

ATTUALITÀ

ANTONIO VELE

Identificazione, intelligenza artificiale e riconoscimento facciale ai sensi dell'art. 349 c.p.p.

L'articolo tratta dell'identificazione e di come approcciare ai nuovi strumenti di riconoscimento facciale alla luce della normativa europea e nazionale, anche sotto il profilo dell'affidabilità degli elementi investigativi.

Artificial intelligence and facial recognition pursuant to article 349 of the code of criminal procedure

The article deals with identification and how to approach new facial recognition tools in light of european and national legislation, also from the perspective of the reliability of investigative elements.

SOMMARIO: 1. L'identificazione e l'identità in generale. - 2. Identificazione soggettiva. - 3. Segue: identificazione di polizia giudiziaria. - 4. Intelligenza artificiale e identificazione facciale.

1. *L'identificazione e l'identità in generale.* L'identificazione presuppone la presenza di una materia e la sua identità riceve linfa dalla capacità di essere identificata, la cui essenza, se non oggetto di manipolazione o speculazione in forza di un determinato ragionamento di appartenenza (di qualsivoglia potere), è momento di rispetto dell'ordine sociale e giuridico in senso complessivo; con tale premessa si vuole affrontare ciò che può apparire di secondo piano nell'ottica generale oltre che in quella specifica, al fine di esaltarne le ragioni intime, in modo da far presente il ruolo principe dell'identificazione nella scena umana. L'identità è legata, anzitutto, alla diversità rispetto alla similitudine di genere e di specie, perché ogni essere umano, pur essendo simile nella "sostanza" si presenta diverso nella "forma" o viceversa; da qui nasce l'esigenza di strutturare strumenti per riconoscere l'identità (= identificare).

In realtà una forma di progresso della società civile è legata proprio alla possibilità di essere riconosciuti nelle proprie caratteristiche psico-fisiche, socio-culturali, morali e spirituali. A sua volta il singolo uomo, all'interno della categoria a cui appartiene, ha il diritto naturale di essere riconosciuto nel suo essere unico, cioè diverso dagli altri¹.

È una “questione” di libertà collettiva e individuale. La diversità, da un lato, comporta, in virtù dello stupore o curiosità, uno stimolo alla conoscenza e al miglioramento mediante il confronto e, dall'altro, implica il diritto di uguaglianza, nel senso che pur essendo diversi dagli altri, a parità di situazioni giuridiche si è sottoposti alle medesime regole; così per diverso, secondo tale paradigma, si intende ovviamente eguale all'altro da un punto di vista della sostanza, ma con una propria identità (s)oggettiva (vale dire uguale a se stesso). Senza sottacere che l'evoluzione della materialità (di qualunque cosa) è legata alla concezione di riuscire ad attribuire a quel qualcosa una propria identità.

Identità, in filosofia, è qualsiasi cosa che rende un'entità definibile e riconoscibile, perché possiede un insieme di qualità o di caratteristiche che la distingue

¹ Su tale base si apre lo sviluppo della convivenza civile (o sociale), delle relazioni interpersonali, dei rapporti commerciali, etc., giacché non sarebbe stato possibile attuare il medesimo se fosse mancata l'idea di realizzare l'atto o il giudizio di identità e quindi procedere con i metodi dell'identificazione per addivenire alla verità. Difatti, ad esempio, noi non avremmo potuto cogliere le differenze dell'accennato sviluppo sul piano della proiezione sociale, e non solo, dei singoli esseri umani, come momento di confronto, di comportamento, di responsabilità, di distinzione di ruoli e di funzioni, etc. Non avremmo potuto distinguere l'oggetto materiale e l'interesse collegato ad esso.

da altre entità. In altri termini identità è ciò che rende due cose la stessa cosa oppure ciò che le rende differenti².

E' chiaro che nello specifico interessa l'identità originaria – soggettiva – e quindi la continuità biologica come insostituibilità dell'essere “che tu sei tu e non un altro soggetto”, vista la naturale mutabilità psico-fisica dell'individuo nel tempo, al fine di garantire al singolo di non subire un procedimento penale ingiusto e poi di tutelare il sistema processuale in modo da non disperdere energie senza giustificazione razionale.

Dunque, vi è la necessità di stabilire “che sei tu” il soggetto indagato e “che sei tu” il soggetto che deve essere sentito come persona informata sui fatti (art. 349 c.p.p.) nel rispetto della funzione e della finalità per cui si procede all'attività di identificazione; siffatta attività è possibile proprio perché ciascuno è dotato di una propria identità soggettiva.

Ritornando alla relazione tra identità e identificazione si comprende che essa è centrale per dare senso all'origine del procedimento penale e quindi all'interesse sotteso ad esso (art. 112 Cost.), dando certezza nella logica della progressione alla fase di accertamento, nel senso che l'imputazione sia riconducibile all'imputato come soggetto identificato. Significativa è poi essa anche nella fase di prevenzione dei reati.

² In argomento cfr., ARISTOTELE, *La metafisica*, trad. di Pietro Eusebiotti, a cura di Oggioni, Padova, 1950; PLATONE, *La Repubblica*, Bari, 1994; KANT, *Critica della ragion pura* trad. di Chiodi, Torino, 1967; LOCKE, *Saggio sull'intelletto umano*, traduzione it., Torino, 1971; HEGEL, *Fenomenologia dello spirito*, trad. it. di De Negri, Firenze, 1973; HUME, *Trattato sulla natura umana*, Bari, 1999; HEIDEGGER, *Identità e differenza*, Milano, 2009.

In questa prospettiva, l'interesse è volto al giudizio di verità espresso dall'attività di identificazione; identificare significa sostanzialmente attribuire un "giudizio" di verità, tra l'altro l'unico che si presenta nell'ambito processuale con il carattere della "certezza", poiché il giudizio di merito si caratterizza come verità processuale, che potrebbe anche rappresentare una verità storica o essere prossima alla medesima, fermo restando che il sistema processuale vigente come è noto non è costruito per raggiungere un simile obiettivo in termini assoluti, dal momento che è bilanciato il rapporto tra il diritto dell'individuo e quello della collettività in direzione della legge fondamentale.

2. Identificazione soggettiva. Sul terreno dell'attività di polizia in generale è di primaria importanza il poter attribuire ad una persona fisica le sue esatte generalità, e cioè, nome, cognome, luogo e data di nascita, residenza e domicilio (se diversi dalla residenza), paternità e maternità. Le esatte generalità sono poi contenute nei registri di stato civile dell'anagrafe del comune ove la persona è nata ed ove risiede (ciò vale sia per i cittadini che per gli stranieri residenti) e la relativa trascrizione ha valore di atto pubblico.

L'accertamento da parte dell'operatore di polizia viene normalmente soddisfatto mediante l'esibizione di un idoneo documento di riconoscimento – carta d'identità o, laddove la legge lo consenta, altro documento equipollente – che consente, altresì, la comparazione tra la persona effigiata nella fotografia con

quella che effettivamente esibisce il documento identificativo³. Laddove, però, l'identificazione tramite un documento di riconoscimento non sia possibile o non sia attuabile, possono subentrare i metodi di identificazione di tipo "scientifico", come l'identificazione dattiloscopica e quella genetica.

Si può, pertanto, subito sgombrare il campo da un equivoco: l'identificazione personale in materia di polizia scientifica non rappresenta un qualcosa di "diverso" rispetto alla identificazione di polizia tradizionalmente intesa, ma costituisce una peculiare modalità attraverso la quale, con il ricorso ad attività tecnico-scientifiche, è possibile stabilire l'identità di una persona.

L'attività di identificazione personale è dunque strumento servente a conseguire un giudizio di identità.

Per una comprensione complessiva dell'identificazione soggettiva, è opportuno procedere ad una preliminare panoramica sui riferimenti normativi dell'attività di fotosegnalamento, richiamando le fonti legislative che ne costituiscono il fondamento.

Secondo la legislazione di pubblica sicurezza, «I rilievi segnaletici per le

³ La carta d'identità, disciplinata in particolare dall'art. 3 t.u.l.p.s., riveste un ruolo fondamentale per la funzione di vigilanza dell'autorità di pubblica sicurezza. È un documento rilasciato dal Sindaco alle persone di età superiore ai 15 anni che ne facciano richiesta, aventi nel comune la loro residenza o dimora, secondo il modello stabilito dal Ministero dell'interno. Tale documento contiene la fotografia, a mezzo busto, senza cappello, del titolare, il numero progressivo, il timbro a secco, la firma, la indicazione delle generalità, dei connotati e i contrassegni salienti. Insieme alla carta d'identità, l'ufficio comunale compila due cartellini: uno è conservato nella segreteria del comune in apposito schedario, in ordine alfabetico sillabico; l'altro è trasmesso al questore della provincia, che ne cura la conservazione in ordine alfabetico, in apposito schedario; essa oggi viene rilasciata su supporto informatico ma, al pari del supporto cartaceo che l'ha preceduta, ha sempre validità di cinque anni. La carta d'identità, infine, è anche documento valido per l'espatrio negli Stati membri dell'Unione europea ed in quelli con cui vigono particolari accordi internazionali. Sul punto, cfr. CALESINI, *Leggi di pubblica sicurezza, illeciti amministrativi*, Roma, 2007, 82 ss.

persone pericolose e sospette e per coloro che non siano in grado o si rifiutino di provare la propria identità, giusta l'art. 4 della legge, sono descrittivi, fotografici, dattiloscopici e antropometrici» (art. 7 reg. del t.u.l.p.s.).

L'art. 349, rubricato Identificazione della persona nei cui confronti vengono svolte le indagini e di altre persone, recita: «Alla identificazione della persona nei cui confronti vengono svolte le indagini può procedersi anche eseguendo, ove occorra, rilievi dattiloscopici, fotografici e antropometrici nonché altri accertamenti...».

L'art. 5 Legge 30 luglio 2002, n. 189 c.d. "legge Bossi-Fini" che ha così modificato l'art. 5 del d.lgs. 25 luglio 1998, n. 286, Testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, stabilisce al comma 2-*bis* che «Lo straniero che richiede il permesso di soggiorno è sottoposto a rilievi fotodattiloscopici» e al comma 4-*bis* «Lo straniero che richiede rinnovo del permesso di soggiorno è sottoposto a rilievi fotodattiloscopici».

Il regolamento (CE) n. 2725/2000 del Consiglio per l'istituzione di Eurodac, all'art. 4 afferma che «Ciascuno Stato membro procede tempestivamente al rilevamento delle impronte digitali di tutte le dita di ogni richiedente asilo di età non inferiore a 14 anni e trasmette sollecitamente all'unità centrale i dati di cui all'articolo 5, paragrafo 1, lettere da a) a f). La procedura di tale rilevamento è stabilita in conformità delle prassi nazionali dello Stato membro interessato e in conformità delle salvaguardie previste dalla Convenzione europea dei diritti dell'Uomo e della Convenzione delle Nazioni Unite sui diritti del

fanciullo».

