

# L'IA nel procedimento penale: tra riconoscimento facciale e finalità investigative

Christian Pallante

## Sommario

1. L'IA e il procedimento penale: un rapporto in continua trasformazione – 2. Il riconoscimento facciale: aspetti tecnici – 3. Le insidie del riconoscimento algoritmico nel contesto eurounitario: tra prospettive nazionali e *AI Act* – 4. Il riconoscimento facciale come elemento di scambio nel contesto unionale: gli approdi del sistema Prüm II – 5. Lo strumento algoritmico nel contesto italiano – 6. Prospettive *de jure condendo*.

## 1. L'IA e il procedimento penale: un rapporto in continua trasformazione

Negli ultimi anni, le nuove tecnologie dotate di intelligenza artificiale (IA) hanno iniziato a permeare ogni aspetto della vita quotidiana, trasformando radicalmente il modo in cui ogni persona lavora, comunica e si relaziona con il mondo.

La c.d. “rivoluzione algoritmica” rappresenta ormai la nuova frontiera tecnologica in cui l'umano è chiamato a “misurarsi” con la macchina<sup>1</sup>.

L'approccio “tradizionale” di taluna dottrina nordeuropea e d'oltreoceano<sup>2</sup> definisce l'IA come l'insieme di applicazioni che svolgono gli ordinari compiti umani in maniera migliore rispetto all'uomo.

Sebbene in parte anacronistica, la definizione in realtà vuole sintetizzare il forte legame che si crea con l'essere umano, il quale risulta essere ancora al centro della “alimentazione” dell'IA.

Detto legame permea anche le dinamiche del procedimento penale, il quale risulta essere il naturale “banco di prova” di questi nuovi strumenti algoritmici<sup>3</sup>.

\* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio “a doppio cieco”.

<sup>1</sup> A tal proposito, S. Lorusso, *La sfida dell'intelligenza artificiale al processo penale nell'era digitale*, in *Sist. pen.*, 28 marzo 2024, 1 s.

<sup>2</sup> Su questa concezione, fra gli altri, P. Russell-S.J. Norvig, *Artificial intelligence. A modern approach*, IV ed., Upper Saddle River, 2021, 3.

<sup>3</sup> In tal senso, fra gli altri, W. Nocerino, *Il principio di immediatezza alla prova della tecnologia*, in F.S. Cassibba-L. Foffani-G. Garuti (a cura di), *La riforma Cartabia. Riflessioni sulla legge delega n. 134 del 2021. Atti della Tavola rotonda del 21 aprile 2022*, Torino, 2021, 110, in cui l'A. ricorda come «[S]e è vero che il processo penale è lo specchio della società e rappresenta

Partendo dalla fase che «non conta[va] e non pesa[va]»<sup>4</sup>, l'IA prosegue la sua corsa inarrestabile fino alla conclusione dell'arco procedimentale, giungendo anche nella c.d. “giustizia predittiva”, ove l'algoritmo tende ad affiancarsi (e, paradossalmente, a “sovrapporsi”) alle classiche funzioni dell'organo giudicante<sup>5</sup>.

Le tecnologie algoritmiche, in quest'ottica, riflettono la profondissima trasformazione del procedimento penale, caratterizzato dalla progressiva perdita di centralità della fase processuale in senso stretto in ragione del massiccio potenziamento delle indagini preliminari. Infatti, queste ultime rappresentano la nuova sede in cui la prova inizia a formarsi<sup>6</sup> e ad essere addirittura acquisita per la valutazione giudiziale.

In tale frangente, gli strumenti dotati di IA – fra cui il riconoscimento facciale – costituiscono uno dei principali elementi del rafforzamento delle operazioni investigative, tramite cui individuare nuovi elementi probatori (se non direttamente prove) per giungere a una tempestiva identificazione dei possibili autori di reato.

Appare, dunque, fondamentale indagare il ruolo dell'IA all'interno di un procedimento penale profondamente mutato rispetto ai suoi canoni originari, ponendo l'accento proprio sui possibili utilizzi del riconoscimento biometrico che rappresentano una parte sempre più rilevante delle modalità investigative.

---

i valori della società in un determinato momento storico, è altrettanto vero che ogni volta in cui cambia la società, cambia il processo»; S. Quattrocolo, *An introduction to AI and criminal justice in Europe*, in *Rev. Bras. der. proc. pen.*, 2019, 1519 ss.; Ead., *Artificial intelligence, computational modelling and criminal procedure*, Cham, 2020, 3 ss. Sulla medesima scia, B. Custers, *AI in criminal law: an overview of AI applications in substantive and procedural criminal law*, in B. Custer-E. Fosch-Villaronga (a cura di), *Law and artificial intelligence*, Berlino, 2022, 205 ss.; G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Dir. pen. cont.*, 4, 2020, 75 ss.; Id., *Perizia, prova scientifica e intelligenza artificiale nel processo penale*, in *Sist. pen.*, 3 giugno 2024, 18 s.

<sup>4</sup> Così, M. Nobili, *Scenari e trasformazioni del processo penale*, Padova, 1998, 35.

<sup>5</sup> Basti pensare ai recenti impieghi dell'IA nel processo penale cinese, in cui negli ultimi anni si è cercato di sperimentare possibili usi dell'algoritmo sia per le attività meramente burocratiche che per la valutazione probatoria, specialmente in casistiche molto semplici. In tema, fra gli altri, G. Barone, *Intelligenza artificiale e metrologia forense. Note a margine delle risoluzioni dell'AIDP su AI e processo penale*, in *Cass. pen.*, 2024, 4063 ss.; I. Cardillo, *Disciplina dell'intelligenza artificiale e intelligentizzazione della giustizia in Cina*, in *Biolaw journal*, 3, 2022, 139 ss.; A. Dell'erba, *La giustizia predittiva come possibile antidoto all'inadeguatezza della giurisdizione*, in *Sist. pen.*, 28 marzo 2024, 2 ss.; R.E. Kostoris, *Intelligenza artificiale, strumenti predittivi e processo penale*, in *Cass. pen.*, 2024, 1642 ss.; G. Ubertis, *Intelligenza artificiale e giustizia predittiva*, in *Sist. pen.*, 16 ottobre 2023, 1 ss.

<sup>6</sup> Su questo profilo, F. Vergine, *Indagini e dibattimento: il singolare funzionamento della clessidra*, in *Dir. pen. proc.*, 2020, 1158, ricorda che il processo penale «[...] è andato (*rectius*, mandato) in crisi, avendo posto in discussione gli stessi ruoli delle varie fasi, decolorando la centralità del dibattimento e arretrando sempre di più il momento tipico dell'accertamento, da un lato rendendo più “libere” le indagini e assegnando una sorta di ultrattività probatoria ai suoi atti e dall'altro intervenendo proprio sul dibattimento ponendo limiti e producendo scorciatoie». Sulla stessa scia, G. Canzio, *AI Act e processo penale: sfide e opportunità*, in *Sist. pen.*, 14 ottobre 2024, 9; W. Nocerino, *La durata delle indagini e il controllo giurisdizionale sui tempi del procedimento*, in *Cass. pen.*, 2023, 2621, la quale precisa che «[S]empre più spesso, infatti, si assiste ad una relazione osmotica tra indagini e giudizio, sia perché gli atti investigativi sono destinati di sovente a trasmigrare nel processo, sia perché molte “prove” sono suscettibili di formarsi già durante la fase preliminare».

