organi giudiziari dell'Illinois[64]. Lo strumento più forte del diritto biometrico americano è dunque puramente orizzontale: vincola gli operatori privati e lascia intatta la polizia. La somiglianza strutturale con l'assetto cinese esaminato *infra*, § 7, è esatta, e conviene enunciarla senza mediazioni: un residente dell'Illinois dispone di un rimedio potente contro l'impresa privata che ne scansiona il volto e di nessun rimedio contro il corpo di polizia che compia la medesima operazione.

Il terzo livello è quello municipale, ed è dove il diritto americano si è mostrato più inventivo. San Francisco ha vietato l'uso da parte dell'amministrazione comunale nel maggio 2019, prima grande città statunitense a farlo; Oakland ha seguito nel luglio 2019 e Boston nel giugno 2020; Portland si è spinta oltre nel settembre 2020, vietando l'impiego tanto agli uffici comunali quanto ai soggetti privati nei luoghi aperti al pubblico, con azione risarcitoria a favore dei residenti, e il divieto è tuttora in vigore a cinque anni di distanza[65]. Queste misure sono, alla lettera, più severe di qualunque disposizione vigente in Italia, Francia o Spagna: il divieto di Portland relativo ai privati non ha equivalente europeo, poiché il regolamento (UE) 2024/1689 lascia in larga misura al diritto nazionale l'impiego commerciale in spazi accessibili al pubblico.

Ed è tuttavia al livello municipale che la falla è più visibile. Un'inchiesta giornalistica pubblicata nel maggio 2024 ha accertato che dipartimenti di polizia di città nelle quali il divieto era vigente, fra cui Austin e San Francisco, avevano ottenuto risultati di riconoscimento facciale chiedendo ad agenzie di giurisdizioni limitrofe di eseguire le ricerche per loro conto[66]. Il divieto vincola l'agenzia; non vincola l'agenzia della porta accanto, e nulla al di sopra delle due le coordina. Un divieto adottato a un livello di governo è vanificato dall'assenza di un divieto al livello superiore – che è il medesimo difetto strutturale, espresso nella geografia del federalismo anziché nella cronologia del controllo, che la frammentazione del livello statale produce.

New Orleans ne offre l'illustrazione più netta, e conviene ricostruirla nella sua sequenza. Nel

[63] Va. Code § 15.2-1723.2, lett. C, in vigore dal 1° luglio 2026.

[64] 740 ILCS 14/10, ove si prevede che la nozione di *private entity* non comprende le agenzie statali o locali, né alcuna corte, cancelleria, giudice o magistrato dell'Illinois. Sull'emendamento del 2024 che ha limitato i danni legali a un solo recupero per tipo di violazione, v. SB 2979, in vigore dal 2 agosto 2024.

[65] San Francisco, *Stop Secret Surveillance Ordinance*, maggio 2019; Oakland, luglio 2019; Boston, giugno 2020; Portland (Oregon), ordinanze 190113 e 190114, adottate il 9 settembre 2020, con efficacia del divieto per i privati dal 1° gennaio 2021. Ulteriori divieti municipali sono in vigore, fra le altre, a Springfield (Massachusetts), Jackson (Mississippi) e Pittsburgh (Pennsylvania); Milwaukee ha adottato un divieto di uso da parte della polizia nel febbraio 2026.

[66] Inchiesta del *Washington Post*, maggio 2024; successivi contenziosi hanno lamentato la reiterata elusione del divieto da parte del dipartimento di polizia di San Francisco.

dicembre 2020 il Consiglio comunale vietò all'unanimità il riconoscimento facciale, la polizia predittiva, il tracciamento per caratteristiche e i simulatori di celle telefoniche, a seguito della rivelazione che il dipartimento di polizia aveva avuto accesso alla tecnologia attraverso partner statali e federali dopo anni di smentite. Nel luglio 2022, in un contesto di aumento dei reati violenti, il Consiglio sostituì il divieto con un'ordinanza sulla tecnologia di sorveglianza e la protezione dei dati che consentiva il riconoscimento facciale per le indagini su reati violenti determinati, con revisione umana da parte di esaminatori qualificati presso il centro di analisi statale e obblighi di rendicontazione verso il Consiglio; l'ordinanza manteneva il divieto espresso di impiegare un sistema di sorveglianza facciale per il monitoraggio generalizzato[67].

Dall'inizio del 2023 all'aprile 2025 il dipartimento di polizia ha nondimeno ricevuto sui telefoni cellulari degli agenti allerte di riconoscimento facciale in tempo reale, provenienti da una rete privata di oltre cinquemila telecamere, duecento delle quali abilitate al riconoscimento biometrico, che confrontava i passanti con un elenco di sorvegliati gestito da un soggetto privato. Il programma non compariva in alcuna delle relazioni pubbliche che l'ordinanza imponeva. È stato rivelato nel maggio 2025 da un'inchiesta giornalistica[68]. Nel giugno 2025 il Consiglio esaminava un'ordinanza che avrebbe autorizzato per il futuro ciò che era stato compiuto senza titolo.

Il dato analiticamente rilevante non è la violazione, ma l'identità del soggetto che l'ha accertata. Non un giudice, che non aveva alcuna causa davanti a sé; non un'autorità indipendente, perché nessuna aveva competenza; non il Consiglio comunale, il cui meccanismo di rendicontazione il programma aveva semplicemente aggirato. La correzione è venuta dalla stampa, con due anni di ritardo, e la sua conseguenza legislativa immediata è stata una proposta di ratifica della prassi. Posta accanto alla sequenza italiana ricostruita *supra*, § 2 – dove un'autorità esterna ha modificato una disposizione poche settimane prima della sua adozione – la differenza non è di severità: entrambe le città e entrambi gli ordinamenti vietano la sorveglianza biometrica generalizzata. La differenza sta nel momento in cui il divieto morde, e nel soggetto che glielo fa fare.