Il fotosegnalamento è, pertanto, definibile come il complesso dei procedimenti tecnici applicati all'identificazione personale, utilizzati ormai in tutto il mondo e che, richiamando le definizioni normative sopra indicate, si distinguono in: rilievi descrittivi, che consistono nella descrizione generale dell'individuo, quanto al colore dei capelli, degli occhi, alla presenza di segni particolari sul corpo⁴; rilievi dattiloscopici, che consistono nel prelievo delle impronte delle falangi delle dita e del palmo delle mani; rilievi fotografici, che consistono nella fotografia dei particolari del volto (viste frontali e laterali) e del corpo intero, in piedi, secondo modalità uniformi.

Il complesso dei rilievi sopra descritti consente di dare una compiuta identità fisica della persona, con un livello di affidabilità tale da prescindere dal fatto che in occasioni diverse il soggetto abbia dato delle generalità differenti riconducibili a molteplici *alias*.

Questa procedura di rilevamento viene effettuata da operatori specializzati e prevede l'adozione di procedure standardizzate e cronologicamente successive. *In primis*, vengono effettuate delle fotografie della persona, realizzate di perfetto fronte e di perfetto profilo destro, eseguite in condizioni di luce analoga, con un apparato che imprime un solo fotogramma, per evitare il

⁴ Tali rilievi avranno ad oggetto tutte le parti normalmente visibili del corpo (cicatrici sul volto, tatuaggi sull'avambraccio o su altre zone comunque scoperte), non comprendenti quindi segni particolari occultati che, per essere individuati e rilevati presuppongono l'esperimento della ispezione corporale.

cambiamento di espressione del viso tra una ripresa e l'altra⁵; si passa poi al prelevamento delle impronte papillari delle falangi distali di ogni dita e dei palmi di entrambe le mani. Fino a qualche anno fa si procedeva con il metodo degli inchiostri, per cui si aveva la diretta apposizione sul cartellino fotosegnale, sul quale venivano impresse separatamente le impronte delle dita, poi tutte insieme simultaneamente quelle delle quattro dita senza il pollice e, infine, parzialmente il palmo della mano.

Oggi tale sistema è stato sostituito da supporti tecnologici che rilevano le impronte digitali mediante la scansione a fascio laser, secondo la metodica *Fingerprint identification technology* (F.I.T.); questi dispositivi ottico-elettronici, denominati *laser scanner*, consentono di acquisire le impronte digitali senza ricorrere alla tradizionale inchiostrazione dei polpastrelli e dei palmi.

Infine, si indicano i caratteri descrittivi della persona da identificare, inerenti ad alcune voci predeterminate quali occhi, capelli, altezza, corporatura, segni distintivi particolari, quali cicatrici o tatuaggi. A seguito della informatizzazione

⁵ Questa modalità di identificazione potrà essere utile per un confronto di identità, valutando le caratteristiche dell'orecchio esterno o meglio più nel dettaglio il padiglione auricolare che presenta elementi utili per identificare un soggetto; il padiglione auricolare è un parametro per l'identificazione più affidabile anche nel tempo rispetto ai sistemi di riconoscimento facciale a causa dei mutamenti causati dalle espressioni del viso o dal passar del tempo. Le orecchie con l'età tendono a diventare più grandi e i lobi ad allungarsi, ma rimangono identiche alla nascita; in argomento cfr. IANNARELLI, *Ear identification, Forensic identification series, Paramount Publishing Company, Fremont, California*, 1989; FARKAS, *Antropometry of the head and face, Raven Press*, 1994; HOWELL EVENS, *The external ear as a means of Identification, Transaction of the Medico Legal Society*, 1910; HOGSTRATE, VAN DEN HEUVEL, HUYBEN, *Ear identification based on surveillance camera's images, Netherlands Forensic Institute*, 2000; BURGE-BURGER, *Ear biometrics, Biometrics: Personal Identification in Networked Society*, ed. Jain A. et al., Kluwer Academic Publishers, 1998; BHAN, CHEN, *Human ear recognition by computer*, Springer-Verlag, 2008; BALOSSINO, LUCENTEFORTE, SIRACUSA, *Analisi biometrica dell'orecchio in ambito forense, Nuove Tecnologie in Medicina*, n. 1-2, 2006.

delle procedure, si è provveduto all'unificazione dei parametri descrittivi, attraverso la predeterminazione dei parametri da inserire, che garantiscono così l'uniformità delle voci e agevolano l'attività di ricerca.

Al termine di questa attività si genera il c.d. cartellino fotosegnaleτικό del soggetto, che viene introdotto nel sistema A.F.I.S. in uso alle forze di polizia, che permette di memorizzare, oltre alle immagini delle impronte, anche le fotografie ed i dati anagrafici e descrittivi dei soggetti. E' in questa fase, relativa al primo fotosegnalamento, che viene generato il C.U.I. (codice univoco identificativo), che è un cifrato alfanumerico direttamente associato all'identificazione biometrica. L'elemento biometrico diventa il "criterio" di identificazione univoca del soggetto, in grado di seguirlo per l'intera vita ed a prescindere dalle generalità (difformi) dichiarate dal soggetto, ovvero nel caso di *alias*.

Nel caso di fotosegnalamenti successivi, l'attività di riscontro nel sistema A.F.I.S. restituirà, proprio in associazione al C.U.I., l'elenco, cronologicamente ordinato, dei precedenti dattiloscopici del soggetto.

Oltre alle impronte digitali occorre considerare un altro tipo di impronte, o meglio tracce, altrettanto fondamentali da un punto di vista investigativo e processuale: quelle biologiche, che evidenziano il DNA (acido desossiribonucleico) di un soggetto.

Il DNA può essere definito come una grande molecola composta da nucleotidi a cui è affidata la codificazione delle informazioni genetiche: tutte le cellule del nostro corpo hanno lo stesso DNA (ad eccezione di quelle riproduttive).

Anche in Italia, con l'introduzione della L. 30 giugno 2009, n. 85⁶, è stata prevista la creazione di una banca-dati nazionale del DNA, con la previsione, all'art. 11, dell'inserimento dei profili genetici solo se provenienti da laboratori accreditati a norma UNI EN ISO/IEC 1705, i cui protocolli, rispettando lo standard di analisi internazionale, sono verificati da un soggetto terzo: l'Ente nazionale di accreditamento, in Italia, Accredia.

E' soltanto nel 2017 che entra in funzione in Italia la banca-dati del DNA che raccoglie tre diverse categorie di profili del DNA⁷: i profili del DNA di persone

⁶ L'attuazione della Legge 30 giugno 2009, n. 85 che ha istituito la banca dati nazionale del DNA si è avuta con il decreto del Presidente della Repubblica del 7 aprile 2016, n. 87. Con il decreto del Ministero dell'interno dell'8 novembre 2016 sono state definite le procedure per il trattamento dei dati da parte della banca dati nazionale del DNA e del laboratorio centrale per la banca dati nazionale del DNA e per la trasmissione del profilo del DNA da parte dei laboratori di istituzioni di elevata specializzazione. Con il decreto del Ministero dell'interno del 12 maggio 2017 sono state definite le modalità di cancellazione dei profili del DNA, di distruzione dei campioni biologici, di immissione e aggiornamento dei dati necessari ai fini della determinazione dei tempi di conservazione dei medesimi profili del DNA. Con il decreto del Ministero dell'interno del 24 maggio 2017, in attuazione dell'articolo 53, co. 3 del decreto legislativo del 30 giugno 2003, n. 196, sono stati individuati i trattamenti dei dati personali contenuti nella Banca Dati Nazionale del DNA individuati alla scheda n. 6. Lo scopo della banca dati in questione ha la finalità di agevolare l'identificazione degli autori dei delitti, delle persone scomparse e per le finalità di collaborazione internazionale di polizia (artt. 5 e 12 della L. 30 giugno 2009, n. 85). Il trattamento dei dati personali relativo al profilo del DNA è ricavato dai soggetti sottoposti alla custodia cautelare in carcere o quella degli arresti domiciliari; dai soggetti arrestati in flagranza di reato o sottoposti a fermo di indiziato di delitto; dai soggetti detenuti o internati a seguito di sentenza irrevocabile, per un delitto non colposo; dai soggetti nei confronti dei quali sia applicata una misura alternativa alla detenzione a seguito di sentenza irrevocabile, per un delitto non colposo; dai soggetti ai quali sia applicata, in via provvisoria o definitiva, una misura di sicurezza detentiva. La tipizzazione del DNA dei predetti soggetti può essere effettuata esclusivamente se si procede nei confronti dei soggetti per delitti, non colposi, per i quali è consentito l'arresto facoltativo in flagranza. Nel caso di arresto in flagranza di reato o di fermo di indiziato di delitto, il prelievo è effettuato dopo la convalida da parte del giudice. Il Titolare del trattamento dei dati della Banca dati nazionale del DNA ai sensi dell'articolo 26, co. 3 del decreto del Presidente della Repubblica del 7 aprile 2016, n. 87 è il Ministero dell'interno. Al Garante per la protezione dei dati personali è attribuito il controllo sulla banca dati nazionale del DNA, nei modi previsti dalla legge e dai regolamenti vigenti, ai sensi dell'art. 15 della L. 30 giugno 2009, n. 85.

⁷ Con il d.P.R. del 7 aprile 2016, n. 87, vengono stabilite le regole per la gestione, la tipizzazione e la conservazione dei campioni biologici nell'archivio genetico, in modo da tutelare sia l'attendibilità dei dati

note detenute o arrestate; i profili del DNA ignoti delle scene del crimine; i profili del DNA delle persone scomparse o di loro congiunti e resti umani. Tranne che in quest'ultimo precipuo caso, è chiaro che l'attività della banca-dati è quella di raffrontare i profili del DNA delle persone note (detenute o arrestate) con quelli ignoti ricavati dalle scene del crimine, al fine di facilitare l'identificazione degli autori di delitti, come previsto dalla stessa legge istitutiva, all'art. 5, co. 1⁸.

Da un punto di vista strettamente tecnico e non investigativo, un riscontro positivo (*match* o *hit*) in banca-dati significa logicamente che il DNA estrapolato da una traccia biologica acquisita sulla scena del crimine è lo stesso della persona presente nella banca-dati⁹; ricercarne, invece, il coinvolgimento nel fatto di reato è, altrettanto logicamente, compito dell'investigatore.

acquisiti che la riservatezza dei soggetti a cui questi appartengono. Sul punto, si rinvia a FELICIONI, *Il regolamento di attuazione della banca dati nazionale del DNA: scienza e diritto si incontrano*, in *Dir. pen. e proc.*, 2016, 724; FANUELE, *Il regolamento attuativo della banca dati nazionale del DNA: nuove garanzie e preesistenti vuoti di tutela*, in *Proc. pen. giust.*, 2017, 1, 121.