## 2. Il riconoscimento facciale: aspetti tecnici

Gli strumenti di riconoscimento biometrico risultano essersi evoluti e trasformati nell'ultimo decennio.

Tale trasformazione, come riportato da parte della dottrina<sup>7</sup>, ha impattato sui tradizionali concetti di "identità" e "identificazione" nel contesto investigativo.

Il primo termine, in particolare, può essere visto come l'insieme delle caratteristiche che connotano un soggetto e che consentono di individuare, o di identificare, quella specifica persona. L'identificazione, invece, rappresenta l'insieme delle tecniche che mira ad attribuire una specifica identità a un soggetto proprio in funzione delle caratteristiche univoche che lo contraddistinguono.

In altri termini, le connotazioni derivanti dal concetto di identità diventano strumentali per l'attività identificativa, considerando che solo grazie a queste peculiarità è possibile distinguere i soggetti d'interesse da una «moltitudine indifferenziata»<sup>8</sup>.

Evidente la portata che queste nuove tecnologie possono avere nelle complesse operazioni di individuazione degli autori di reato.

Volendo addentrarsi nell'aspetto più propriamente tecnico, occorre preliminarmente comprendere in cosa si sostanzia il riconoscimento facciale. Attualmente, questo strumento rappresenta l'insieme delle applicazioni di IA che permettono, mediante l'ausilio di algoritmi, di eseguire delle analisi sui tratti biometrici del volto di una persona e, al contempo, di confrontarli con le sembianze dei soggetti inserite in un apposito *database*<sup>9</sup>, oltre che di conservarli all'interno della medesima banca dati<sup>10</sup>.

Occorre distinguere principalmente due funzioni: il riconoscimento in differita e quello in tempo reale.

In particolare, la prima funzione permette di ricercare – all'interno di una banca dati – l'identità di un volto presente in un'immagine selezionabile di volta in volta dall'operatore. In questo caso, l'apparato di videosorveglianza e la banca dati agiscono in maniera asincrona.

La modalità *Real-time*, invece, permette un riconoscimento pressoché immediato su più video provenienti da impianti di video sorveglianza, in cui la ripresa del soggetto e la sua identificazione sono contestuali.

Dal punto di vista operativo, è innegabile il potente apporto che queste

<sup>7</sup> Sul punto, K. La Regina, *L'identificazione della voce nel processo penale*, Padova, 2018, 2. Più recentemente, C. Pallante, *Identità e identificazione: uno scopo, tante normative*, in G. Bottaro (a cura di), *Identità europea. Storia, tradizione, innovazione*, Messina, in press.

<sup>8</sup> Così, P. Foschini, *Le parti responsabili penali*, in *Arch. pen.*, 1954, 31.

<sup>9</sup> Su questi profili, C.S. Milligan, *Facial recognition technology, video surveillance, and privacy*, in *Southern California interdisciplinary law journal*, 9, 1999, 304 ss.; D. Morane-R. Pagar-K. Patil-S. Patil-P.N. Pathak, *Criminal identification using facial recognition*, in *International research journal of modernization in engineering technology and science*, 5(5), 2023, 54; K. Y. Santamaria, *Facial recognition technology and law enforcement: select constitutional consideration*, in W. Lambert (a cura di), *Issues with facial recognition technology*, New York, 2021, 3.

<sup>10</sup> In argomento, E. Wright, *The future of facial recognition is not fully known: developing privacy and security regulatory mechanisms for facial recognition in the retail sector*, in *Fordham intellectual property media & entertainment law journal*, 2019, 29, 621 ss.

tecnologie forniscono alle indagini<sup>11</sup> – tanto nella fase procedimentale, quanto in quella preventiva –, rendendole maggiormente performanti e veloci<sup>12</sup> e determinando, nel medesimo frangente, un forte impatto sui diritti fondamentali delle persone interessate.

Proprio su questo fronte si registrano alcune questioni critiche legate, per ora, al dato tecnico, dal momento che vi possono essere elementi che intaccano l'accuratezza dei riconoscimenti, limitandone fortemente l'affidabilità.

*In primis*, la scarsa qualità degli strumenti video-fotografici e, conseguentemente, delle immagini catturate da suddette strumentazioni. Infatti, con *frames* di bassa qualità, il programma non ha a disposizione le caratteristiche univoche per associare il volto e fornire un'identificazione, creando il rischio di individuare un soggetto diverso da quello impresso nella foto<sup>13</sup>. In secondo luogo, talune prassi investigative poco chiare, le quali alimentano ulteriori dubbi sull'uso di detti strumenti.

A tal proposito, si possono ricordare alcune casistiche della polizia di New York riguardanti una serie di furti in supermercati<sup>14</sup>. In questi casi, l'indagato viene ripreso da una videocamera posta all'interno del *locus commissi delicti* ma i fotogrammi risultano poco nitidi e il *database* non riesce a fornire alcun riscontro.

Gli investigatori sostituiscono, a loro piacimento, suddetta immagine con una foto dell'attore Woody Harrelson, in quanto dotata (a loro dire) di caratteristiche simili, riuscendo a trovare un possibile risultato nella banca dati<sup>15</sup>. Ciò fornisce molteplici incertezze sull'affidabilità del riconoscimento effettuato.

---

<sup>11</sup> In tal senso, G.M. Baccari, *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati*, in A. Cadoppi-S. Canestrari-A. Manna-M. Papa (a cura di), *Cybercrime*, II ed., Torino, 2022, 1868 ss.; E.M. Mancuso, *L'ingresso dei big data nel procedimento penale*, in Associazione tra gli studiosi del processo penale (a cura di), *Diritti della persona e nuove sfide del processo penale*, Milano, 2019, 171 ss.

<sup>12</sup> Si può ben citare il pensiero di K.A. Gates, *Our biometric future. Facial recognition technology and the culture of surveillance*, New York, 2011, 1 s., in cui l'A. ricorda come queste tecnologie potessero essere d'aiuto già nell'attentato delle *Twin towers* che ha cambiato la visione di sicurezza a livello internazionale. Sulla stessa scia Q. Bu, *The global governance on automated facial recognition (AFR): ethical and legal opportunities and privacy challenges*, in *International cybersecurity law review*, 2, 2021, 114 ss.

<sup>13</sup> In tema, M. Jacquet-C. Champod, *Automated face recognition in forensic science: review and perspectives*, in *Forensic science international*, 2020, 307, 110124 ss.; H.P. Filho, A. Trajcevski, K. Bhargava, N. Jawed, J.H. Elder, *Attentive sensing for long-range face recognition*, in The Computer Vision Foundation (a cura di), *Proceedings of the IEEE/CVF winter conference on applications of computer vision (WACV) workshops*, 2023, 613 ss.; R.A. Waelen, *The struggle for recognition in the age of facial recognition technology*, in *AI and ethics*, 3, 2023, 216 s.