Va infine registrata un'ultima vulnerabilità del livello municipale, che completa il quadro di un sistema privo di pavimento. I divieti comunali esistono per concessione dello Stato, e diversi Stati hanno adottato o preso in considerazione misure che precludono agli enti locali la regolazione delle tecnologie di sorveglianza. Ove tale preclusione operi, il livello più protettivo del sistema americano è anche il più agevolmente sopprimibile – non dal corpo elettorale che lo ha adottato, ma da un legislatore posto al di sopra di esso. L'assetto europeo rovescia questa relazione: la fonte sovranazionale fissa un minimo al di sotto del quale il diritto nazionale non può scendere, e lascia gli Stati membri liberi di legiferare al di sopra. È la direzione nella quale la gerarchia opera, e non la sua mera esistenza, a distinguere un pavimento da un soffitto.

7. Il termine esterno di controllo: la Repubblica popolare cinese. Il regolamento del Consiglio di Stato sull'amministrazione dei sistemi di videosorveglianza di pubblica sicurezza – ordinanza n. 799, adottata il 16 dicembre 2024 e in vigore dal 1° aprile 2025 – e le Misure per la gestione della sicurezza nell'applicazione della tecnologia di riconoscimento facciale, adottate congiuntamente dalla Cyberspace Administration of China e dal Ministero della

[67] New Orleans, ordinanza 33021, dicembre 2020; *Surveillance Technology and Data Protection Ordinance*, adottata il 21 luglio 2022, New Orleans City Code § 147-2.

[68] Inchiesta del *Washington Post* pubblicata il 19 maggio 2025; comunicato dell'American Civil Liberties Union del 20 maggio 2025. Le allerte sono state sospese dal sovrintendente di polizia nell'aprile 2025; alla fine di quell'anno l'assetto del 2022 restava lo strumento vigente.

pubblica sicurezza con ordinanza n. 19 del 13 marzo 2025, non contengono, a scorrerne il testo, alcuna disposizione che esenti espressamente gli organi di pubblica sicurezza dagli obblighi che pure impongono a ogni altro titolare del trattamento. L'esenzione, quando opera, risulta da un sistema di clausole di rinvio disseminate nel secondo dei due testi, ciascuna delle quali cede il passo a «leggi e regolamenti amministrativi» ulteriori senza indicarne il contenuto. L'art. 8 vincola la conservazione del dato biometrico all'interno del dispositivo e ne vieta la trasmissione in rete, salvo quanto diversamente disposto da leggi e regolamenti amministrativi. L'art. 10, c. 2, vieta l'impiego del riconoscimento facciale come unico metodo di verifica dell'identità quando esistano alternative, ma cede anch'esso il passo a «diverse disposizioni statali» sulla verifica dell'identità mediante la stessa tecnologia: una clausola che si presta a ricomprendere, senza nominarla, la disciplina della pubblica sicurezza[69]. Una terza clausola si trova nel penultimo comma dell'art. 5, che fa prevalere le disposizioni di leggi e regolamenti amministrativi che consentano di omettere l'informativa preventiva; l'ultimo comma riguarda invece l'accessibilità dell'informativa per le persone con disabilità e per gli anziani[70].

Le Misure del 2025 non operano, tuttavia, in un vuoto normativo: si innestano su un impianto generale che la legge sulla protezione delle informazioni personali del 2021 aveva già costruito per l'intera categoria dei dati biometrici, qualificati come «informazioni personali sensibili». L'art. 28 di quella legge definisce sensibile l'informazione che, se divulgata o utilizzata illecitamente, può facilmente ledere la dignità della persona o mettere a rischio la sua sicurezza personale o patrimoniale, e vi include espressamente i dati biometrici accanto al credo religioso, all'identità specifica, ai dati sanitari, ai conti finanziari, alla localizzazione e ai dati dei minori di quattordici anni; gli artt. 29-30 impongono, per il trattamento di questa categoria, il consenso separato dell'interessato e un'informativa rafforzata sulla necessità del trattamento e sul suo impatto[71]. È rispetto a questo regime generale, non rispetto a un vuoto di tutela, che l'art. 26 della medesima legge opera come norma speciale per la pubblica sicurezza: pone come regola che i dati raccolti mediante dispositivi di acquisizione immagine o di identificazione personale installati in luoghi pubblici possano essere utilizzati soltanto per finalità di mantenimento della sicurezza pubblica, ed è solo per questo impiego, coincidente con la finalità dichiarata dell'installazione, che il consenso separato altrimenti richiesto dall'art. 29 non è necessario[72]. Il raffronto con il modello europeo va condotto, su questo punto, sul terreno della base giuridica e non su quello del consenso. Neppure nel diritto dell'Unione il consenso è la base ordinaria dei trattamenti a fini di polizia: la direttiva (UE) 2016/680 li fonda sulla necessità per l'esecuzione di un compito previsto dalla legge e, per i dati biometrici, sulla stretta necessità, così come la legge cinese ammette il trattamento senza consenso quando sia necessario all'adempimento di doveri od obblighi di legge. La differenza non sta dunque nella rinuncia al consenso, comune ai due sistemi, ma in ciò che ne prende il posto: nel modello europeo, un requisito di stretta necessità la cui osservanza è verificabile da un'autorità esterna; nell'art. 26, una destinazione funzionale – l'uso per la sicurezza pubblica – che coincide con la finalità dichiarata dall'apparato che installa i dispositivi, e la cui osservanza è verificata, come si vedrà, all'interno del medesimo apparato.