⁸ Il DNA di ciascuna persona è composto da 22 cromosomi e da una coppia di cromosomi sessuali: XY, nel caso di DNA maschile, ed XX nel caso di DNA femminile. Ciascuna coppia deriva da un cromosoma di origine paterna e uno di origine materna. Questo significa che durante l'analisi di ogni singolo punto, detto *locus*, del DNA analizzato, si traduce in due diversi valori, uno di origine paterna e uno di origine materna. L'impronta genetica è quindi una sequenza di coppie di numeri per ogni punto del DNA analizzato a partire o dal campione biologico riferito ad una persona nota o da un reperto biologico ignoto acquisito sulla scena del crimine. Una sequenza di 23 punti del DNA, in pratica, si traduce in una sequenza di 46 numeri. L'unico caso di dubbio identificativo resta nell'ipotesi dei cosiddetti gemelli identici: provenendo dallo stesso ovulo e spermatozoo (monozigoti) che però in una delle prime fasi della vita si è diviso, ci troviamo di fronte a due individui geneticamente identici, dello stesso sesso e con lo stesso DNA.

⁹ Più di recente in argomento v. FANUELE, *La prova del DNA*, in *Prova scientifica e processo penale*, a cura di Canzio e Luparià Donati, Milano, 2025, 623.

3. *Segue: identificazione di polizia giudiziaria.* L'identificazione di polizia giudiziaria ai sensi dell'art. 349 c.p.p., costituisce il prodromo logico di ogni successivo atto di indagine e riguarda sia l'indagato che le persone che possono riferire circostanze utili per la ricostruzione dei fatti¹⁰.

L'art. 349 c.p.p., contempla un'attività tesa alla verifica della corrispondenza della reale identità di un soggetto rispetto a quella dichiarata¹¹. Nello specifico, gli ufficiali e gli agenti di polizia giudiziaria sono tenuti ad invitare la persona sottoposta alle indagini ad indicare le generalità e tutte le altre notizie utili per la sua completa identificazione: dunque, un concetto ampio di identificazione perché comprende non soltanto il "chi è" di un soggetto, ma anche il "cosa è", cioè le sue qualità, la professione che svolge, etc.

In particolare, l'indagato, dopo la richiesta di esibizione di un valido documento di riconoscimento, deve essere invitato a dichiarare le proprie generalità nonché ad indicare eventuali pseudonimi o soprannomi, la situazione patrimoniale, le condizioni di vita individuale, familiare e sociale, la sottoposizione ad altri processi penali, le condanne riportate nello Stato o all'estero e, laddove risulti necessario, a fornire notizie su eventuali uffici, servizi o cariche pubbliche ricoperte (art. 21 disp. att. c.p.p.).

Tali dichiarazioni rappresentano un obbligo penalmente sanzionato (artt. 495 e 651 c.p.) per cui i soggetti interessati devono essere ammoniti circa le

¹⁰ Cfr. COLANGELI, *Identificazione*, in *Dig. pen.*, VI, Torino, 1992, 66; CURTOTTI, *Rilievi e accertamenti tecnici sulla persona tra coazione fisica e garanzie individuali*, Padova, 2013, 111 ss.

¹¹ Cfr., MANGANELLI-F. GABRIELLI, *Investigare*, Padova, 2007, 77.

conseguenze a cui si espone colui che si rifiuta di fornire le proprie generalità o rende dichiarazioni false; i dati relativi alle proprie generalità, infatti, esulano dall'area del diritto di difesa e del diritto al silenzio, configurandosi alla stregua di un ineludibile dovere di collaborazione nei confronti dell'autorità procedente.

La polizia giudiziaria può effettuare sulla persona sottoposta alle indagini (non però su altri soggetti), ove occorra, rilievi dattiloscopici, fotografici e antropometrici e tutti gli altri accertamenti utili; l'inciso «ove occorra», impiegato quale condizione legittimante l'identificazione tramite rilievi e accertamenti, può riguardare tanto la qualità del soggetto, così applicandosi in relazione agli apolidi, agli stranieri, a persone prive di documenti, o a latitanti e pregiudicati, quanto il dubbio sull'autenticità dei documenti forniti o delle dichiarazioni rese. Questi rilievi e accertamenti presentano una valenza squisitamente indiziaria.

Con i rilievi descrittivi, fotografici e dattiloscopici del soggetto avviene l'attività di fotosegnalamento. Come già evidenziato, essi sono descrittivi in quanto espongono i caratteri di un soggetto, fotografici poiché rappresentano fotograficamente siffatti caratteri e dattiloscopici che consistono nel prelievo delle impronte delle falangi e dei palmi delle mani.

In concreto, l'attività consistente in rilievi e accertamenti si traduce in operazioni di natura prevalentemente materiale. Sul punto, secondo la Corte costituzionale, eccezion fatta per le ispezioni personali, vietate alla polizia giudiziaria, tutti i rilievi che riguardino l'aspetto esteriore della persona risultano

compatibili con il valore della libertà personale, in quanto non consistenti in una restrizione psico-fisica collidente con l'art. 13 Cost.¹²

Così argomentando, ben si comprende la disciplina contenuta nell'art. 349, co. 2-*bis* c.p.p., introdotto dall'art. 10, co. 1 d.l. 27 luglio 2005, convertito nella L. 31 luglio 2005, n. 155 (Misure urgenti per il contrasto al terrorismo internazionale), secondo cui, partendo dal presupposto che per l'acquisizione di campioni biologici occorre il consenso della persona interessata, in assenza di tale assenso si consente alla polizia giudiziaria di procedere coattivamente al

¹² Corte cost., 27 marzo 1962, n. 30, secondo cui i «rilievi descrittivi, fotografici e antropometrici possono richiedere talvolta complesse indagini che potrebbero incidere sulla libertà fisica o morale della persona: si pensi ai casi, non cervellotici di fronte allo sviluppo della scienza e della tecnica, di rilievi che richiedessero prelievi di sangue o complesse indagini di ordine psicologico o psichiatrico. Più frequentemente quei rilievi possono rendere necessari accertamenti che vengano a menomare la libertà morale della persona, come, per esempio, nel caso in cui debbano essere compiuti su parti del corpo non esposte normalmente alla vista altrui, e specialmente nel caso in cui ciò possa importare un mancato riguardo all'intimità o al pudore della persona. In altri casi i rilievi descrittivi, fotografici ed antropometrici, e sempre i rilievi dattiloscopici (almeno nella forma in cui sono attualmente eseguiti in ogni paese del mondo), non importano menomazione della libertà personale, anche se essi possano talvolta richiedere una momentanea immobilizzazione della persona per descriverne o fotografarne o misurarne gli aspetti nelle parti normalmente esposte all'altrui vista o richiedere una momentanea costrizione tendente alla fissazione delle impronte digitali. A ben guardare, la sostanziale differenza tra i due ordini di casi sopra esposti non consiste tanto nella momentaneità o nella levità della eventuale coercizione quanto, essenzialmente, nel fatto che nel secondo ordine di casi i rilievi, pur avendo per oggetto la persona, riguardano l'aspetto esteriore della persona, la cui sfera di libertà resta integra, mentre nel primo i rilievi importano una menomazione della libertà della persona pari a quella dell'arresto. In definitiva, l'esecuzione dei rilievi esteriori costituisce soltanto una forma di prestazione imposta, al fine della prevenzione dei reati, a certi individui che si trovino in determinate condizioni previste dalla legge, mentre i rilievi che assoggettino la persona a sostanziali restrizioni, fisiche o morali, di libertà, equiparabili all'arresto, sono da comprendere tra le ispezioni personali previste dall'art. 13 della Costituzione». In tema è opportuno richiamare l'intervento della Corte costituzionale: Corte cost., 9 luglio 1996, n. 238, il giudice delle leggi ha dichiarato l'illegittimità costituzionale dell'art. 224, co. 2 (seconda proposizione), del codice di procedura penale, nella parte in cui consente misure restrittive della libertà personale finalizzate alla esecuzione della perizia, ed in particolare il prelievo ematico coattivo, senza determinare la tipologia delle misure esperibili e senza precisare i casi ed i modi in cui esse possono essere adottate; tale sentenza fonda sul fatto che il prelievo ematico da eseguire coattivamente in mancanza di consenso della persona sottoposta all'esame peritale è un atto invasivo della sfera corporale sia pure in misura minima.

prelievo di capelli o saliva, previa autorizzazione (anche orale, poi confermata per iscritto) data dal pubblico ministero; fermo restando l'obbligo, in ogni caso, di eseguire l'operazione nel rispetto della dignità umana.

Occorre, inoltre, precisare che, in virtù dell'art. 4 *quater* della predetta normativa in materia di contrasto al terrorismo, il prelievo coattivo trova applicazione anche nell'ambito delle procedure di identificazione per motivi di polizia di sicurezza di cui all'art. 11, L. 18 maggio 1978, n. 191, il quale, come già specificato, attribuisce agli ufficiali ed agenti di polizia il potere di accompagnare nei propri uffici coloro i quali si rifiutino di dichiarare le proprie generalità o vi siano sufficienti indizi per ritenere che le dichiarazioni fornite siano false ovvero siano falsi i documenti esibiti, e di trattenerli per il tempo strettamente necessario per la loro identificazione e, comunque, non oltre le 24 ore (il c.d. fermo per identificazione).

A causa dell'invasività di simili rilievi sulla persona e i conseguenti dubbi di legittimità costituzionale che continuano a sollevarsi in materia (per violazione dell'art. 13, co. 2 Cost.)¹³ nonostante l'intervento chiarificatore della

¹³ Sui profili di incostituzionalità dell'art. 349, co. 2-bis c.p.p., v. KOSTORIS, *Prelievi biologici coattivi*, a cura di Kistoris-Orlandi, *Contrasto al terrorismo interno e internazionale*, Torino, 2006, 336; LUPARIA, *Attività di indagine a iniziativa della polizia giudiziaria*, in Spangher, *Trattato*, III, 180; UBERTIS, *Attività investigativa e prelievo di campioni biologici*, in *Cass. pen.*, 2008, 8; ZACCHÈ, *Gli effetti della giurisprudenza europea in tema di privilegio contro le autoincriminazioni e diritto al silenzio*, in *Giurisprudenza europea e processo penale italiano*, a cura di Balsamo-Kistoris, Torino, 2008, 179.

giurisprudenza costituzionale¹⁴, la disciplina sui prelievi biologici coattivi prevista dall'art. 349 c.p.p., deve essere interpretata restrittivamente¹⁵.