<sup>14</sup> L'uso di immagini di tal tipo, legato a prassi investigative poco affidabili, ha portato la dottrina americana a parlare di “*fringe techniques*”. Il termine esplica efficacemente la predisposizione delle forze di polizia a utilizzare tecniche che talvolta si pongono nel sottilissimo confine tra affidabilità probatoria e inattendibilità. Per tutti, R.D. Goldberg, *You can see my face, why can't I? Facial recognition and Brady*, in *HRLR online*, 5, 2021, 270 s.

<sup>15</sup> Sul punto, G. Edmond-D. White-A. Towler-M. San Roque-R. Kemp, *Facial recognition and image comparison evidence: identification by investigators, familiars, experts, super-recognisers and algorithms*, in *Melbourne university law review*, 45(1), 2021, 31 ss.; A. Pin, “*A Novel and controversial technology*”. *Artificial face recognition, privacy protection, and algorithm bias in Europe*, in *William & Mary bill of rights journal*, 30(2), 2021, 306 ss.

Inoltre, le medesime perplessità vengono in evidenza anche con riferimento ai soggetti appartenenti alle c.d. minoranze.

Proprio nel contesto statunitense è stato studiato, a più riprese, l'impatto negativo che queste tecnologie registrano nei confronti di cittadini afro-americani e asiatici<sup>16</sup>.

Questa criticità è dovuta principalmente alla costruzione dei c.d. *dataset*, vale a dire l'insieme di dati che vengono raggruppati all'interno della banca dati, e più precisamente alla scarsa numerosità e rappresentatività di tali dati che non permette all'intelligenza artificiale di "apprendere" nuove caratteristiche per migliorare il proprio algoritmo e, dunque, di giungere a risultati conformi alla realtà<sup>17</sup>.

### **3. Le insidie del riconoscimento algoritmico nel contesto eurounitario: tra prospettive nazionali e AI Act**

In definitiva, il diritto è sicuramente chiamato a contemperare le esigenze investigative e securitarie con i diritti posti in gioco<sup>18</sup>, circoscrivendo le potenzialità d'uso di tecnologie così invasive.

Partendo da tale assunto, bisogna constatare che proprio nel contesto eurounitario si assiste a una stratificazione di provvedimenti<sup>19</sup>, talvolta direttamente applicabili, che propongono i consueti problemi generati dal multilivello normativo<sup>20</sup>.

Al contrario, sul piano nazionale sono pochissime le realtà che hanno iniziato a legiferare in tal senso, mentre la stragrande maggioranza degli Stati continua a navigare in "zone grigie"<sup>21</sup>.

Fra i rari Paesi che hanno avviato un *iter* normativo in suddetta direzione, merita di essere citata la Francia.

---

<sup>16</sup> In suddetto contesto è stata registrata la massiccia presenza di falsi positivi sia nei cittadini afro-americani, specialmente se di sesso femminile, sia in quelli asiatici. Così, P. Grouter-M. Ngan-H. Hanaoka, *Face recognition vendor test (FRVT) part 3: demographic effects*, in *nist.gov*, 2019, 2 ss.; S. Perkowitz, *The bias in the machine: facial recognition technology and racial disparities*, in *MIT case studies in social and ethical responsibilities of computing*, 5 febbraio 2021, 1 ss.

<sup>17</sup> In tema, A. Holkar-R. Walambe-K. Kotecha, *Few-shot learning for face recognition in the presence of image discrepancies for limited multi-class datasets*, in *Image and vision computing*, 120, 2022, 104420 ss.; G.M. Ruotolo, *Scritti di diritto internazionale ed europeo dei dati*, Bari, 2021, 158 ss.

<sup>18</sup> Cfr. L. Lupària Donati-G. Fiorelli, *Diritto probatorio e giudizi criminali ai tempi dell'Intelligenza Artificiale*, in *Dir. pen. cont.*, 2, 2022, 39; M. R. Magliulo, *L'intelligenza artificiale nel processo penale: progresso o rischio per la tutela dei diritti costituzionali?*, in *Il Processo*, 3, 2022, 578; A. Pin, *Non esiste la "pallottola d'argento": l'Artificial Face Recognition al vaglio giudiziario per la prima volta*, in *DPCE on line*, 4, 2019, 3081.

<sup>19</sup> Si pensi, ad esempio, anticipando quanto si dirà meglio *infra* alle dir. n. 680/2016 e n. 794/2016 e al Reg. n. 982/2024, nonché all'*AI Act* (Reg. n. 1689/2024).

<sup>20</sup> Si rinvia, su tutti, a R.E. Kostoris, *Diritto europeo e giustizia penale*, in *Id.* (a cura di), *Manuale di procedura penale europea*, V ed., Milano, 2022, 1 ss.

<sup>21</sup> Cfr. A. Ramiro-L. Cruz, *The grey-zones of public-private surveillance: policy tendencies of facial recognition for public security in Brazilian cities*, in *Internet Policy Review*, 12(1), 2023, 1 ss.

Pur essendo un modello tipicamente connotato da una legislazione “d’emergenza”, ossia caratterizzata dall’uso di situazioni emergenziali (come quelle securitarie) per normatizzare nuovi istituti procedurali e per renderli applicabili anche nei contesti ordinari, il sistema francese da diversi decenni punta a disciplinare gli strumenti d’indagine, cercando di creare normative specifiche e puntuali in questa delicata materia<sup>22</sup>.

Su tale scorta, in tempi più recenti, si sta procedendo a legiferare in merito ai nuovi possibili utilizzi del riconoscimento facciale<sup>23</sup>.

Un primo impiego di tale tecnica è già rintracciabile nel casellario giudiziale, dove a norma dell’art. R40-26 c.p.p. è possibile ricorrere all’uso del riconoscimento facciale sulle foto conservate<sup>24</sup>, in quanto si tratta di immagini di soggetti condannati e, in casi residuali, di persone scomparse<sup>25</sup>.

Un ulteriore utilizzo dello strumento è disciplinato nel c.d. Sistema Parafe, introdotto con il decreto n. 1113 del 4 dicembre 2013 negli artt. R232-6 ss. del codice di sicurezza interna (CSI), che ne prevede l’uso per il controllo automatizzato dei viaggiatori entranti o uscenti dallo spazio Schengen. In tal caso, le immagini del volto sono catturate in tempo reale dagli apparati di videosorveglianza ma non vengono conservate per fini di alimentazione dei *database*<sup>26</sup>.

Sulla stessa scia si pone anche la recente normativa in merito alle misure di sicurezza adottate per i giochi olimpici e paraolimpici del 2024<sup>27</sup>, in cui il legislatore francese prevede un utilizzo dei sistemi di videosorveglianza in tempo reale, a titolo sperimentale, al solo fine di segnalare eventuali rischi alla sicurezza degli eventi senza ricorrere al riconoscimento facciale<sup>28</sup>.