---

[69] Misure per la gestione della sicurezza nell'applicazione della tecnologia di riconoscimento facciale, ordinanza congiunta Cyberspace Administration of China – Ministero della pubblica sicurezza n. 19, adottata il 30 settembre 2024, promulgata il 13 marzo 2025, in vigore dal 1° giugno 2025, artt. 8 e 10, c. 2.

[70] Ordinanza n. 19, art. 5, penultimo comma.

[71] Legge sulla protezione delle informazioni personali della RPC, approvata il 20 agosto 2021, in vigore dal 1° novembre 2021, artt. 28-30.

[72] Legge sulla protezione delle informazioni personali della RPC, art. 26; sulle basi giuridiche diverse dal consenso, art. 13, c. 1, n. 3. Per il diritto dell'Unione, dir. UE 2016/680, artt. 8 e 10, e considerando 35.

Sarebbe però inesatto affermare che gli organi statali siano del tutto liberi dagli obblighi della legge. Il Capo II, Sezione III, ne pone alcuni specificamente a loro carico: il trattamento non deve eccedere gli scopi necessari all'adempimento dei doveri e delle responsabilità previste dalla legge; salvo urgenza, necessità o emergenza, l'organo statale deve notificare all'interessato scopi e responsabilità del trattamento; i dati trattati dallo Stato, o da organizzazioni autorizzate per suo conto, sono conservati nel territorio della Repubblica popolare[73]. La differenza non sta dunque nell'assenza di obblighi, ma nella loro asimmetria e, soprattutto, nel meccanismo che ne assicura l'osservanza. È il rilievo che ha mosso la dottrina comparatistica italiana all'indomani dell'entrata in vigore della legge, osservando che questa non pone in capo alle autorità statali gli stessi obblighi cui sono soggetti i gestori privati del trattamento, e che l'Amministrazione cinese del ciberspazio cumula in sé il ruolo di produttore attivo delle disposizioni e quello di controllore della loro applicazione, in un contesto istituzionale nel quale le agenzie governative non sono indipendenti[74]. La medesima analisi segnala inoltre che l'art. 3, c. 2, n. 3, della legge consente a nuove leggi e regolamenti amministrativi di richiamarne direttamente l'applicazione, lasciando all'Amministrazione del ciberspazio la facoltà di estenderne o integrarne l'ambito: lo stesso meccanismo di rinvio aperto che si è visto operare, in senso inverso, nelle Misure del 2025 e nel regolamento n. 799.

Il meccanismo di controllo sull'osservanza di queste regole conferma, sul piano dell'art. 32 del regolamento n. 799, la coincidenza fra vigilante e vigilato che il presente lavoro ha assunto come tratto del modello: la violazione delle norme da parte degli organi di pubblica sicurezza è sanzionata, in via amministrativa, dall'organo di pubblica sicurezza gerarchicamente superiore o dal dipartimento competente della medesima amministrazione, non da un'autorità esterna alla gerarchia esecutiva[75]. È il medesimo testo che colloca, all'art. 3, l'adesione alla direzione del Partito comunista cinese nel dispositivo della disciplina sulla gestione del sistema di videosorveglianza, e non nel preambolo, come si è già segnalato *supra*, § 1[76]. Su un piano affatto diverso, e puramente tecnico, si colloca invece la disciplina della conservazione. L'art. 17 la articola in tre membri distinti, che conviene tenere separati. Il primo è un termine minimo, non inferiore a trenta giorni, che non è una garanzia per l'interessato ma un obbligo di disponibilità del dato a fini di verifica. Il secondo è un obbligo di cancellazione, decorso quel termine, dei dati il cui scopo di trattamento sia stato realizzato: e questa è una garanzia in senso proprio, non meno stringente di quelle europee. Il terzo è un'ulteriore clausola di rinvio, che fa prevalere le diverse disposizioni eventualmente contenute in leggi e regolamenti amministrativi sui termini di conservazione, replicando anche qui il meccanismo già osservato negli artt. 5, 8 e 10, c. 2, delle Misure del 2025[77].

Sul fronte del rimedio individuale, il precedente più noto resta la controversia fra Guo Bing e lo zoo safari di Hangzhou, che merita qui una ricostruzione più fedele di quanto la sua fama

[73] Legge sulla protezione delle informazioni personali della RPC, artt. 34, 35 e 37.

[74] D. Clementi, *La legge cinese sulla protezione delle informazioni personali: un GDPR con caratteristiche cinesi?*, in *Rivista di diritti comparati*, 1, 2022, 189 ss., spec. 213-214. Dello stesso contributo si vedano, per la ricostruzione del sistema duale introdotto dal Codice civile del 2020, che distingue il diritto alla *privacy* (*yinsi quan*), di natura negativa, dal diritto alla protezione delle informazioni personali, di natura positiva e di controllo, le pagine 194-197. Sul sistema di credito sociale come regolazione sociotecnica mediante sorveglianza, valutazione e sanzione, v. E. Consiglio, G. Sartor, *Il sistema di credito sociale cinese: una «nuova» regolazione sociotecnica mediante sorveglianza, valutazione e sanzione*, in *Tigor*, XIII, 2, 2021, 139 ss.

[75] Regolamento sull'amministrazione dei sistemi di videosorveglianza di pubblica sicurezza, ordinanza del Consiglio di Stato n. 799, adottata il 16 dicembre 2024, promulgata il 13 gennaio 2025, in vigore dal 1° aprile 2025, art. 32.