Anzitutto, deve ritenersi che tale strada per l'identificazione dell'indagato possa essere percorsa soltanto qualora allo stesso risultato non sia possibile giungere attraverso altri metodi identificativi, dotati di minore capacità coattiva. In secondo luogo, occorre tener presente che si tratta di un prelievo forzoso oggettivamente vincolato: la polizia, cioè, può prelevare solo il materiale organico espressamente indicato (capelli o saliva) rappresentando la relativa indicazione normativa un *numerus clausus*, così come la stessa alternativa "capelli o saliva"; infatti, è proprio la disgiuntiva «o» utilizzata dal legislatore che orienta una tale interpretazione (si può procedere a prelevare capelli o saliva, ma non entrambi contemporaneamente).

Una conferma in tal senso sembra del resto potersi ricavare dalla sostituzione, in sede di conversione del d.l. 27 luglio 2005, n. 144, del prelievo "di materiale

¹⁴ ALESCI, *Il corpo umano fonte di prova*, Padova, 2017; Id., *Corpo dell'imputato (fonte di prova nel processo penale)*, in *Dig. pen.*, agg., X, Torino, 2018, 76 ss., secondo cui gli standard di garanzia costituzionali in materia di libertà personale, invece di «essere "indicati tassativamente dalla legge", come prescrive l'art. 13, co. 3 Cost., [per cui] i casi in cui la polizia giudiziaria può procedere al prelievo di capelli o saliva sono "diluiti" all'interno di una formulazione evanescente e indeterminata»; in tema v. CURTOTTI, *Rilevi ed accertamenti tecnici sulla persona tra coazione fisica e garanzie individuali*, cit., 110 ss.; C. GABRIELLI, *Il prelievo coattivo di campioni biologici, nel sistema penale*, Torino, 2012, 51.

¹⁵ In questo quadro di riflessione, anche in altri contesti processuali (diversi dalla mera identificazione) mediante lo strumento dell'IA di riconoscimento di dati biometrici e genetici si potrebbe, a seconda del caso concreto, attenuare il ricorrere agli strumenti particolarmente invasivi che incidono sulla libertà personale quando non vi è il consenso della persona (il prelievo di capelli, di peli o mucosa orale per perizie o consulenze tecniche ai fini della determinazione del profilo del dna), oltre al fatto che usando il corpo umano come fonte investigativa e/o probatoria sullo sfondo permangono i dubbi sul dato che l'indagato ha il diritto a non autoincriminarsi e dovrebbe avere il diritto di impedire un prelievo forzoso sul proprio corpo, dal cui accertamento risulta un elemento a sé sfavorevole.

biologico del cavo orale” con il diverso sintagma “capelli o saliva” trasfuso nell’art. 349, co. 2-*bis* c.p.p.; una modifica operata, verosimilmente, al fine di offrire alla polizia giudiziaria una concreta alternativa facilmente praticabile, anche tenuto conto che il prelievo di un capello è da ritenere, almeno in linea di principio, meno invasivo del prelievo di saliva.

Il prelievo coattivo, inoltre, risulta essere teleologicamente e soggettivamente vincolato: esso, cioè, serve solo all’identificazione e può essere svolto solo sull’indagato. Quanto al primo profilo, è ragionevole ritenere che i risultati che scaturiscono dal prelievo coattivo non debbano rivestire alcuna valenza ulteriore rispetto a quella identificativa, riscontrando così la sola corrispondenza tra identità fisica ed identità anagrafica. Per quanto riguarda, invece, il vincolo soggettivo, l’unico destinatario di tale operazione è la persona nei cui confronti vengono svolte le indagini, prescindendosi dal relativo consenso.

Su questo terreno, però, potrebbe porsi il seguente interrogativo: il fatto che la mancanza del consenso dell’indagato sia irrilevante ai fini della realizzazione del prelievo può indurre a ritenere che la polizia possa esimersi dal richiederlo? Invero, l’esplicito riferimento normativo alla dignità della persona da identificare porta a ritenere che quest’ultima dovrebbe essere comunque informata sulle finalità del prelievo e, conseguentemente, sul fatto che può prestare consenso e che in caso contrario si procederà a prescindere dal medesimo. La giurisprudenza, peraltro, ha sostenuto che l’acquisizione del materiale biologico al fine delle indagini, e in particolare per l’accertamento del DNA, che non comporti modalità coattive, deve ritenersi pienamente legittima, anche se

avvenuta all'insaputa dell'indagato, non determinando alcuna incidenza sulla sfera di libertà¹⁶.

Il limite della dignità della persona, in realtà, potrebbe (dovrebbe) operare anche sotto altro profilo. E' noto il ruolo assunto dai mass-media negli ultimi anni relativamente ai fatti di cronaca. L'interesse, quasi morboso, dimostrato dalle testate televisive e giornalistiche per la cronaca nera, l'eccesso di informazione che viene data già nella delicata fase delle primissime indagini, attesta, probabilmente, la necessità che gli organi inquirenti mantengano il più stretto riserbo, evitando "fughe di notizie", e che svolgano le operazioni di prelievo in maniera tale da salvaguardare la riservatezza del soggetto da identificare; l'essere sottoposto ad un prelievo biologico, infatti, potrebbe essere interpretato in chiave colpevolista, come affermazione di responsabilità della persona nei cui confronti vengono svolte le indagini, e non come accertamento sull'identità.

Da un punto di vista operativo, il legislatore ha disciplinato analiticamente anche l'ipotesi in cui la persona sottoposta alle indagini o le altre persone a conoscenza di circostanze utili per la ricostruzione dei fatti non intendano sottoporsi all'identificazione, oppure forniscano generalità o documenti di identificazione in relazione ai quali sussistono sufficienti elementi per ritenerne la falsità (art. 349, co. 4 c.p.p.), prevedendo uno specifico accompagnamento presso gli uffici di polizia.

¹⁶ In tal senso, Cass., Sez. I, 23 ottobre 2008, Tripodi, in *Guida dir.*, 2009, I, 95. Tale principio, ha precisato il giudice di legittimità, va ribadito, a maggior ragione, quando il prelievo (nella specie di saliva) non sia avvenuto all'insaputa dell'indagato, ma con il suo consenso, restando in proposito processualmente del tutto privo di rilievo che all'indagato non sia stata comunicata dagli inquirenti la specifica finalità del prelievo.

Il soggetto, in questo caso, deve essere trattenuto per il tempo strettamente necessario per l'identificazione e, comunque, non oltre le 12 ore; occorre, sul punto, precisare che, a seguito della già accennate modifiche apportate dal d.l. 27 luglio 2005, n. 144 convertito nella L. 31 luglio 2005, n. 155 (Misure urgenti per il contrasto al terrorismo internazionale) attualmente la polizia giudiziaria può trattenere la persona da identificare nei propri uffici non oltre le 24 ore quando l'identificazione risulti particolarmente complessa (e qui il pensiero va proprio al prelievo coattivo di capelli e saliva) oppure nell'ipotesi in cui si renda necessaria l'assistenza dell'autorità consolare o di un interprete; in questo caso, la persona trattenuta per l'identificazione può chiedere che venga dato avviso ad un familiare o un convivente.

Dato per scontato che la norma possa riferirsi anche a persone che ancora non risultino formalmente sottoposte ad indagini, presupponendo tale "qualità" proprio l'atto di identificazione, il legislatore ha apposto una duplice forma di controllo, affidata al pubblico ministero: da un lato, immediatamente informato dell'accompagnamento e dell'ora di esso, egli può ordinare il rilascio della persona qualora ritenga mancanti le condizioni legittimanti (art. 349, co. 5 c.p.p.); dall'altro, al pubblico ministero deve essere data notizia anche del rilascio della persona accompagnata, con specificazione dell'ora in cui ciò ha avuto luogo (art. 349, co. 6 c.p.p.).

4. *Intelligenza artificiale ed identificazione facciale.* La nascita dell'intelligenza artificiale è riconducibile ad un lavoro pubblicato nel 1943, ove si prospettava

uno dei primi modelli matematici di un neurone artificiale¹⁷. In questo modello¹⁸, ogni *input* viene moltiplicato per il suo peso, i risultati vengono sommati, e poi questa somma passa attraverso una funzione di attivazione per produrre l'*output*. Questo processo è alla base del funzionamento dei neuroni artificiali nelle reti neurali. Sulla natura dell'intelligenza delle macchine (le macchine sono in grado di pensare?) il matematico e decrittatore Turing propose di guardare al comportamento esteriore (manifestazione) delle macchine, dato che anche la vita interiore dell'uomo è inconoscibile, puntando a misurare l'intelligenza sul risultato prodotto dalle stesse. Egli proponeva il "gioco dell'imitazione" e, quindi, ove gli osservatori non erano in grado di distinguere il comportamento della macchina da quello dell'uomo, allora questa doveva essere ritenuta intelligente (test di Turing)¹⁹.

L'espressione «intelligenza artificiale» è, invece, da attribuire al matematico McCarthy²⁰, il quale insieme ad altri scienziati voleva dimostrare che era possibile costruire una macchina in grado di simulare la conoscenza umana²¹, con

¹⁷ MCCULLOCH-PITTS, *A logical calculus of the ideas immanent in nervous activity*, in *The Bulletin of mathematical biophysics*, 1943, 5, 115-133.

¹⁸ Questo semplice modello somma i segnali di ingresso (*input*) ricevuti, li pondera (asigna loro pesi) e utilizza una funzione di attivazione per determinare l'*output*. Se la somma ponderata supera una certa soglia, il neurone si "attiva" e produce un *output*. In tema, v. NIELSEN, *Neural networks and deep learning*, 2015; CHARU, *Neural networks and deep learning*, 2024.

¹⁹ TURING, *Computing Machinery and intelligence*, in *Mind*, LIX, 1950, 433-460.

²⁰ MCCARTHY e altri, *A proposal for the Dartmouth Summer Research Project in Artificial Intelligence*, sottoposta alla Rockefeller Foundation, 1955, ristampa in *AI Magazine*, XXVII, 2006.

²¹ MCCARTHY e altri, *A proposal for the Dartmouth Summer Research Project in Artificial Intelligence*, cit. Tali scienziati ipotizzarono uno studio sulla «congettura per cui ogni aspetto dell'apprendimento o qualsiasi altra caratteristica dell'intelligenza è, in linea di principio, descrivibile con precisione tale da poter costruire una macchina capace di simularla».

l'aspirazione che le macchine sarebbero state in grado di fare qualsiasi lavoro che un uomo sa fare.