Si è poi avuta anche l’approvazione della legge n. 646/2021 «*pour une sécurité globale préservant les libertés*», con cui vengono potenziate le possibilità di utilizzare videocamere nel corso dell’attività investigativa<sup>29</sup>, come nel caso delle *bodycam*.

La Francia, in questo frangente, dimostra di aver scelto di limitare temporaneamente l’uso delle tecnologie algoritmiche con lo scopo di compren-

<sup>22</sup> Ne sono chiari esempi l’*IMSI Catcher* e l’attività investigativa su *server* disciplinati nella sezione relativa alle altre tecniche speciali d’indagine del codice di procedura penale francese. Per un’analisi sulla disciplina, D. Curtotti-V. Rizzi-W. Nocerino-A.M. Russitto-G. Giliberti-G. Scarpa, *Piattaforme criptate e prova penale*, in *Sist. pen.*, 6, 2023, 173 ss.; S. Guinchard-J. Buisson, *Procédure pénale*, XV ed., Parigi, 2022, 715 ss.; W. Nocerino, *La tipizzazione dell’IMSI Catcher in Francia: sistemi a confronto*, in *Portale intelligence, security & investigation*, 23 giugno 2022; V. Wester-Ouisse, *État d’urgence et procédure pénale*, in *Revue juridique de l’ouest*, 1, 2016, 7 ss.

<sup>23</sup> In tema, M. Picaud, *La reconnaissance faciale: un marché en construction?*, in *Futuribles*, 16 aprile 2020.

<sup>24</sup> Questa disposizione è stata introdotta con il decreto n. 652/2012, relativo al trattamento dei precedenti giudiziari. Sul punto, H. Vlamync, *Droit de police*, VII ed., Parigi, 2021, 540.

<sup>25</sup> Come previsto dall’art. R40-26, c. 3, c.p.p.

<sup>26</sup> Come sancito dall’art. R232-7, c. 2, CSI.

<sup>27</sup> Trattasi della L. n. 2023-380 del 19 maggio 2023. Per un’analisi completa, Sénat, *Rapport d’information sur le projet de loi relatif aux jeux olympiques et paralympiques de 2024*, in *sénat.fr*, 18 gennaio 2023.

<sup>28</sup> Questo aspetto viene ben evidenziato dall’art. 10, c. 4, della normativa.

<sup>29</sup> In argomento, F. De Simone, *Una nuova tipologia di misure di prevenzione: algoritmi, intelligenza artificiale e riconoscimento facciale*, in *Arch. pen.*, 2, 2023, 32 s.

derne gli effetti e di regolamentarlo in tempi più maturi<sup>30</sup>.

Gli *escamotages*, tuttavia, non mancano. Proprio con riferimento al riconoscimento facciale, un'indagine amministrativa è stata avviata dal ministro dell'interno e condotta dalla *Commission Nationale de l'Informatique et des Libertés* (CNIL) nei confronti della polizia nazionale francese.

In particolare, a seguito del rapporto pubblicato dal giornale investigativo “*Disclose*”<sup>31</sup>, emerge un possibile aggiramento della normativa vigente in quanto la *Police Nationale* utilizza un sistema dotato di IA che consente di svolgere il riconoscimento facciale. Il sistema in questione, denominato “*Video synopsis*” e fabbricato dall'azienda israeliana *Briefcam*, permette di analizzare lunghi video nel giro di pochi minuti e di seguire una persona o un veicolo ripresi da più videocamere grazie al proprio abbigliamento o al numero di targa. Il rapporto, più nel dettaglio, evidenzia come suddetto strumento sia stato sperimentato già a partire dal 2015, per poi essere implementato sempre più nelle singole articolazioni della polizia francese. La questione più spinosa attiene alla possibile elusione della normativa europea, vale a dire la direttiva (UE) 680/2016, che prevede una valutazione d'impatto delle nuove tecnologie utilizzate nel caso in cui queste interferiscano pesantemente con i diritti e le libertà dei soggetti coinvolti, come specificato dall'art. 27 della direttiva.

Il quadro delineato appare sempre più incerto e l'unica possibile via risolutiva diventa un intervento legislativo piuttosto deciso che ne disciplini i limiti applicativi nelle indagini preliminari e, conseguentemente, ne legittimi l'utilizzabilità probatoria in sede processuale<sup>32</sup>.

Volgendo lo sguardo al contesto eurounitario, è degno di nota il regolamento di recente approvazione teso a delineare i possibili usi dell'intelligenza artificiale, ossia il c.d. *AI Act* (Regolamento (UE) 1689/2024, “Regolamento”).

In questa normativa, l'uso del riconoscimento facciale in sede investigativa viene relegato all'interno degli artt. 5 e 26, scindendo le due modalità di utilizzo, ossia in tempo reale e in differita.

Per quanto riguarda il *real time*, l'art. 5 pone un iniziale divieto di utilizzo degli strumenti di intelligenza artificiale, costruendo una successiva eccezione al veto in ragione della ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani e sfruttamento sessuale e di persone scomparse; della prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche e per quella relativa ad un attacco terroristico; la localizzazione e l'identificazione di una persona sospettata di aver commesso un reato, collegandosi con lo svolgimento di un'attività investigativa, con l'esercizio dell'azione penale e con l'esecuzione di una sanzione penale (art. 5, par. 1, lett. h), *AI Act*).

---

<sup>30</sup> Si può segnalare il rapporto informativo del Senato francese, in cui si riflette sui possibili rischi di detta tecnologia e si cerca di definire una serie di proposte per una futura legislazione in materia. Cfr. Sénat, *Rapport d'information sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles*, in *sénat.fr*, 10 maggio 2022.

<sup>31</sup> Sul punto, M. Destal-C. Le Foll-G. Livolsi, *La police nationale utilise illégalement un logiciel israélien de reconnaissance faciale*, in *Disclose*, 14 novembre 2023.

<sup>32</sup> In argomento, S. Etoa, *L'image et le son? Le déploiement de la surveillance algorithmique dans l'espace public*, in *Cahiers de la recherche sur les droits fondamentaux*, 2023, 21, 82.

In questo caso, l'*AI Act* cerca di perimetrare l'utilizzo di queste strumentazioni sia per fini preventivi che repressivi sulla scorta dei reati previsti dall'allegato II<sup>33</sup> del Regolamento e della punibilità in concreto degli stessi con una pena o misura di sicurezza di almeno quattro anni, ma di fatto si indirizza sui c.d. "sospettati di reati" senza fornire adeguate garanzie<sup>34</sup> e, soprattutto, con un catalogo di fattispecie piuttosto ampio e poco circoscritto.

Dunque, l'art. 5 si profila come una norma costruita su "apparenti" divieti che, in conseguenza delle continue eccezioni previste, decadono in ragione di finalità chiaramente securitarie.

Inoltre, l'art. 5, par. 3, specifica la necessità di un atto autorizzativo *ex ante* da parte di un'autorità giudiziaria o amministrativa, con natura vincolante, qualora venga utilizzato un sistema di IA dotato di riconoscimento biometrico in tempo reale in spazi accessibili al pubblico.