[76] Reg. n. 799, art. 3 (v. *supra*, § 1, nota 7).

[77] Reg. n. 799, art. 17.

mediatica lasci intendere. Il tribunale del distretto di Fuyang decideva quando né il codice civile né la legge sulla protezione delle informazioni personali erano ancora in vigore. Ha perciò fondato la motivazione sulla legge sulla tutela dei consumatori, qualificando il dato biometrico come informazione la cui raccolta deve rispettare, anche in assenza di una legge speciale, i principi di legittimità, correttezza e necessità. Secondo la sentenza, l'informazione biometrica riflette in profondità le caratteristiche fisiologiche e comportamentali della persona e ha un forte carattere personale; se divulgata o usata illecitamente, può condurre a discriminazioni o a pregiudizi imprevedibili per la sicurezza personale o patrimoniale, e richiede perciò un trattamento particolarmente cauto e una protezione rafforzata[78]. È una motivazione di rilievo, ma va collocata nella sua esatta portata: la parte più consistente delle domande di Guo Bing – la richiesta di dichiarare invalidi gli avvisi contrattuali dello zoo, non solo di ottenere la cancellazione dei propri dati – è stata respinta in entrambi i gradi di giudizio, sul rilievo che l'informativa esposta al pubblico soddisfaceva comunque i requisiti di trasparenza e di consenso richiesti dalla legge sulla tutela dei consumatori[79]. Il precedente resta dunque, con precisione, un rimedio privatistico per violazione dello scopo dichiarato della raccolta – lo zoo aveva attivato il riconoscimento facciale su fotografie raccolte per un fine diverso, quello dell'identificazione tramite impronta digitale – e non una vittoria generale del principio del consenso informato sulla raccolta di dati biometrici in quanto tale: una precisazione che non sminuisce l'importanza del caso, ma ne colloca correttamente la portata, distinguendo un rimedio orizzontale fra privati da un controllo verticale sull'apparato pubblico, che è invece l'oggetto proprio di questo lavoro. Va aggiunto, per prevenire un fraintendimento che la formula «assenza di controllo verticale» potrebbe alimentare, che tale assenza non è una lacuna accidentale né un ritardo di maturazione dell'ordinamento cinese, colmabile in via interpretativa o destinato a essere superato dall'evoluzione normativa: è una scelta deliberata di *design* istituzionale, e i testi ne recano traccia esplicita. L'art. 32 del regolamento n. 799 non tace sul controllo, lo disciplina, affidandolo all'organo di pubblica sicurezza gerarchicamente superiore; l'art. 26 della legge sulla protezione delle informazioni personali non dimentica la pubblica sicurezza, la esonera espressamente dal consenso separato; l'art. 3 del medesimo regolamento colloca nel dispositivo, e non nel preambolo, il principio della direzione del Partito. Un ordinamento che regola il controllo interno con questo grado di dettaglio non ha omesso di prevedere quello esterno: ha scelto di non prevederlo.

Il nesso fra questo precedente e la disciplina locale non si esaurisce nell'omonimia della città: il regolamento sulla gestione condominiale di Hangzhou, che vieta agli amministratori di imporre ai residenti l'uso dell'impronta digitale o del riconoscimento facciale per l'accesso alle parti comuni, è stato promosso in sede di audizione pubblica dallo stesso Guo Bing, a saldatura fra il fronte contrattuale e quello regolamentare locale della medesima vicenda[80]. Le altre due discipline locali censite mostrano la stessa direzione di marcia su un piano più generale: il regolamento sui dati di Shanghai, in vigore dal 1° gennaio 2022, subordina il

[78] Tribunale del distretto di Fuyang (Hangzhou), 20 novembre 2020, n. (2019) Zhe 0111 Min Chu 6971, *Guo Bing c. Hangzhou Safari Park Co., Ltd.*; corte intermedia di Hangzhou, 9 aprile 2021, n. (2020) Zhe 01 Min Zhong 10940, che riproduce e conferma la medesima motivazione.

[79] Il tribunale del distretto di Fuyang, nel respingere la domanda di invalidità degli avvisi contrattuali, ha ritenuto che la raccolta di dati biometrici da parte dello zoo rispondesse ai criteri di legittimità, correttezza e necessità richiesti dall'art. 29 della legge sulla tutela dei diritti e degli interessi dei consumatori; la corte intermedia di Hangzhou ha confermato questo punto in appello, respingendo la generalità delle ulteriori domande di Guo Bing.

[80] *Hangzhou shi wuye guanli tiaoli*, seconda revisione approvata il 29 giugno 2021, approvata dal Comitato permanente dell'Assemblea popolare dello Zhejiang il 30 luglio 2021, in vigore dal 1° marzo 2022.

trattamento dei dati biometrici al principio di necessità e al consenso separato, e vieta l'uso dei dispositivi di acquisizione immagine installati in luoghi pubblici come unico metodo di verifica per l'accesso[81]; il regolamento sui dati della zona economica speciale di Shenzhen, in vigore dalla stessa data, definisce puntualmente il dato biometrico e impone, per il suo trattamento, il consenso esplicito e l'offerta di un'alternativa non biometrica[82]. Sono discipline che confermano, sul piano locale e in materie estranee alla pubblica sicurezza, un livello di garanzia non inferiore a quello europeo – a riprova che il punto di divaricazione fra i due modelli non sta nel contenuto delle regole, ma nella loro applicabilità all'apparato che le impone a se stesso.

.