Nonostante l'evoluzione nel campo dell'informatica che si è avuta dal 1950 ad oggi, con la creazione di intelligenze artificiali che pareggiano o superano i risultati umani in forza del potenziamento di algoritmi di apprendimento automatico, che sono differenti dagli algoritmi classici²², manca nello “strumento informatico” l'ingrediente naturale dell'emotività, dell'empatia e della riflessione umana; in questo senso, perciò, il ragionamento dell'uomo non è tecnologicamente imitabile o assimilabile con approcci o metodi matematici (si pensi, stando al nostro campo di interesse, alla valutazione complessiva del giudice ai fini di una decisione sulla responsabilità di un fatto illecito).

Discorso diverso si potrebbe imbastire per l'assistenza al giudice nei giudizi in virtù del progresso tecnologico; in tal caso però l'intelligenza artificiale deve essere in grado di “spiegare” come è giunta alle proprie conclusioni²³, ove determinati *software* – oggi o domani – siano in grado di evidenziare i passaggi logici del risultato prodotto.

Da questo punto di vista l'intelligenza artificiale generativa sta progredendo in maniera sorprendente ed imprevedibile: in questo senso si pensi ai principali

²² Gli algoritmi classici consistono in operazioni per produrre risultati precisi e prevedibili (sulla base di *input* e *output* esatti); gli algoritmi dell'apprendimento automatico invece consistono in operazioni dirette a produrre miglioramenti sulla base di risultati imprecisi.

²³ MENNA, *Intelligenza artificiale e controllo contenutistico delle “forme” di produzione dei suoi outputs conoscitivi*, in *Arch. pen.*, 3, 2024, secondo cui in termini di verifica logico formale, rispetto all'intelligenza generativa, bisognerebbe concentrarsi non tanto sul riscontro *ex ante* della macchina, visto che il percorso di connessioni logico formali e le analogie operate dal sistema operativo mutano, ma sulla possibilità di riscontro *ex post* del percorso conoscitivo operato dalla macchina.

modelli di AI generativa diventati modelli di *reasoning*. Questi nuovi modelli – di *reasoning* linguistici – non generano solo il testo, non si limitano a recuperare informazioni o a basarsi su quanto “afferrato” nel percorso dell’addestramento, ma sono programmati per simulare un processo di ragionamento, vale a dire ricostruiscono i passaggi intermedi, raggiungendo una conclusione logica più comprensibile.

Tra le principali tecniche di *reasoning* vi sono quelle che consentono al modello di scomporre il problema ed evidenziare i passaggi intermedi che lo portano alla soluzione (*chain-of-thought*); quelle che portano il modello a creare ragionamenti alternativi e a scegliere quello più convincente riducendo errori e allucinazioni (*self-consistency*); quelli che sulla scorta di una tecnica più evoluta consentono di esplorare diversi segmenti di ragionamento, valutando quale di essi porta al miglior risultato.

Siffatti modelli, con queste tecniche, ci fanno comprendere che gli strumenti di IA ci forniscono non solo il risultato, ma anche il “percorso logico” da loro seguito, con la possibilità di avere un effettivo controllo umano in chiave di identificazione e correzione dei passaggi critici, fermo restando che ad oggi questi modelli possono ancora commettere errori in calcoli complessi e richiedere più risorse computazionali, incidendo sulla velocità del sistema; ancora, il modello può apparire affidabile anche quando il ragionamento contiene errori logici difficili o non facili da rilevare (ad esempio il testo generato dà

un'impressione di coerenza e correttezza anche quando i passaggi logici non lo sono)²⁴.

L'intelligenza artificiale potrebbe apportare, quindi, dei contributi in ambito processuale²⁵, ma non potrebbe svolgere determinate funzioni giurisdizionali, se non in contrapposizione ai valori fondamentali²⁶. Nello specifico non è

²⁴ In tema si rinvia a WEI-WANG-SCHUURMANS, et al., *Chain-of-Thought Prompting Elicits Reasoning in Large Language Models*, 2022; HUANG-CHANG, *Towards Reasoning in Large Language Models: A Survey*, 2022; PLAAT-WONG-VERBERNE, et al., *Reasoning with Large Language Models: A Survey*, 2024; HONG-PANG-ZHANG, *Advances in Reasoning by Prompting Large Language Models: A Survey. Cognitive Artificial Intelligence*, 2023; LIU-FU, et al., *Logical Reasoning in Large Language Models: A Survey*, 2025.

²⁵ ALGERI, *Intelligenza artificiale e polizia predittiva*, in *Dir. pen. proc.*, 2021, 724; CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale*, in *Sist. pen.*, 2021; FINOCCHIARO, *Intelligenza Artificiale e protezione dei dati personali*, in *Giur. it.*, 2019, 1676; QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Springer, Berlin, 2020; ID., *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgenza discussione tra scienze penali e informatiche*, in www.lalegislazionepenale.eu, 2018; ID., *Equo processo penale e slide della società algoritmica*, in *BioLaw Journal*, 2019, 1, 135 ss.; RICCIO, *Ragionando su intelligenza artificiale e processo penale*, in *Arch. pen.*, 2019, 3; RUFFOLO, *Artificiale, machine learning e responsabilità da algoritmo*, in *Giur. it.*, 2019, 1689; SANTOSUOSSO, *Intelligenza artificiale e diritto*, Milano, 2020.

²⁶ Sull'intelligenza predittiva e riflessione sui valori fondamentali cfr., UBERTIS, *Intelligenza artificiale e giustizia predittiva*, in *Sist. pen.*, 2023. Sulle diverse criticità della giustizia predittiva v., altresì, il recente contributo di AA.VV., *Intelligenza artificiale e processo penale*, a cura di Di Paolo e Presacco, Trento, 2022 (con contributi di QUATTROCOLO, DELLA TORRE, LASAGNI, PRESACCO, MALDONATO e di BARONE), *Giustizia predittiva e certezza del diritto*, Roma, 2024, 9 ss.; sul tema cfr. anche BARONE, *Intelligenza artificiale e processo penale: la linea dura del parlamento europeo. Considerazioni a margine della risoluzione del parlamento europeo del 6 ottobre, 2021*, in *Cass. pen.*, 2022, 3, 1182; CONTISSA, LASAGNI, SARTOR, *Quando a decidere in materia penale sono (anche) gli algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Riv. trim. diritto di internet*, 2009, 4, 619 ss.; GIALUZ, *Quando il processo penale incontra l'intelligenza artificiale: luci ed ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *Sist. Pen. (web)*, 2019; KOSTORIS, *Predizione decisoria, diversione processuale e archiviazione*, in *Sist. Pen.*, 2021, 1 ss.; ID., *Intelligenza artificiale, strumenti predittivi e processo penale*, in *Discrimen*, 5 febbraio 2024, 1 ss.; LUPARIA DONATI, *Prova giudiziaria e ragionamento artificiale: alcune possibili chiavi di lettura*, in *Il concetto di prova alla luce dell'intelligenza artificiale*, a cura di Sallantin e Szczechiniarz, Milano, 2005; PAULESU, *Intelligenza artificiale e giustizia penale. Una lettura attraverso i principi*, in *Arch. pen.*, 2022, 1; POLIDORO, *Tecnologie informatiche e procedimento penale: la giustizia penale "messa alla prova" dall'intelligenza artificiale*, in *Arch. pen.*, 2020, 3, 1 ss.; QUATTROCOLO, *Equità del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell'uomo*, in *Revista Italo-*

possibile che lo strumento dell'intelligenza artificiale in via autonoma condanni o assolva sulla base dei dati acquisiti nel processo, perché la sensibile percezione dell'uomo ai fini valutativi dei dati probatori comunicativi e rappresentativi non è sostituibile da metodi matematici-algoritmi, giacché il momento valutativo non va confuso con l'acquisizione specifica di un *output* sottoposto a critica e valutazione in funzione dell'oggetto del giudizio (artt. 25 co. 1, 111 co. 6, 111 co. 2 e 101 co. 1 Cost.).

L'impiego di «strumenti di IA può fornire sostegno al potere decisionale dei giudici o all'indipendenza del potere giudiziario, ma non dovrebbe sostituirlo: il processo decisionale finale deve rimanere un'attività a guida umana»²⁷. La L. 23 settembre 2025, n. 132 (disposizioni e deleghe al Governo in materia di IA) all'art. 15 prevede che nei casi dei sistemi di intelligenza artificiale nell'attività giudiziaria è sempre riservata al magistrato ogni decisione sull'interpretazione

Espanola de Derecho Procesal, 2019, 2 ss.; MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in *Discrimen*, 15 maggio 2020, 1; NAGNI, *Artificial intelligence, l'innovativo rapporto di (in)compatibilità tra machina sapiens e processo penale*, in *Sist. pen.*, 2021, 7, 5 ss.; SCERBO, *Equilibrio tra esigenze di tutela della sicurezza collettiva e tutela delle libertà fondamentali. Nuove tecnologie nella giustizia penale? A.I. (artificial intelligence), Trojan horse (captatore informatico) e gestione dei dati da parte dell'autorità come case studies*, in *Arch. pen.*, 2004, 1, 1 ss.; SIGNORATO, *Giustizia penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo*, in *Riv. dir. proc.*, 2020, 605; ID., *Il diritto a decisioni penali non basate esclusivamente su trattamenti automatizzati: un nuovo diritto derivante dal rispetto della dignità umana*, *ivi*, 2021, 101.

²⁷ In tal senso, il Considerando n. 61 del regolamento UE 2024/1689 del Parlamento europeo e del Consiglio; in tale considerando è spiegato però che non è «opportuno estendere la classificazione dei sistemi di IA come ad alto rischio ai sistemi di IA destinati ad attività amministrative puramente accessorie, che non incidono sull'effettiva amministrazione della giustizia nei singoli casi, quali l'anonimizzazione o la pseudonimizzazione di decisioni, documenti o dati giudiziari, la comunicazione tra il personale, i compiti amministrativi». Secondo l'allegato III n. 8 del citato regolamento sono ad alto rischio i sistemi che riguardano l'amministrazione della giustizia e processi democratici: «i sistemi di IA destinati a essere usati da un'autorità giudiziaria o per suo conto per assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti, o a essere utilizzati in modo analogo nella risoluzione alternativa delle controversie».

e sull'applicazione della legge, sulla valutazione dei fatti e delle prove e sull'adozione dei provvedimenti²⁸.

Sostanzialmente l'IA è uno strumento che produce un risultato valutabile dal giudice sul terreno della verifica logico formale. Dalla L. 23 settembre 2025, n. 132, però, non si evincono i poteri di controllo del giudice sullo strumento in questione, né i divieti per acquisire e valutare i risultati prodotti dai sistemi di intelligenza artificiale²⁹.