In casi di urgenza debitamente giustificati è possibile usare il sistema anche in assenza di autorizzazione, a condizione che l'atto sia trasmesso alla competente autorità entro 24 ore per ottenerne l'assenso.

Anche il relativo par. 5 lascia un ampio spazio di manovra nelle mani dei legislatori nazionali, i quali saranno liberi di decidere circa la possibilità di introdurre o meno una specifica procedura autorizzativa.

Tale assetto viene confermato anche dalle linee guida della Commissione europea in merito agli utilizzi "proibiti" del riconoscimento facciale in tempo reale<sup>35</sup>, non ancora formalmente adottate.

Per quanto attiene al riconoscimento facciale in differita, invece, l'art. 26, par. 10, del Regolamento inserisce come punto nodale la richiesta di un'apposita autorizzazione *ex ante* o senza indebito ritardo ed entro le 48 ore di un'autorità giudiziaria o amministrativa, la cui decisione deve essere vincolante e soggetta al controllo giurisdizionale.

L'unica eccezione a questa regola generale è dettata dall'identificazione iniziale di un potenziale sospetto sulla base di fatti oggettivi e verificabili direttamente connessi al reato, su cui tuttavia il Regolamento non fornisce alcuna linea esplicativa.

Si delinea, così, un regime differenziato per l'utilizzo di queste tecnologie, per cui il riconoscimento in differita appare tendenzialmente più garantito rispetto a quello in tempo reale. Infatti, proprio sull'uso in *real time* si profila un prevalere piuttosto netto delle operazioni a carattere preventivo rispetto alle garanzie dei soggetti coinvolti, con il pericolo di penetrare

---

<sup>33</sup> Si tratta, in particolare, dei reati di terrorismo, tratta di esseri umani, sfruttamento sessuale di minori e pornografia minorile, traffico illecito di stupefacenti o sostanze psicotrope, traffico illecito di armi, munizioni ed esplosivi, omicidio volontario, lesioni gravi, traffico illecito di organi e tessuti umani, traffico illecito di materie nucleari e radioattive, sequestro, detenzione illegale e presa di ostaggi, reati che rientrano nella competenza giurisdizionale della Corte penale internazionale, illecita cattura di aeromobile o nave, violenza sessuale, reato ambientale, rapina organizzata o a mano armata, sabotaggio e di partecipazione in un'organizzazione criminale finalizzata al compimento di reati.

<sup>34</sup> In tal senso, W. Nocerino, *Sulle modalità di acquisizione delle immagini provenienti dalle videocamere di sorveglianza*, in *Cass. pen.*, 2024, 2425.

<sup>35</sup> Sul punto, Commissione Europea, *Commission guidelines on prohibited artificial intelligence practises established by Regulation (EU) 2024/1689 (AI Act)*, in *digital-strategy.ec.europa.eu*, 4 febbraio 2025, 120 s.

sempre più nelle vicende procedurali.

### **4. Il riconoscimento facciale come elemento di scambio nel contesto unionale: gli approdi del sistema Prüm II**

Sul piano eurounitario, bisogna segnalare che i dati biometrici e, più nello specifico, il riconoscimento facciale fungono anche da nuovi elementi di scambio tra le forze di polizia europee. Infatti, con il fine di fornire un assetto legislativo che funga da guida, l'Unione europea sta cercando di irrobustire il sistema di cooperazione investigativa, tramite l'ammodernamento del Sistema Prüm<sup>36</sup>.

La disciplina, nata sotto forma di proposta nel 2021, è attualmente contenuta nel Regolamento n. 982/2024 che il legislatore europeo ha sviluppato cercando di seguire le osservazioni critiche espresse dallo *European Data Protection Supervisor* in punto di mancanza di limitazioni allo scambio delle informazioni biometriche<sup>37</sup> e sulle misure tecniche da adottare per la protezione di suddetti dati<sup>38</sup>, considerando che i criteri di raccolta adottati differiscono in ciascuna Nazione<sup>39</sup>.

In particolare, il nuovo Sistema Prüm II rappresenta un'evoluzione dell'attuale struttura di scambio di dati tra Nazioni, in cui vengono inseriti nell'alveo delle informazioni – oltre alle impronte digitali, al DNA e ai dati di immatricolazione di veicoli – le immagini dei volti e il casellario giudiziale. Alla luce dei nuovi innesti normativi, il sistema amplia le sue finalità applicative – inizialmente ricomprese nella sola repressione dei reati – fino ad annoverare la fase preventiva, la ricerca di persone scomparse e l'identificazione di resti umani.

Dal punto di vista della sua struttura, suddetto sistema viene centralizzato mediante l'adozione di un *router*<sup>40</sup> che fornisce agli Stati membri e a Euro-

---

<sup>36</sup> In tema, A. Procaccino, *Securizzazione dell'Unione europea e poteri concorrenti. Dall'investigazione, alla prevenzione, all'osservazione*, in *Dir. pen. cont.*, 1, 2023, 165; L. Scaffardi, *Next Generation Prüm e le scelte strategiche della UE: dall'ampliamento nello spazio dei dati genetici all'introduzione del riconoscimento facciale*, in *Federalismi*, 8, 2021, 211 ss.

<sup>37</sup> Il Garante europeo nota, in particolare, la mancanza di una gradazione dei reati che permettono la ricerca e, il conseguente scambio, dei dati e che giustificerebbe l'attività di cooperazione tra Stati e la limitazione dei diritti dei soggetti interessati. Così, European Data Protection Supervisor, *Opinion 4/2022 on the proposal for a regulation on automated data exchange for police cooperation ("Prüm II")*, in *edps.europa.eu*, 2 marzo 2022, 9 ss.

<sup>38</sup> Specialmente considerando che la tecnica di pseudonimizzazione è insufficiente a garantire una proporzionalità delle attività. Su questo profilo European Data Protection Supervisor, *Opinion 4/2022 on the proposal for a regulation on automated data exchange for police cooperation ("Prüm II")*, cit., 12.

<sup>39</sup> Questa criticità è ancora presente anche nella precedente situazione delineata dal sistema Prüm. In tal senso, V. Toom-R. Granja-A. Ludwig, *The Prüm decisions as an aspirational regime: reviewing a decade of cross-border exchange and comparison of forensic DNA data*, in *Forensic science international: genetics*, 2019, 41, 50 ss.

<sup>40</sup> Come chiarito dall'art. 35, il *router* è formato da un'infrastruttura centrale, da un canale di comunicazione sicuro fra l'infrastruttura centrale e i punti di contatto delle singole Nazioni e, infine, da un'infrastruttura di comunicazione fra la struttura centrale e

pol la possibilità di ricercare eventuali corrispondenze con le informazioni raccolte da altri Paesi del contesto unionale.

Scendendo più in profondità, il Regolamento prevede, da un lato, l'alimentazione delle banche dati nazionali – indicizzando i dati per permettere un'associazione diretta con il soggetto interessato –, mentre dall'altro regola la consultazione automatizzata dei dati indicizzati messi a disposizione dagli Stati membri e da Europol.

Si precisa che la normativa definisce anche il tempo di risposta del sistema – e quindi di scambio – in un massimo di 48 ore, velocizzando di fatto la cooperazione investigativa.