8. La variabile discriminante. I paragrafi che precedono consentono ora di tornare alla domanda posta in apertura con un materiale sufficiente a scioglierla, e la risposta che se ne ricava non è quella che l'intuizione avrebbe suggerito. Il rigore contenutistico delle garanzie non è la variabile che separa il modello europeo dall'esperienza cinese: su singoli punti, anzi, quest'ultima non è meno puntuale. La disciplina della conservazione ne offre un esempio istruttivo, purché non se ne semplifichi la struttura. L'art. 10, c. 7, del d.lgs. n. 160/2026 fissa in sette giorni il termine di conservazione dei dati nella base dati di riferimento, con cancellazione automatica alla scadenza. L'art. 17 del regolamento del Consiglio di Stato n. 799 combina invece un termine minimo di trenta giorni, che è obbligo di disponibilità e non garanzia, con un obbligo di cancellazione dei dati il cui scopo sia stato realizzato, che garanzia lo è in senso proprio. Le due discipline muovono da esigenze diverse e non sono sovrapponibili quanto alla durata, ma nessuna delle due è meno precisa dell'altra quanto al presidio della cancellazione[83]. Lo stesso vale per altri due profili. L'obbligo di notificazione preventiva e il divieto di trasmissione in rete del dato biometrico, che le Misure congiunte del 2025 impongono a ogni titolare del trattamento non coperto dalle clausole di rinvio esaminate *supra*, § 7, non sono meno stringenti delle corrispondenti garanzie europee, e si innestano su un regime generale del dato sensibile che la legge del 2021 sulla protezione delle informazioni personali ha costruito con cura non inferiore a quella del regolamento (UE) 2016/679. Le discipline locali di Shanghai e Shenzhen, infine, estranee alla pubblica sicurezza, si collocano su uno standard di consenso e di necessità pienamente comparabile a quello europeo[84]. Se la comparazione si fermasse al contenuto delle regole, la linea di displuvio fra i due modelli risulterebbe assai più sfumata di quanto la premessa intuitiva induca a credere. La variabile discriminante è un'altra, ed è quella che il presente lavoro ha isolato *supra*, § 1, come tratto strutturale anziché come appartenenza a una famiglia giuridica: la separazione fra chi impiega la tecnologia di identificazione biometrica e chi ne controlla l'osservanza. Nei tre ordinamenti europei esaminati questa separazione ricorre in forme testuali diverse – delega legislativa, legge sperimentale, legge organica – ma converge su un dato comune, verificato *supra*, § 5: un soggetto esterno alla catena di comando che impiega la tecnologia interviene prima che il procedimento, normativo o autorizzatorio, si sia concluso, e non soltanto a valle di esso. Nell'ordinamento cinese, per converso, il controllo sull'osservanza delle regole – puntuali quanto si è detto – resta interno alla medesima gerarchia amministrativa che quelle regole applica: l'art. 32 del regolamento n. 799 affida la sanzione

[81] *Shanghai shi shuju tiaoli*, approvato il 25 novembre 2021, in vigore dal 1° gennaio 2022, artt. 22 e 24.
[82] *Shenzhen jingji tequ shuju tiaoli*, approvato il 29 giugno 2021, pubblicato il 6 luglio 2021, in vigore dal 1° gennaio 2022, art. 2, punto 4, e art. 19.
[83] D.lgs. n. 160/2026, art. 10, c. 7 (v. *supra*, § 2, nota 14); Reg. n. 799, art. 17 (v. *supra*, § 7, nota 77).
[84] Ordinanza n. 19, artt. 4, 6, 9 e 10 (v. *supra*, § 7, nota 69); *Shanghai shi shuju tiaoli*, artt. 22 e 24; *Shenzhen jingji tequ shuju tiaoli*, art. 2, punto 4, e art. 19 (v. *supra*, § 7, note 81-82).