L'intelligenza artificiale non sostituisce quella naturale o autentica, giacché la stessa è frutto di quella umana ed è uno strumento tecnologico che agevola la vita dell'uomo nei diversi settori; può anche sostituire l'applicazione o l'operatività dell'uomo, ma in virtù di una sua decisione e ove sia possibile. Senza contare che anche da un punto di vista generale l'intelligenza artificiale non è in grado di comprendere il mondo, ma di elaborare dati ai fini di produrre un

²⁸ La L. 23 settembre 2025, n. 132, Disposizioni e deleghe al Governo in materia di intelligenza artificiale, in *Gazz. uff.*, n. 223, 25 settembre 2025, si affianca al regolamento (UE) 2024/1689 (AI Act), del 13 giugno 2024. Secondo l'art. 15, della citata fonte nazionale, per l'interpretazione e l'applicazione della legge, la valutazione dei fatti e delle prove e l'adozione dei provvedimenti viene esclusa la possibilità di fare ricorso all'intelligenza artificiale. Tale disposizione «non consentirebbe l'impiego dei sistemi di AI riconducibili alla c.d. "giustizia predittiva", ovvero di sistemi che, sulla base di un modello statistico elaborato in maniera autonoma dal sistema stesso a seguito dell'analisi di una mole significativa di atti giuridici, sono in grado di formulare una previsione che può giungere fino al possibile esito di un giudizio». L'originaria formulazione del testo dell'articolo 15 prevedeva l'utilizzo dei sistemi di intelligenza artificiale per le attività di ricerca giurisprudenziale e dottrinale, per le quali dovrebbe ritenersi applicabile la disciplina di cui al successivo comma 2 che prevede che il Ministero della giustizia disciplina gli «impieghi dei sistemi di intelligenza artificiale per l'organizzazione dei servizi relativi alla giustizia, per la semplificazione del lavoro giudiziario e per le attività amministrative accessorie»; sul punto, cfr. Dossier n. 289/4, XIX Legislatura, *Disposizioni e delega al Governo in materia di intelligenza artificiale*, 27 giugno 2025, *A.S. n. 1146-B*, in *www.senato.it*, 56 ss.

²⁹ Sul punto, già prima dell'approvazione definitiva della L. 23 settembre 2025, n. 132, SCALEFATI, *IA e processo penale: prospettive d'impiego e livelli di rischio*, in *Proc. pen. giust.*, 2024, 1409; CANZIO, *AI ACT e processo penale: sfide e opportunità*, in *Sist. pen.*, 2024, 11.

risultato anche al fine di supportare l'uomo nella comprensione delle cose e situazioni.

Manca una definizione di intelligenza artificiale universale³⁰, in quanto essa abbraccia l'evoluzione delle diverse conoscenze dell'uomo in vari ambiti, come la matematica, la filosofia, l'economia, la psicologia, la linguistica, l'ingegneria informatica, l'informatica giuridica, le neuroscienze, la cibernetica³¹; di qui i ricercatori procedono senza una direzione specifica e con un progredire germogliante e al tempo stesso con il rischio di sconfinamenti etici e violazioni dei diritti fondamentali.

Un tratto comune della definizione di intelligenza artificiale è oggi rinvenibile nel regolamento (UE) del Parlamento e del Consiglio europeo 2014/1689 (*AI Act*) del 13 giugno 2024³², secondo il quale un siffatto sistema è in grado di inferire (“dedurre”) determinati *output* sulla base di *input* o dati al fine di operare in virtù di obiettivi espliciti definiti o di obiettivi impliciti³³. Il verbo “inferire

³⁰ In tema cfr. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Sist. Pen.*, 2020, 2; TURNER, *Robot Rules. Regulating Artificial Intelligence*, London, 2019, 7 ss.; CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Dir. pubblico comparato ed europeo*, 2019, 102; D'ALOIA, *Il diritto verso “il mondo nuovo”. Le sfide dell'Intelligenza Artificiale*, in *Riv. bio dir.*, 2019, 1, 8; SHERER, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies and Strategies*, in *Harvard Journal of Law & Technology*, 2016, 2, 359.

³¹ Sul contributo delle diverse branche del sapere sull'evoluzione dell'intelligenza artificiale v., RUSSELL-NOVIG, *Intelligenza artificiale. Un approccio moderno*, Milano, 2021, 8 ss.

³² Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione (art. 1, regolamento UE).

³³ Cfr., regolamento (UE) del Parlamento e del Consiglio europeo 2014/1689 (*AI Act*).

o “dedurre” evidenzia la differenza tra il *software* che si limita ad eseguire una serie di istruzioni per produrre un risultato (*output*), da quello di intelligenza artificiale che si fonda su un algoritmo ed attraverso esso si realizza un’operazione di inferenza che da un punto di vista matematico e filosofico significa partire da ciò che conosciamo per arrivare ad una conclusione.

La prerogativa basilare dei sistemi di intelligenza artificiale è la capacità inferenziale. Il regolamento europeo prevede, difatti, la seguente definizione del sistema di intelligenza artificiale: «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'*input* che riceve come generare *output* quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali» (art. 3).

Per comprendere meglio tale definizione è opportuno far riferimento alle premesse introduttive di valore interpretativo (non vincolanti) del regolamento europeo. Nel considerando n. 12 del regolamento europeo è evidenziata la «capacità dei sistemi di IA di ricavare modelli o algoritmi, o entrambi, da input o dati» e quindi le «tecniche che consentono l'inferenza nella costruzione di un sistema di IA comprendono approcci di apprendimento automatico che imparano dai dati come conseguire determinati obiettivi»; tali approcci sono basati sulla logica traendo inferenze dalla conoscenza codificata o dalla rappresentazione simbolica del compito da risolvere (considerando n. 12)³⁴.

³⁴ Cfr., regolamento (UE) del Parlamento e del Consiglio europeo 2014/1689 (*AI Act*).

Così la «capacità inferenziale di un sistema di IA trascende l'elaborazione di base dei dati consentendo l'apprendimento, il ragionamento o la modellizzazione. Il termine «automatizzato» si riferisce al fatto che il funzionamento dei sistemi di IA prevede l'uso di macchine. Il riferimento a obiettivi espliciti o impliciti sottolinea che i sistemi di IA possono operare in base a obiettivi espliciti definiti o a obiettivi impliciti. Gli obiettivi del sistema di IA possono essere diversi dalla finalità prevista del sistema di IA in un contesto specifico.

Ai fini del regolamento in esame, gli ambienti dovrebbero essere intesi come i contesti in cui operano i sistemi di IA, mentre gli *output* generati dal sistema di IA riflettono le diverse funzioni svolte dai sistemi di IA e comprendono previsioni, contenuti, raccomandazioni o decisioni. I sistemi di IA sono progettati per funzionare con livelli di autonomia variabili, il che significa che dispongono di un certo grado di autonomia di azione rispetto al coinvolgimento umano e di capacità di funzionare senza l'intervento umano. «L'adattabilità che un sistema di IA potrebbe presentare dopo la diffusione si riferisce alle capacità di autoapprendimento, che consentono al sistema di cambiare durante l'uso»³⁵.

Uno strumento di identificazione di polizia giudiziaria (sistema automatizzato di riconoscimento delle immagini³⁶) che agisce sugli algoritmi elabora e riporta

³⁵ Inoltre, secondo il considerando n. 12 del regolamento (UE) del Parlamento e del Consiglio europeo 2024/1689 (*AI Act*) «I sistemi di IA possono essere utilizzati come elementi indipendenti (stand-alone) o come componenti di un prodotto, a prescindere dal fatto che il sistema sia fisicamente incorporato nel prodotto (integrato) o assista la funzionalità del prodotto senza esservi incorporato (non integrato)».

³⁶ In tema v., LOPEZ, *La rappresentazione facciale tramite software*, in Scalfati, *Le indagini atipiche*, Torino, 2019, II, 239 ss.; DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in *Sist. Pen.*, 2020.

il dato di quanti soggetti simili ci sono nella banca dati³⁷. In pratica con l'inserimento di un'immagine fotografica di un soggetto ignoto e/o sospettato il sistema presenta all'operatore di polizia giudiziaria un elenco di foto segnaletiche somiglianti ordinate in virtù di un criterio di affinità insieme ad una percentuale di *matching*.

In sostanza viene prodotta una lista di immagini con relativa indicazione della percentuale di compatibilità. Più è alta la percentuale indicata dal SARI più è probabile che il volto sottoposto al controllo corrisponda a quello contenuto nella banca dati. Dunque, il soggetto di polizia giudiziaria dovrà effettuare necessariamente degli accertamenti investigativi per verificare la corrispondenza ai fini dell'identificazione. Il risultato prodotto dal SARI è di aiuto al soggetto di polizia giudiziaria, ma non è in grado di fornire alcuna certezza in tema di identificazione della persona.

E' un sistema - prodotto - di intelligenza artificiale, poiché in forza di un *input* (dato inserito) vi è una ricerca sulla base di immagini mediante algoritmi di riconoscimento facciale, i quali si servono delle c.d. rete neurali, in modo da produrre un risultato (*output*).

La piattaforma informatica c.d. SARI *Enterprise*, oltre ad essere utilizzata dagli investigatori per le ricerche di tipo testuale su dati anagrafici, descrittivi ed elementi del segnalamento, permette anche agli operatori di inserire nella

³⁷ La piattaforma informatica SARI consente ricerche di tipo testuale su tutte le informazioni connesse al fotosegnalamento (dati anagrafici, descrittivi e circostanze del segnalamento), ma permette di effettuare ricerche sulla base di immagini mediante algoritmi di riconoscimento facciale. A tal proposito cfr., *Capitolato tecnico, procedura volta alla fornitura della soluzione integrata per il sistema automatico di riconoscimento immagini SARI*, in www.poliziadistato.it

suindicata piattaforma un'immagine estrapolata da una videoregistrazione, in modo che venga ricercata come specificato mediante il sistema di riconoscimento facciale.

Siffatto sistema avviato dal Ministero dell'interno nel 2018 ha ricevuto parere favorevole dall'Autorità garante per la protezione dei dati personali in quanto rientra nell'attività disciplinata dall'art. 349 c.p.p., poiché la ricerca è effettuata sulla base di immagini foto-segnalate e contenute nella banca dati. Il SARI *Enterprise* non realizza un nuovo reperimento di dati personali, ma rappresenta una diversa modalità automatizzata di lettura di dati che sono già nella disponibilità dell'operatore.