Nell'espletamento della consultazione dei dati, le autorità competenti sono tenute a fornire una valida giustificazione che contenga la finalità dell'attività e il tipo di soggetto da individuare. Si precisa che tale atto dovrà specificare anche l'intenzione di ottenere maggiori informazioni su persone note oppure di identificare semplicemente autori (o presunti tali) ignoti<sup>41</sup>. Questo passaggio diventa essenziale per garantire la proporzionalità e la necessità dell'utilizzo del sistema per i fini investigativi e preventivi, assicurando una protezione dei dati da accessi non autorizzati e sproporzionati.

A questo profilo si collegano i controlli endogeni ed esogeni – da parte di titolari del trattamento nazionali e garanti per la protezione dei dati personali nazionali ed europei – previsti dall'art. 55 del Regolamento.

In questo caso, sebbene la rubrica indichi soltanto una “verifica interna”, il tenore letterale della disposizione suggerisce una correlazione con le autorità di controllo nazionali e con il garante europeo.

Si ricorda che il sistema mantiene traccia su base triennale delle giustificazioni fornite e delle registrazioni delle interrogazioni svolte sul sistema dalle Forze di polizia.

La definizione delle sanzioni per l'uso improprio dello scambio e della consultazione di dati viene rimessa integralmente agli Stati membri, richiamando i canoni dell'effettività, della proporzionalità e della dissuasività<sup>42</sup>.

I dati devono essere cifrati – in linea di continuità con il Regolamento europeo sulla protezione dei dati personali, n. 679/2016 (GDPR) – e gli Stati membri sono tenuti ad assicurare le misure appropriate per tutelarli.

Il periodo di conservazione di suddette informazioni viene regolato dall'art. 51.

In particolare, si disciplina la loro cancellazione quando non sono più necessari per le finalità investigative, oppure nel periodo specificato dalla normativa nazionale o, in alternativa, nel termine previsto dalla dir. n. 794/2016<sup>43</sup>.

---

il portale di ricerca europeo.

<sup>41</sup> La disciplina inerente la giustificazione statale dell'interrogazione del sistema è indicata dall'art. 33.

<sup>42</sup> Come esplicitato dall'art. 56. Per un'analisi sui canoni di effettività, proporzionalità e dissuasività, si v. D. Vozza, *Le tecniche gradate di armonizzazione delle sanzioni penali nei recenti interventi dell'Unione europea*, in *Dir. pen. cont.*, 3, 2015, 19 ss.

<sup>43</sup> La direttiva n. 794/2016 sull'istituzione di Europol prevede all'art. 31, c. 2, un termine *standard* triennale che può essere esteso – previa giustificazione dei motivi per cui la conservazione è necessaria – ad ulteriori tre anni. Al superamento del periodo triennale,

Inoltre, la procedura di scambio delle informazioni viene sviluppata in maniera più specifica. Infatti, in questo frangente, il punto di contatto nazionale – che funge da collegamento con la piattaforma – deve confermare la corrispondenza evidenziata dal sistema per autorizzare lo scambio informativo e, come condizione aggiuntiva, tale compito spetta anche al personale qualificato mediante un esame manuale delle tracce interessate<sup>44</sup>. Entra così in gioco il necessario intervento umano, evidenziato dalla normativa come correttivo agli eventuali errori della “macchina”.

Occorre precisare che i dati posti alla base del sistema devono rispettare degli *standard* minimi per il loro utilizzo – come un numero minimo di loci per il DNA o la qualità delle immagini dei volti e delle impronte digitali – che dovranno essere definiti dalla Commissione europea con successivi atti integrativi<sup>45</sup>.

Per quanto attiene al collegamento con Europol, si prevede la possibilità di utilizzo dei dati da essa detenuti e, contestualmente, anche la consultazione delle banche dati nazionali da parte dell’Ufficio di polizia europeo. In quest’ultimo caso, come chiarito dall’art. 49 del Regolamento, il passaggio di informazioni avviene solo dopo il soddisfacimento di alcune condizioni. In particolare, Europol deve trasmettere allo Stato membro interessato il nome del Paese terzo che ha fornito i dati oggetto di confronto, una descrizione dei fatti e del reato per cui si procede e, infine, deve confermare la comparazione tramite un esperto qualificato.

La normativa, inoltre, prevede come condizione necessaria, per connettere le banche dati al sistema centrale, una valutazione d’impatto – in continuità con l’art. 27 della dir. n. 680/2016 –, considerando l’elevato rischio che tale trattamento può comportare sui dati e la possibilità di consultare l’autorità nazionale di controllo<sup>46</sup>.

In questo modo, il garante risulta informato sulle condizioni di strutturazione e impiego dei *database* e può svolgere gli opportuni controlli in caso di violazioni.

Il Regolamento, oltre agli aspetti legati alla protezione dei dati contenuti, si ispira al dettato normativo del Regolamento n. 679/2016 (il c.d. GDPR) e della dir. n. 794/2016<sup>47</sup> anche per disciplinare lo scambio di dati a Paesi terzi, mediante l’azione di Europol.

In particolare, Europol può fornire i dati a Nazioni non appartenenti all’Ue – previo consenso dello Stato membro detentore delle informazioni –, in presenza di una decisione di adeguatezza della Commissione

---

Europol dovrà eseguire una nuova analisi per verificare la necessità di conservare i dati e, qualora il periodo complessivo superi i cinque anni, dovrà informare il Garante europeo per la protezione dei dati personali.

<sup>44</sup> Il Regolamento prevede all’art. 72, par. 1, lett. h), una corrispondenza tra profili legati a soggetti noti e tracce repertate sulla scena del crimine, oppure tra singole tracce o tra profili non noti.

<sup>45</sup> Il riferimento a una successiva definizione degli *standard* di qualità è ben visibile negli artt. 9, 13 e 22 del Regolamento.

<sup>46</sup> La necessità della valutazione d’impatto è stata inserita nell’art. 50, par. 4, del Regolamento.

<sup>47</sup> Si tratta del Regolamento istitutivo di *Europol*.

europea<sup>48</sup> o di un accordo internazionale o di cooperazione tra l'Ue e il Paese terzo interessato<sup>49</sup>.

Alla luce del quadro delineato si possono trarre alcune considerazioni.

Innanzitutto, l'aspetto maggiormente problematico è l'inserimento dei sospetti – rifacendosi alla definizione<sup>50</sup> offerta dall'art. 6, lett. a), della dir. n. 680/2016 – tra le categorie di soggetti su cui è possibile eseguire il riconoscimento biometrico e le successive operazioni di scambio tra Forze di polizia.

In tal caso, le previsioni in esame ampliano il novero di candidati fortificando le possibilità investigative ma non forniscono delle vere e proprie distinzioni tra soggetti noti e sospetti. Nel primo caso, trattandosi di persone condannate, si pongono sicuramente minori problemi, mentre per i semplici sospetti non vengono fornite garanzie ulteriori.