delle violazioni all'organo di pubblica sicurezza superiore, non a un'autorità terza.
È qui che l'inserimento del termine intermedio ricostruito *supra*, § 6, mostra la propria utilità, perché impedisce di arrestarsi a una contrapposizione binaria che i soli dati europei e cinesi avrebbero suggerito. Gli Stati Uniti possiedono la separazione strutturale in misura piena: le corti federali e statali sono indipendenti dall'esecutivo in un senso che nessuna autorità amministrativa europea può rivendicare, e tre Stati prevedono per giunta il mandato giudiziario, e un quarto, il Maine, uno standard sostanziale di *probable cause*. Se la separazione bastasse, l'esperienza americana dovrebbe collocarsi al livello europeo o al di sopra di esso. Non vi si colloca, e le ragioni sono due, entrambe estranee alla nozione di separazione.
La prima è l'assenza di uniformità. La garanzia esiste soltanto in una parte degli Stati, fra quindici e ventiquattro secondo il criterio di computo, varia nel contenuto fra di essi, e può essere ritirata da una sessione legislativa successiva, come la Virginia ha dimostrato attraversando tre regimi in cinque anni. Il difetto opera per giunta in due direzioni. Orizzontalmente, un divieto vincola l'agenzia che se lo è dato e non quella della giurisdizione confinante, sicché il divieto municipale è soddisfatto nella forma chiedendo al vicino non vincolato di eseguire la ricerca. Verticalmente, la gerarchia corre nel senso sbagliato: le tutele comunali esistono per concessione dello Stato e possono essere precluse dall'alto, mentre il diritto nazionale europeo può salire sopra il pavimento fissato dalla fonte unionale ma non scendere al di sotto.
La seconda è l'assenza di anticipazione. Il controllo americano, dove pure esiste e dove pure è affidato a un organo pienamente indipendente, interviene su una causa già instaurata, cioè su un danno già prodotto. La vicenda di New Orleans lo mostra con nettezza: per due anni la violazione di un'ordinanza vigente non ha trovato alcun correttore istituzionale, e l'indipendenza delle corti non ha giovato ai residenti perché nessuna corte aveva davanti a sé una controversia. Il medesimo rilievo vale per San Francisco e per Austin, i cui divieti municipali sono stati rispettati nella forma mentre i risultati venivano ottenuti tramite agenzie non vincolate.
Ne risultano tre posizioni, e non un continuo dal permissivo al restrittivo. L'Europa combina separazione, uniformità e anticipazione. Gli Stati Uniti hanno la separazione senza l'uniformità, e l'anticipazione soltanto dove un singolo legislatore statale abbia scelto di apprestarla. La Cina non ha la separazione, e non ha perciò occasione di porsi il problema delle altre due. La posizione americana è quella analiticamente decisiva, perché dimostra che la separazione dei poteri, intesa come indipendenza istituzionale dell'organo controllante, è condizione necessaria ma non sufficiente: ciò che qualifica il modello europeo è la sua congiunzione con l'uniformità del pavimento e con la tempestività dell'intervento.
Conviene esplicitare il rapporto fra questi tre elementi e le quattro invarianti indotte in precedenza (*supra*, § 5), perché non si tratta di due elenchi concorrenti. Le invarianti descrivono come il modello europeo si presenta nei testi; i tre elementi isolano ciò che, fra quei tratti, risulta discriminante una volta introdotti i termini di confronto esterni. La separazione è il tratto comune alla seconda e alla terza invariante, e la quarta ne costituisce il presidio giurisdizionale; l'anticipazione corrisponde alla terza, nella misura in cui il diritto dell'Unione la rende obbligatoria; l'uniformità del pavimento non coincide con alcuna invariante, perché non è un tratto dei singoli ordinamenti ma del loro rapporto con la fonte sovranazionale, ed è per questo che il confronto fra i soli ordinamenti europei, tutti soggetti al medesimo pavimento, non poteva farla emergere. La riserva di legge, infine, è condizione degli altri elementi più che elemento autonomo: senza una fonte legislativa non vi sarebbe una regola cui il controllo esterno possa commisurarsi, ma la sua presenza, come mostrano le leggi statali americane, non basta a qualificare il modello.
A questa ricostruzione si può opporre un'obiezione di metodo, che merita risposta esplicita

Issn 2421-0528

prima di trarre le conclusioni. Si potrebbe osservare che la stessa nozione di «autorità indipendente» impiegata in questo lavoro è meno netta di quanto sembri: si è visto *supra*, § 4, che l'AESIA spagnola, cui la legge affida un ruolo di coordinamento generale, non è indipendente in senso tecnico, essendo incardinata in un ministero; e si potrebbe aggiungere che anche il Garante italiano, per quanto qualificato come autorità indipendente, è nominato dal Parlamento secondo un procedimento che ne rende la composizione sensibile agli equilibri politici del momento. Se la linea fra modello europeo e modello cinese dipendesse da un'indipendenza istituzionale piena e incondizionata, l'obiezione coglierebbe nel segno, e la distinzione qui proposta rischierebbe di ridursi a una differenza di grado, non di natura. Ma non è questo il criterio impiegato: la terza invariante richiede non l'indipendenza assoluta di ogni autorità coinvolta, bensì l'esistenza di *almeno un soggetto* esterno alla catena di comando dell'esecutivo che impiega la tecnologia, dotato del potere di incidere sulla norma prima che essa si consolidi – e un simile soggetto, come mostra il caso italiano dell'estate 2026, può intervenire con effetti reali anche restando imperfettamente indipendente sul piano della propria genesi istituzionale. È l'effetto sul procedimento, non la purezza della fonte, il tratto che qui si misura.

La vicenda italiana dell'estate 2026, ricostruita *supra*, § 2, offre in questo senso una verifica empirica particolarmente istruttiva, perché mostra la variabile discriminante operare su un procedimento normativo in corso, e per giunta due volte. Il parere del Garante del 14 luglio 2026 non si è limitato a segnalare una criticità: ha inciso sulla struttura della disposizione, e il testo pubblicato ne reca traccia testuale, sia nella memorizzazione delle immagini «senza elaborazione dei relativi dati biometrici» (art. 10, c. 4), sia nel richiamo all'art. 8 del d.lgs. n. 51/2018 (art. 10, c. 10)[85]. Le Commissioni parlamentari, a loro volta, organo per definizione interno al circuito maggioranza-Governo e dunque tutt'altro che indipendente in senso tecnico, hanno formulato, anche per voce della maggioranza, l'osservazione sulla non incrementalità delle banche dati, che il testo pubblicato ha recepito quasi alla lettera (art. 8, c. 3). Anche un organo politico, quando la separazione strutturale è già incorporata nel procedimento come regola di metodo, può concorrere a rafforzarla. Ciò conferma che il tratto discriminante è la struttura del procedimento, cioè la sua apertura a un intervento correttivo prima della conclusione, e non la composizione dell'organo che lo esercita. Su questo punto l'ipotesi di lavoro formulata in apertura, che attribuiva la tenuta della separazione a un ceto professionale, va dunque corretta: la tripartizione di Mattei resta utile a qualificare l'esperienza cinese come diritto di tipo politico, ma nel modello europeo la separazione non è monopolio dei giuristi di professione, e può essere sostenuta anche da un organo politico, purché il procedimento ne preveda l'intervento prima che la norma si consolidi. È esattamente il tipo di intervento che, nel modello cinese ricostruito *supra*, § 7, non ha un corrispondente strutturale: un controllo equivalente su una disposizione del regolamento n. 799 seguirebbe, se mai fosse esercitato, il canale interno dell'art. 32, cioè un organo di pubblica sicurezza superiore che richiama all'osservanza un organo subordinato, e non un'autorità, indipendente o meno, esterna a quella gerarchia.