L'Autorità garante ha specificato, inoltre, che non si effettuano interventi ulteriori rispetto al *database* AFIS-SSA, ma vi sono alcune operazioni automatizzate invece di un inserimento manuale di connotati identificativi. Per cui non ci troviamo di fronte ad operazioni basate esclusivamente su un trattamento automatizzato di dati, che in quanto tali sarebbero vietate secondo l'art. 8 del d.lgs. 18 maggio 2018, n. 51. Il confronto avviene tra l'immagine reperita ed immessa nel sistema dagli operatori e quanto già contenuto nella banca dati.

Il garante della protezione dei dati personali, sul punto, ha evidenziato che l'operazione in discorso è di «mero ausilio all'agire umano, avente lo scopo di velocizzare l'identificazione, da parte dell'operatore di polizia, di un soggetto ricercato della cui immagine facciale si disponga, ferma restando l'esigenza

dell'intervento dell'operatore per verificare l'attendibilità dei risultati prodotti dal sistema automatizzato»³⁸.

Altro sistema è il SARI *Real-Time*. E' un tipo di sistema di riconoscimento facciale non attivo in grado di garantire dei risultati in tempo reale su più flussi video *live* provenienti da telecamere. I volti presenti nei fotogrammi dei diversi *stream* video sono analizzati e confrontati mediante un algoritmo di riconoscimento con quelli presenti in una *watch-list* (della grandezza dell'ordine delle migliaia di immagini).

Nel caso di confronto positivo (*match*) il sistema genera un *alert* che richiama l'attenzione degli operatori.

Il SARI *Real-time* è concepito, quindi, da un sistema video in grado di analizzare in tempo reale i volti dei soggetti ripresi dalle telecamere situate in punti di osservazione confrontandoli con un limite massimo di 10.000 foto-segnalistiche contenute e/o estratte da AFIS.

Il sistema memorizzerà il volto sottoposto al controllo solo in caso di esito positivo (*match*) dal confronto con le foto-segnalistiche, fermo restando che il risultato prodotto dal *software* dovrà essere riscontrato dal soggetto qualificato. Il sistema consente, inoltre, di registrare i flussi video delle telecamere fungendo come "attività di video sorveglianza".

Siffatto sistema è stato creato come soluzione mobile, in modo da poter essere installato direttamente presso il sito ove sorge l'esigenza di disporre di una tecnologia di riconoscimento facciale in grado di coadiuvare le forze di polizia

³⁸ Cfr., Provvedimento dell'Autorità garante per la protezione dei dati personali, 26 luglio 2018, n. 440.

nella gestione dell'ordine e della sicurezza pubblica, ovvero in relazione a specifiche esigenze di polizia giudiziaria, come risulta dalla descrizione e bozza valutativa di impatto inviata dal Ministero dell'interno-dipartimento di pubblica sicurezza all'Autorità garante della protezione dei dati personali.

L'Autorità garante ha espresso parere negativo, in quanto il trattamento dei dati biometrici tramite il sistema *SARI Real Time*, non risulta conforme alla disciplina di cui al decreto legislativo del 30 giugno 2003, n. 196, integrato con le modifiche introdotte dal decreto legislativo 10 agosto 2018, n. 101, in assenza di un'adeguata e specifica normativa che legittimi il riconoscimento facciale in tempo reale, dal momento che da una sorveglianza mirata di alcuni individui si passa alla possibilità di una «sorveglianza universale allo scopo di identificare alcuni individui», interferendo con la vita privata di questi³⁹.

Con il regolamento europeo è necessario analizzare questi sistemi e ragionare sul rischio degli stessi e comprendere come regolarli in ambito processuale. Nel caso, invece, di assenza di regole processuali bisogna indagare su quali siano gli effetti sul risultato prodotto dall'IA.

In sintesi lo scopo del regolamento europeo sull'intelligenza artificiale è quello di istituire regole armonizzate per lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale nell'Unione, garantendo un'innovazione tecnologica affidabile, non a discapito della protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta

³⁹ Provvedimento dell'Autorità garante per la protezione dei dati personali, n. 127, del 25 marzo 2021.

dell'unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente (considerando n. 1 e 2 del regolamento europeo *AI Act*).

Il testo del regolamento europeo si compone di 113 articoli e tredici allegati (c.d. tecnica annessa con una periodica revisione quinquennale). Il regolamento è basato su una scala di rischi, in virtù dei quali vi è una gradazione di disciplina a seconda del livello di rischio: al rischio inaccettabile vi è la previsione di attività vietate (art. 5); al rischio elevato vi è l'esigenza di valutazione di conformità e obblighi (art. 6); all'Intelligenza artificiale per finalità generali con rischio sistemico è richiesta la trasparenza più la valutazione e mitigazione dei rischi (art. 55); al rischio limitato è richiesta la trasparenza (art. 50); al rischio minimo sono previsti codici di buona condotta (art. 95).

Stando al tema di interesse, in questa sede, i sistemi di intelligenza artificiale usati ai fini delle attività di contrasto sono ritenuti ad alto rischio e di conseguenza sono vietati, ma con delle eccezioni qui riportate.

Secondo l'art 5, par. 1, lett. h) del regolamento europeo è vietato l'uso di sistemi di identificazione biometrica remota in tempo reale in spazi accessibili al pubblico ai fini di attività di contrasto a meno che siano strettamente necessari per uno dei seguenti obiettivi: la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse; la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico; la localizzazione o l'identificazione di una persona sospettata di aver commesso un

reato, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'allegato II, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni.

In tali situazioni eccezionali i sistemi di riconoscimento biometrico, mediante l'uso di intelligenza artificiale, rientrano nella classificazione di pratiche ad alto rischio, secondo le previsioni dell'art. 6 par. 2 e allegato III, par. 1, lett. a).

L'art. 5, par. 2, prevede che l'uso di sistemi di identificazione biometrica remota in tempo reale in spazi accessibili al pubblico nei casi indicati al par. 1 lett. h) può essere utilizzato soltanto per confermare l'identità della persona specificamente interessata, il cui uso deve tener conto della situazione che genera la necessità di operare con tale strumento, considerando in particolare la gravità, la probabilità e l'entità del danno che potrebbe verificarsi nella non attivazione dello stesso; ancora degli effetti dell'uso del sistema sui diritti e libertà fondamentali di tutte le persone interessate, in virtù della gravità, la probabilità e l'entità di tali conseguenze.

Il regolamento europeo richiede che lo Stato membro per l'impiego di tecnologie di riconoscimento facciale da remoto preveda una riserva di legge e di giurisdizione.

La ragione è nella tutela di diritti fondamentali. Perciò occorre che lo Stato membro faccia delle valutazioni sugli obiettivi indicati dall'art. 5, par. 1, lett. h) e preveda apposite garanzie. A questo punto che tipo di riflessione dovrebbe fare il legislatore?

Bisognerebbe ragionare sulla previsione di una richiesta motivata del pubblico ministero in relazione alla gravità del reato (determinata secondo il criterio qualitativo e quantitativo) e delle ragioni di indispensabilità alla prosecuzione dell'identificazione (vuol dire che non si possa espletare l'identificazione con gli strumenti classici previsti dall'art. 349 c.p.p.), con conseguente provvedimento del giudice delle indagini preliminari sulla scorta di questi presupposti, soddisfacendo il criterio della proporzionalità e della necessità; ancora regolare l'urgenza con convalida del predetto giudice e prevedere la cancellazione dei dati (*output*) ottenuti in mancanza di convalida, oltre che l'interruzione dell'attività in corso. Si dovrebbe stabilire, inoltre, la durata e l'indicazione del luogo per lo svolgimento dell'identificazione. Peraltro, bisognerebbe considerare che l'identificazione con intelligenza artificiale di elementi biometrici dovrebbe essere preferita al prelievo coattivo di materiale biologico (art. 349, co. 2-*bis* c.p.p.), essendo uno strumento meno invasivo nella sfera personale dell'indagato.

L'uso dello strumento ad alto rischio in questione senza che il legislatore intervenga non potrà essere impiegato in virtù del regolamento europeo, la cui attivazione determina l'inutilizzabilità dei risultati in forza di un'attività che comprime i diritti fondamentali.

Il sistema SARI *Enterprise* è, invece, meno invasivo, poiché il confronto tra i dati legittimi e contenuti nell'apposita banca dati e l'immagine inserita nel sistema ai fini identificativi è limitata ad un compito specifico, oltre a non sostituire l'intervento dell'operatore prima e dopo il risultato frutto dell'IA. Di qui,

il legislatore per tale tipologia di strumento potrebbe valutare di introdurre un'autorizzazione preventiva del pubblico ministero per l'utilizzo ai fini identificativi di cui all'art. 349 c.p.p., non aprendo una finestra di giurisdizione per l'autorizzazione. Difatti, l'art. 6, par. 3 del regolamento europeo, prevede che un sistema di IA di cui all'allegato III non è considerato pericoloso se non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone, anche nel senso di non influenzare materialmente il risultato del processo decisionale. L'importante è che il sistema di IA soddisfi almeno una delle seguenti condizioni: il sistema di intelligenza artificiale è indirizzato a eseguire un compito procedurale limitato; è volto a migliorare il risultato di un'attività umana precedentemente completata; a rilevare schemi decisionali o deviazioni da schemi decisionali precedenti e non a sostituire o influenzare la valutazione umana precedentemente completata senza un'adeguata revisione umana; a eseguire un compito preparatorio per una valutazione pertinente ai fini dei casi di cui all'allegato III.

Nel caso poi dovesse essere usato anche a conferma e/o verifica identificativa in relazione a quanto dichiarato dalla persona fisica, l'allegato III del Regolamento europeo stabilisce che non sono inclusi i «sistemi di IA destinati a essere utilizzati per la verifica biometrica la cui finalità è confermare che una determinata persona fisica è la persona che dice di essere».

Altra riflessione riguarda il quesito se i sistemi di IA ad alto rischio dovessero essere utilizzati per valutare l'affidabilità degli elementi probatori nel corso delle indagini. Tra i sistemi ad alto rischio, difatti, a norma dell'art. 6, par. 2,

rientrano quelli previsti dall'allegato III; secondo il citato allegato rientrano nel settore di rischio «i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto per valutare l'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati» (allegato III, par. 6 lett. c), del regolamento europeo *AI Act*)⁴⁰.

A questo punto i sistemi di intelligenza artificiale come il riconoscimento facciale o altro tipo di riconoscimento potrebbero essere impiegati ai fini investigativi pur essendo sistemi ad alto rischio; tra l'altro si potrebbe apportare un

⁴⁰ Altri settori indicati come sistemi di intelligenza artificiale ad alto rischio, nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso, sono: i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto o per loro conto, per determinare il rischio per una persona fisica di diventare vittima di reati; i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto, per determinare il rischio di commissione del reato o di recidiva in relazione a una persona fisica non solo sulla base della profilazione delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 o per valutare i tratti e le caratteristiche della personalità o il comportamento criminale pregresso di persone fisiche o gruppi; i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto, per effettuare la profilazione delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 nel corso dell'indagine, dell'accertamento e del perseguimento di reati (allegato III, par. 6, del regolamento europeo *IA Act*).

contributo di affidabilità all'individuazione che oggi viene fatta con una certa "superficialità"⁴¹ ed incide o toglie valore alla ricognizione⁴².