Inoltre, si notano continui rinvii ad atti integrativi per definire alcuni aspetti peculiari della disciplina, come l'entrata in vigore della normativa e la definizione dei criteri *standard* di qualità del materiale da scambiare, rendendo di fatto meno organica la materia *de qua*.

La disciplina europea lascia ampissimi margini di manovra agli Stati membri sia nella definizione degli aspetti tecnici (come l'acquisizione degli elementi probatori) che sulle procedure di utilizzo e di scambio dei dati, non diventando pienamente applicabile in questi frangenti.

Questo approccio fa, dunque, scorgere all'orizzonte l'insorgere di normative nazionali che dovranno disciplinare il funzionamento delle nuove banche dati – come quella per il riconoscimento facciale – e le procedure di collegamento con la moderna infrastruttura europea.

Ciò dimostra come, sebbene sia forte l'intenzione delle istituzioni europee di coniugare tra loro le discipline dei singoli Stati membri, non si può ancora affermare che si sia raggiunta un'armonizzazione concreta delle normative<sup>51</sup>, considerando l'enorme distanza esistente tra i legislatori di ciascun contesto nazionale e le zone “d'ombra” ancora presenti.

---

<sup>48</sup> La decisione di adeguatezza è un atto con cui la Commissione europea deve esaminare il livello di protezione dei dati personali offerto dallo Stato non membro dell'Unione europea verso cui andrebbero trasferiti i dati. Per un'analisi dettagliata, si v. F. Balducci Romano, *I trasferimenti di dati personali*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 953 s.

<sup>49</sup> In particolare, l'art. 60 del Regolamento fornisce un rimando all'art. 25 della dir. n. 794/2016, in cui vengono esplicate le condizioni con cui Europol può trasferire i dati.

<sup>50</sup> L'art. 6, lett. a), della dir. 680/2016 annovera i dati delle «[...] persone per le quali vi sono fondati motivi di ritenere che abbiano commesso o stiano per commettere un reato».

<sup>51</sup> In tal senso, D. Curtotti, *Indagini hi-tech, spazio cyber, scambi probatori tra Stati e Internet provider service e “Vecchia Europa”: una normativa che non c'è (ancora)*, in *Dir. pen. proc.*, 2021, 759, la quale ricorda che oggi la difficoltà è nel «[...] trovare soluzioni di bilanciamento, per un verso, tra interessi in gioco quali la sicurezza pubblica e diritti fondamentali (privacy, diritto di difesa, ecc.), e per altro verso tra normative statali ancora distanti tra loro».

## 5. Lo strumento algoritmico nel contesto italiano

Sul fronte nazionale, la situazione non appare più rassicurante.

Innanzitutto, dal punto di vista operativo, è attualmente in funzione il Sistema Automatico di Riconoscimento Immagini (S.A.R.I.) presso la Polizia di Stato.

Quest'ultimo si presenta come un *software*, basato su algoritmi, in grado di confrontare volti ignoti con quelli di soggetti foto-segnalati. Anche in questo caso si possono individuare due distinte procedure operative di suddetto programma, vale a dire le modalità *Enterprise* e *Real-time*<sup>52</sup>.

In particolare, la prima procedura permette di ricercare, mediante un sistema automatico, l'identità di un volto presente in un'immagine all'interno di una banca dati di grandi dimensioni (con un massimo di 10 milioni di immagini), selezionabile di volta in volta dall'operatore. Suddetta attività può avvenire su base volto, su base anagrafica/descrittiva<sup>53</sup> o integrando entrambe le metodologie.

La modalità *Real-time*, invece, permette un riconoscimento in tempo reale su più video provenienti da impianti di video sorveglianza. I volti presenti nei fotogrammi vengono analizzati e confrontati, tramite un algoritmo di riconoscimento, con quelli presenti in una *watchlist* (con un massimo di circa 10.000 volti). Nel caso di *match*, ossia di confronto positivo, il sistema genera un *alert* che permette di avvisare l'operatore.

Detta piattaforma è stata oggetto di varie critiche.

Innanzitutto, la scelta di non inserire degli *standard* minimi per la qualità delle immagini da utilizzare rischia di amplificare il pericolo di un riconoscimento non attendibile<sup>54</sup>, aumentando il tasso di errore<sup>55</sup>.

Sebbene l'uso in differita del SARI sia stato approvato dal Garante per la Protezione dei Dati Personali<sup>56</sup>, altrettanto non può dirsi per il *real-time*. Infatti, in questo caso la decisione negativa dell'autorità amministrativa è dettata dalla mancanza di una normativa, vista come situazione preoccupante per il rischio di sorveglianza massiva<sup>57</sup>.

Dal punto del procedimento penale, bisogna comprendere quale possa essere la portata di uno strumento di tal tipo e se sia effettivamente ascrivibile all'interno degli istituti esistenti; in altre parole, è necessario capire

---

<sup>52</sup> Su suddette modalità Ministero dell'Interno, *Capitolato tecnico. Procedura volta alla fornitura della soluzione integrata per il Sistema Automatico di Riconoscimento Immagini (S.A.R.I.)*, in *polizjadistato.it*, 2016, 14 ss.

<sup>53</sup> La base analitica/descrittiva prevede una ricerca sulla base di informazioni anagrafiche o descrittive associate alle immagini nella banca dati dei soggetti fotosegnalati.

<sup>54</sup> Così, R. Lopez, *La rappresentazione facciale tramite software*, in A. Scalfati (a cura di), *Le indagini atipiche*, II ed., Torino, 2019, 244.

<sup>55</sup> Sul punto, C. Castelluccia-D. Le Métayer, *Analyse des impacts de la reconnaissance faciale. Quelques éléments de méthode*, in *Inria*, 20 novembre 2019, 8.

<sup>56</sup> Cfr. Garante privacy, *Sistema automatico di ricerca dell'identità di un volto*, 26 luglio 2018 (doc. web 9040256).

<sup>57</sup> A tal proposito, Garante privacy, *Parere sul sistema Sari Real Time*, 25 marzo 2021 (doc. web 9575877); R. Lopez, *Videosorveglianza biometrica tramite riconoscimento facciale: parere negativo del Garante per la "privacy"*, in *Proc. pen. giust.*, 2022, 798 ss.

come quest'ultimo si collochi nella tassonomia probatoria.

Innanzitutto, non appare molto condivisibile l'impostazione fornita da parte della dottrina<sup>58</sup> per cui il riconoscimento facciale sarebbe accostabile, seppur sotto forma di "filiazione spuria"<sup>59</sup>, all'individuazione di persone e cose prevista dall'art. 361 c.p.p.

*In primis*, per lo scopo di questa disposizione. Non a caso, quest'ultima punta maggiormente alla "necessaria prosecuzione delle indagini" piuttosto che ad un suo possibile utilizzo in sede processuale. Infatti, sebbene il risultato dell'attività possa giungere nella fase di giudizio mediante l'*escamotage* della testimonianza dell'"individuatore", nella sostanza l'atto rimane nelle mani del p.m. e, tendenzialmente su sua delega, della p.g. e si colloca direttamente nelle indagini preliminari.