Una seconda obiezione possibile riguarda proprio il caso Guo Bing, ricostruito *supra*, § 7: se un rimedio giurisdizionale contro l'uso indebito della biometria esiste anche in Cina, si potrebbe dire, la distinzione fra i due modelli si attenua anche sul piano del sindacato giurisdizionale, non solo su quello del contenuto delle regole. La risposta sta nella distinzione, già proposta in quella sede, fra rimedio orizzontale e controllo verticale: la sentenza di Fuyang e la sua conferma in appello intervengono in una controversia fra privati, per violazione di

[85] Garante per la protezione dei dati personali, provv. n. 531 del 14 luglio 2026 (v. *supra*, § 2, nota 15); d.lgs. n. 160/2026, art. 10, cc. 4 e 10, e art. 8, c. 3.

un vincolo contrattuale e dello scopo dichiarato della raccolta, e lasciano del tutto impregiudicato il quesito, proprio di questo lavoro, di chi controlli l'apparato di pubblica sicurezza quando è quest'ultimo, e non un gestore di parco privato, a impiegare la tecnologia. Un consumatore può ottenere, in Cina, la cancellazione del proprio dato biometrico da un soggetto privato inadempiente; nessuna disposizione fin qui esaminata gli consente di ottenere un controllo equivalente sull'operato di un organo di pubblica sicurezza che agisca nei limiti, per quanto ampi, della propria gerarchia interna.

Il confronto con il termine esterno non è, del resto, un artificio dell'analisi comparatistica: è entrato nel dibattito pubblico italiano sullo schema di decreto, e vi è entrato come accusa. Il 30 luglio 2026 il relatore per la I Commissione della Camera ha respinto come «non corretta» la lettura di quanti, sulla stampa, evocavano «schedature di massa», il «Grande Fratello» e «modelli cinesi»; e il 1° agosto, a decreto approvato in via preliminare ma non ancora in via definitiva, un docente universitario ha sostenuto in un'intervista che l'Italia si stesse muovendo proprio in quella direzione, indicando due profili: la possibilità per le forze dell'ordine di attivare la sorveglianza tecnologica in tempo reale senza autorizzazione di un giudice, e la conservazione per una settimana dei dati raccolti con uno *screening* preventivo di massa, senza distinzione fra sospettati e cittadini che semplicemente attraversino un luogo pubblico[86]. I due rilievi vanno tenuti distinti, perché solo il secondo coglie nel segno nei termini in cui è formulato. Quanto al primo, si è visto *supra*, § 2, che il decreto conosce due canali per il tempo reale, e che quello a fini investigativi richiede l'autorizzazione del giudice per le indagini preliminari; l'assenza di autorizzazione giudiziaria riguarda il canale preventivo, dove interviene comunque il Procuratore della Repubblica, e la stessa Camera aveva chiesto di unificare i due regimi verso l'alto. Quanto al secondo, il rilievo coglieva nel segno sul testo dello schema, e coincideva con quello del Garante; ma il testo approvato tre giorni dopo ha accolto proprio la soluzione indicata dal Garante, sicché le immagini conservate per sette giorni sono memorizzate senza elaborazione biometrica, e l'elaborazione è consentita solo dopo la commissione di un reato (art. 10, cc. 4 e 7). Ma è proprio la vicenda dell'intervista a offrire la prova più immediata della tesi qui sostenuta: la critica è stata formulata pubblicamente, da un accademico, in un quotidiano, prima dell'approvazione definitiva, e si aggiunge a un parere di un'autorità indipendente reso in corso di procedimento e alle osservazioni di due Commissioni parlamentari. Un simile concorso di controlli esterni non è concepibile nell'assetto ricostruito *supra*, § 7, e la sua stessa possibilità è ciò che separa i due modelli assai più di quanto li separi il contenuto delle rispettive garanzie.

Vi è, infine, una controprova che la clausola di salvezza dell'art. 8, c. 8, offre alla tesi qui sostenuta, e che conviene esplicitare perché mostra la variabile discriminante operare per difetto anziché per eccesso. Si è visto *supra*, § 2, che la clausola sottrae all'obbligo di cancellazione gli elementi acquisiti «sotto altra base giuridica conforme al decreto legislativo n. 51 del 2018»: il testo pubblicato ha delimitato l'ambito dei titoli invocabili, ma non li ha tipizzati, né ha richiesto che la loro sussistenza sia accertata da un terzo. Se la prassi ne trae la conseguenza più immediata, sarà la medesima autorità che ha impiegato illegittimamente il sistema a valutare se un titolo alternativo giustifichi la conservazione di ciò che ha raccolto. Il controllo sull'osservanza della regola tornerebbe allora a coincidere con l'apparato che quella regola vincola, e la separazione strutturale verrebbe meno proprio nel segmento in cui è più necessaria, cioè a valle di una violazione già consumata. Non si tratterebbe di una convergenza sui contenuti, che si è visto essere ampia e non decisiva. Si tratterebbe di una

[86] Intervista a M. Colajanni, *L'Italia va verso la Cina sul riconoscimento facciale*, in *Il Fatto Quotidiano*, 1° agosto 2026. I due profili segnalati corrispondono, rispettivamente, al canale dell'art. 8 e all'art. 10, cc. 3 e 6, dello schema (cc. 4 e 7 del testo pubblicato).

replica surrettizia dell'assetto ricostruito *supra*, § 7: coincidenza fra vigilante e vigilato, con l'unica differenza che in Cina essa è dichiarata nel testo, all'art. 32 del regolamento n. 799, mentre qui risulterebbe dalla genericità di una clausola di salvezza. È per questo che il rilievo del Garante, e la richiesta di tipizzazione che lo accompagna, cui il testo pubblicato ha risposto solo in parte, non attengono a un dettaglio tecnico della disciplina della cancellazione: toccano il punto in cui il modello europeo, se cede, cessa di essere tale.