In tali casi, lo strumento investigativo per il riconoscimento facciale o altro elemento identificativo del corpo umano essendo ad alto rischio richiederebbe l'osservanza della riserva di legge e di giurisdizione per la immediata prosecuzione delle indagini. Qui, non parliamo di identificazione legata ad un aspetto formale, ma ad un riconoscimento connesso al fatto per cui si procede. Ad esempio, nel caso emblematico di un'immagine tratta da una videoregistrazione di un soggetto che sta commettendo il reato, potrebbe sorgere la necessità – ove con l'individuazione di cui all'art. 361 (individuazione personale, fotografica o dell'immagine video) non fosse possibile ottenere un soddisfacente riconoscimento – per il pubblico ministero di farsi autorizzare a ricorrere allo

⁴¹ L'individuazione secondo disposizione normativa ex art. 361 c.p.p. è un atto tipico del pubblico ministero, delegabile alla polizia giudiziaria, ed è effettuata con minori garanzie, in particolare dell'assistenza tecnica del difensore nel momento dell'individuazione (riconoscimento) della persona sottoposta alle indagini. L'espletamento poi della ricognizione in dibattimento subisce il condizionamento dell'individuazione priva di garanzie avvenuta nella fase delle indagini, in forza della capacità del cervello di immagazzinare e recuperare informazioni. Peraltro, tale osservazione a maggior ragione ha una sua rilevanza, in quanto la prassi giurisprudenziale attribuisce valore alla ricognizione informale, aprendo le porte con più leggerezza alla "ripetibilità" di un risultato investigativo: Cass., Sez. I, 17 febbraio 2016, n. 37545; Id., Sez. II, 5 maggio 2011, in *Mass. uff.*, n. 250081; Id., Sez. II, 10 aprile 1997 in *Guida dir.*, 1, 71, con nota di RIVELLO, *Anche il riconoscimento informale tra le prove atipiche ammesse dal legislatore*. In argomento v. ALESCI, *Corpo dell'imputato, (fonte di prova nel processo penale)*, cit.

⁴² Sulla ricognizione di persone cfr., CAVINI, *Le ricognizioni e i confronti*, Milano, 2015; CECANESE, *Confronto, ricognizione ed esperimento giudiziale nella logica dei mezzi di prova*, Napoli, 2013; MENNA, Sub art. 213, in *Comm. c.p.p.* Giarda-Spangher, I, Milano, 2010, 2152; BERNASCONI, *La ricognizione di persone nel processo penale*, Torino, 2003; CAPITTA, *Ricognizioni e individuazioni di persone nel diritto delle prove penali*, Milano, 2001; TRIGGIANI, *La ricognizione personale: struttura ed efficacia*, in *Riv. it. dir. proc. pen.*, 1996, 728; Id., *Ricognizioni mezzo di prova nel nuovo processo penale*, Milano, 1998; MOSCARINI, voce *Ricognizioni* (proc. pen.), in *Enc. giur.*, XXVII, Roma, 1991, 3; DELL'ANNO, *Osservazioni in tema di individuazione e ricognizione di persone nel nuovo codice di procedura penale*, in *Cass. pen.*, 1991, 1898.

strumento dell'IA in modo da confrontare quanto contenuto nella banca dati con l'immagine estrapolata dal video al fine di rendere più affidabile l'elemento investigativo. Oppure si potrebbe, a seconda del caso concreto, attivare lo strumento dell'IA ai fini della prosecuzione delle indagini e poi ricorrere ad altro strumento investigativo quale l'individuazione di cui all'art. 361 c.p.p. in virtù del risultato raggiunto con l'IA.

E' chiaro che occorra un intervento del legislatore per prevedere i presupposti e l'autorizzazione del giudice funzionalmente competente per proseguire con lo strumento ad alto rischio per il riconoscimento facciale. Peraltro, l'individuazione prevede un riconoscimento operato dalla persona fisica differente da quello effettuato dal *software* e quindi lo strumento di intelligenza artificiale allo stato non può essere inquadrato nell'art. 361 c.p.p. in quanto necessita di specifiche garanzie in virtù della natura del mezzo investigativo.

Va specificato, viste le perplessità che si nutrono al riguardo⁴³, che senza timore l'algoritmo potrebbe anche essere più affidabile di un riconoscimento effettuato da una persona fisica, poiché su un compito specifico come il

⁴³ Si ritiene che le capacità dell'algoritmo fondate su enorme quantità di dati si differenziano dalle capacità intellettive dell'uomo di riconoscere le immagini facciali, in quanto la macchina non possiede i processi neurologici e intuitivi umani. Sul punto cfr., MEZIO, *Tecnologie di riconoscimento facciale: una riflessione sul loro impiego con finalità investigative e probatorie*, in *Cass. pen.*, 2025, 645 ss.; BELVINI, *Intelligenza artificiale e circuito investigativo*, Bari, 2025, 174 ss.; MOBILIO, *Tecnologie di riconoscimento facciale*, Napoli, 2021, 42; COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Diritto penale e intelligenza artificiale*, a cura di Balbi-De Simone-Esposito-Manacorda, Torino, 2022, 128; DE CARO, *Le delicate traiettorie dell'informazione digitale nel processo penale*, in *Arch. pen.*, 2025, 18 ss., secondo cui, in generale sul calcolo algoritmico effettuato dalla macchina, vi è l'opportunità di un controllo umano incisivo «capace di mantenere il primato dell'uomo sui processi di automazione che possono incidere direttamente sulla decisione».

riconoscimento visivo (su persone e oggetti) le macchine ormai trascendono e superano i limiti umani non solo nell'accuratezza, ma anche nella quantità di categorie che possono processare e da cui possono imparare. Le reti neurali convoluzionali profonde (*deep convolutional neural nets*), almeno nel caso dell'IA ristretta, hanno raggiunto prestazioni eccellenti nella classificazione delle immagini e nel riconoscimento facciale⁴⁴. La rete neurale consente all'intelligenza artificiale di cogliere con l'approfondimento profondo connessioni intricate e complesse, anche quelle che sfuggono all'osservazione dell'uomo (la precisione della rete dipende dalla qualità dei dati su cui la stessa è addestrata)⁴⁵. A monte, ovviamente, l'algoritmo non deve essere pregiudicato da parte dei produttori del *software*⁴⁶ e proprio per questo sono state introdotte regole e controlli per legittimare l'impiego degli strumenti di IA. Una volta superata la barriera dei controlli e delle verifiche dei testi eseguiti e riscontro del tasso di errore – e con la previsione di regole processuali – il risultato ottenuto con l'intelligenza artificiale può essere approfondito, confrontato e poi valutato complessivamente con gli altri elementi d'indagine.

In conclusione, la L. 23 settembre 2025, n. 132, contiene una delega al Governo per l'adozione, entro dodici mesi dall'entrata in vigore del provvedimento, di uno o più decreti legislativi che adeguino la normativa nazionale al

⁴⁴ CRISTIANINI, *Sovrumano. Oltre i limiti della nostra intelligenza*, Bologna, 2025.

⁴⁵ KISSINGER-SCHMIDT-HUTTENLOCHER, *L'era dell'intelligenza artificiale*, Milano, 2023.

⁴⁶ Nel caso di compromissione dell'algoritmo sorge la necessità di comprendere la natura della responsabilità giuridica del produttore o di altri soggetti (ad esempio addestratori ed alimentatori di dati pregiudizievoli).

regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio - *AI Act* (art. 24, co. 1). L'esercizio della delega è subordinato oltre che al rispetto dei principi e criteri direttivi generali di cui all'articolo 32 della L. 24 dicembre 2012, n. 234, ai principi e criteri direttivi specifici (art. 24, co. 2).

Tra i principi e criteri direttivi specifici è fissata la previsione di un'apposita disciplina per l'utilizzo di sistemi di intelligenza artificiale per l'attività di polizia (art. 24, co. 2, lett. h); è prevista la definizione dei poteri di vigilanza dell'autorità di vigilanza del mercato che conferiscano all'autorità i poteri di imporre ai fornitori e ai potenziali fornitori di trasmettere informazioni, di effettuare ispezioni a distanza o in loco, anche senza preavviso, e di svolgere controlli sulla conduzione delle prove in condizioni reali e sui relativi sistemi di intelligenza artificiale ad alto rischio (art. 24, co. 2, lett. m); la regolazione dell'utilizzo dei sistemi di intelligenza artificiale nelle indagini preliminari, nel rispetto delle garanzie inerenti al diritto di difesa e ai dati personali dei terzi, nonché dei principi di proporzionalità, non discriminazione e trasparenza (art. 24, co. 5 lett. e); è previsto di individuare ipotesi per le quali appare necessario dettare il regime giuridico dell'utilizzo di dati, algoritmi e metodi matematici per l'addestramento di sistemi di intelligenza artificiale, nonché i diritti e gli obblighi gravanti sulla parte che intenda procedere al suddetto utilizzo (art. 16, co. 3)⁴⁷.

⁴⁷ Il Governo è delegato ad adottare, entro dodici mesi dalla data di entrata in vigore della presente legge, uno o più decreti legislativi per definire una disciplina organica relativa all'utilizzo di dati, algoritmi e metodi matematici per l'addestramento di sistemi di intelligenza artificiale senza obblighi ulteriori, negli ambiti soggetti al regolamento (UE) 2024/1689, rispetto a quanto già stabilito da quest'ultimo provvedimento (art. 16, co. 1).

I contenuti della delega, stando al procedimento penale, si concentrano in particolare sulla fase preliminare; di conseguenza in sede di attuazione delle deleghe legislative il Governo dovrà delineare la tipologia e le modalità di impiego dei sistemi di intelligenza artificiale sulla base della necessità e proporzionalità e stabilire i divieti nel rispetto della normativa nazionale che si affianca a quella europea, in modo da riempire di contenuto i requisiti di conoscibilità, trasparenza, spiegabilità, assicurando il controllo umano dei predetti sistemi e i relativi diritti di difesa, quanto meno nell'ambito delle indagini preliminari⁴⁸.

⁴⁸ Il presente contributo ha origine da uno studio e/o ricerca svolta nell'ambito del Prin 2022 su "Prova e processo informatizzato", Missione 4 - Componente 2, Cup (E53D23006850006 – soggetto attuatore).