Che la separazione strutturale tenga anche quando la sua fonte muta radicalmente è quanto la corroborazione tedesca, discussa *supra*, § 5, ha permesso di mostrare: dove manca una riserva di legge specifica sulla biometria, il vincolo sull'esecutivo può provenire dalla giurisprudenza costituzionale, e restare nondimeno esterno alla catena di comando che la tecnologia impiega[87]. È questa persistenza, attraverso mutamenti così radicali nella fonte del vincolo – dalla delega legislativa al precedente costituzionale, dall'autorizzazione del pubblico ministero al parere di un'autorità indipendente in corso di procedimento, fino all'osservazione di una Commissione parlamentare che riproduce lo stesso rilievo con altri strumenti – a segnalare che la separazione strutturale non è un prodotto contingente della famiglia giuridica romanistica, né è legata a un unico tipo di organo che la eserciti.

Il confronto a tre termini consente però di formulare la conclusione in modo più esatto di quanto il solo raffronto europeo-cinese avrebbe permesso. Ciò che qualifica il modello europeo non è la severità delle sue regole, che si è visto essere in più punti pareggiata dall'ordinamento cinese e in taluni superata da quello virginiano; e non è nemmeno la sola separazione fra chi impiega la tecnologia e chi ne controlla l'osservanza, che gli Stati Uniti possiedono in misura piena senza per questo assicurare una tutela superiore. È la congiunzione di tre elementi: un pavimento uniforme, fissato da una fonte sovraordinata al di sotto del quale il legislatore nazionale non può scendere pur restando libero di salire; la separazione strutturale del controllo dalla catena di comando che la tecnologia impiega; e la collocazione di quel controllo a monte, in un momento nel quale la norma o l'autorizzazione non si sono ancora consolidate. Sottratto il primo elemento si ottiene la frammentazione americana, dove la garanzia dipende da quale confine si sia attraversato e da quale sessione legislativa abbia da ultimo affrontato la questione. Sottratto il secondo si ottiene l'assetto cinese, dove regole anche puntuali sono affidate all'autocontrollo dell'apparato che ne è destinatario. Sottratto il terzo si ottiene una tutela che interviene sempre dopo il danno, e talvolta – come a New Orleans – non interviene affatto, se non per iniziativa di un soggetto, la stampa, che nessun ordinamento può istituzionalizzare come organo di controllo.

È questa, in definitiva, la risposta che il confronto consente di dare alla domanda posta nel titolo[88]: chi custodisca i custodi non dipende dalla severità delle regole che li vincolano, ma dall'esistenza, prima che la regola si consolidi, di un custode che non appartenga alla loro stessa gerarchia.

Abstract. Il contributo esamina l'identificazione biometrica remota a fini di polizia in Italia, Francia e Spagna nel quadro del regolamento (UE) 2024/1689, e ne confronta la disciplina con quella degli Stati Uniti d'America e della Repubblica popolare cinese. Ne emergono quattro invarianti del modello europeo: riserva di legge, autorizzazione di un terzo, vigilanza indipendente incidente sul procedimento, sindacato giurisdizionale. Il confronto mostra che la variabile discriminante non è il contenuto delle garanzie, talvolta non meno puntuali in

[87] BVerfG, *Urteil des Ersten Senats* del 16 febbraio 2023, 1 BvR 1547/19 e 1 BvR 2634/20 (v. *supra*, § 1, nota 9 e § 5, nota 53).

[88] Giovenale, *Satirae*, VI, 347-348: «*sed quis custodiet ipsos / custodes?*». Nel contesto originario la domanda riguarda i guardiani posti a sorveglianza della fedeltà di una moglie; l'uso che qui se ne fa, corrente nel lessico costituzionale, ne trasferisce il senso al controllo sul potere pubblico.

Cina o più avanzate negli Stati Uniti, ma la congiunzione di tre elementi: un pavimento normativo uniforme, la separazione fra chi impiega la tecnologia e chi ne controlla l'uso, e un controllo che interviene prima che la norma si consolidi.

Abstract. The article examines remote biometric identification for police purposes in Italy, France and Spain under Regulation (EU) 2024/1689, and compares it with the United States and the People's Republic of China. It identifies four invariants of the European model: reservation of law, third-party authorisation, independent oversight capable of shaping the procedure, and judicial review. The comparison shows that the discriminating variable is not the content of the safeguards, at times no less precise in China or more advanced in the United States, but the conjunction of three elements: a uniform regulatory floor, the separation between those who deploy the technology and those who oversee its use, and oversight that intervenes before the rule becomes settled.

Parole chiave. Identificazione biometrica remota – Regolamento (UE) 2024/1689 – Comparazione giuridica – Separazione dei poteri – Repubblica popolare cinese.

Key words. Remote biometric identification – Regulation (EU) 2024/1689 – Comparative law – Separation of powers – People's Republic of China.