In secondo luogo, si tratta di un istituto piuttosto scarno<sup>60</sup>, privo di una descrizione dettagliata delle modalità esecutive e documentative e influenzato dalla capacità mnemonica e dalle condizioni psicofisiche della persona chiamata a svolgere l'individuazione<sup>61</sup>.

Sarebbe, quindi, impensabile assimilare la capacità di un soggetto a fare un "riconoscimento" con quella di un sistema algoritmico che punta a confrontare meccanicamente le caratteristiche dei volti. Si rischierebbe di confondere i processi della mente umana con quelli della macchina.

Analoghi problemi interpretativi si pongono anche con riferimento alla tesi di un uso "pacifico" dello strumento per le finalità dell'art. 349 c.p.p.<sup>62</sup>. Proprio sul fronte delle attività volte all'identificazione dell'indagato, la norma prevede la possibilità di eseguire «[...] ove occorra, rilievi dattiloscopici, fotografici e antropometrici nonché altri accertamenti».

Innanzitutto, risulterebbe complesso ridurre l'operazione di confronto e di analisi svolta dallo strumento tecnologico alle sole ipotesi previste dalla disposizione in esame.

Come evidenziato dalla dottrina<sup>63</sup>, anche con riferimento alle altre tipologie di attività, il concetto di identificazione si è sviluppato mentre il dato normativo sembra ancora risentire di un mancato adeguamento all'odierna realtà operativa d'indagine.

Sicuramente il rilievo fotografico – connotato da una meccanicità dell'attività posta in essere<sup>64</sup> – risiede maggiormente nel fotosegnalamento del

---

<sup>58</sup> Tra gli altri, R. Lopez, *La rappresentazione facciale tramite software*, cit., 253.

<sup>59</sup> *Ibidem*.

<sup>60</sup> Sui problemi della disciplina dell'art. 361 c.p.p., fra gli altri, si v. T. Alesci, *Il corpo umano fonte di prova*, Padova, 2017, 92 s.

<sup>61</sup> Dal punto di vista dell'"individuatore" bisogna ricordare che ci sono dei fattori, sia di tipo emotivo che fisico, che possono distorcere la ricostruzione e il conseguente ricordo dell'immagine della persona da riconoscere. Su questi profili, G. Cecanese, *Aspetti problematici e snodi interpretativi dell'individuazione di persone e di cose*, in *Arch. pen.*, 2018, 1, 20; D. Mastro, *Le cause degli errori giudiziari e i meccanismi di prevenzione e riparazione delle condanne e imputazioni ingiuste*, in *Rev. Bras. dir. proc. pen.*, 8(3), 2021, 1383 ss.

<sup>62</sup> Così, M. Torre, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Dir. pen. proc.*, 8, 2021, 1052 ss.

<sup>63</sup> Su questi profili si rimanda alla puntuale analisi di D. Curtotti, *Rilievi e accertamenti tecnici*, Milano, 2013, 108 ss.

<sup>64</sup> In tema, A. Chelo, *Rilievi, accertamenti e accertamenti tecnici*, in C. Conti, A. Marandola (a

soggetto piuttosto che in una successiva operazione di confronto tra l'immagine della persona sottoposta alle indagini e quelle conservate in un'apposita banca dati, specialmente considerando che la seconda attività ha un grado di complessità maggiore e i suoi risultati sono connotati da un valore probatorio più profondo<sup>65</sup>.

A tal proposito, non va trascurato l'ingente apporto che dovrebbe essere fornito dagli operatori che procedono al riconoscimento algoritmico, cadendo quindi in un accertamento, per verificare l'attività svolta dalla macchina. Si potrebbe ragionevolmente pensare che sia ricompreso negli "altri accertamenti" richiamati dalla disposizione *de qua*, ma ciò rischierebbe di ampliare eccessivamente le maglie entro cui può muoversi la p.g. nell'espletamento delle operazioni identificative, senza esplicitare i limiti di un insieme di operazioni piuttosto invasive per il soggetto *ivi* sottoposto. Inoltre, la finalità delle attività identificative si dovrebbe ridurre ad una valenza meramente indiziaria e, quindi, per l'immediata prosecuzione delle indagini<sup>66</sup>.

Al pari, non convince neppure una possibile interpretazione estensiva dell'art. 189 c.p.p. Difatti, la c.d. "prova atipica" consta di tre importanti limiti, ossia deve essere idonea ad accertare il fatto da provare, deve rispettare la libertà morale dei soggetti coinvolti e, sotto il punto di vista processuale, richiede un contraddittorio anticipato tra le parti sulle modalità di acquisizione probatoria<sup>67</sup>. Applicare questi criteri al riconoscimento facciale non appare molto agevole<sup>68</sup>, considerando che questa disposizione rappresenta un vero e proprio "escamotage investigativo"<sup>69</sup>.

Innanzitutto, l'autorità giudiziaria non ha modo di valutare in maniera concreta l'idoneità del *software* per i fini di accertamento del fatto<sup>70</sup>. Ciò è dovuto alla circostanza per cui la procedura eseguita per individuare la persona e, conseguentemente, le componenti specifiche – vale a dire il tasso di errore, la grandezza del *dataset* di cui è costituito e la qualità delle

---

cura di), *La prova scientifica*, Milano, 2023, 711 ss.; D. Curtotti, *Rilievi e accertamenti tecnici*, cit., 14 ss.

<sup>65</sup> In tal senso, R.E. Kostoris, *Prelevi biologici coattivi*, in R.E. Kostoris-R. Orlandi (a cura di), *Contrasto al terrorismo interno e internazionale*, Torino, 2005, 329.

<sup>66</sup> In argomento, P.P. Paulesu, Sub art. 349 c.p.p., in A. Giarda-G. Spangher (a cura di), *Codice di procedura penale commentato*, VI ed., II, Padova, 2023, 1678 ss.

<sup>67</sup> Con riferimento ai dubbi interpretativi legati alla possibile lettura estensiva dell'art. 189 c.p.p., si v., fra gli altri, C. Conti, Sub art. 189 c.p.p., in A. Giarda-G. Spangher (a cura di), *Codice di procedura penale commentato*, I, cit., 2601 ss.; P. Ferrua, *Ammissibilità della prova e divieti probatori*, in *Rev. Bras. dir. proc. pen.*, 7(1), 2021, 228 s.; A. Procaccino, *Prove atipiche*, in A. Gaito (a cura di), *La prova penale*, Milano, 2008, 265 ss.; P. Tonini-C. Conti, *Il diritto delle prove penali*, II ed., Milano, 2014, 196 ss.

<sup>68</sup> Su questo profilo, tra gli altri, G. Borgia, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, in *Legisl. Pen.*, 11 dicembre 2021, 23.

<sup>69</sup> Come ben sottolinea A. Scalfati, *IA e processo penale: prospettive d'impiego e livelli di rischio*, in *Proc. pen. giust.*, 2024, 1408, l'art. 189 c.p.p. diventa «[...] il canale mediante cui profittarne [...]», creando rischi sui diritti fondamentali e contestazioni sul risultato probatorio prospettato.

<sup>70</sup> In tema, A. Marandola, *Il riconoscimento facciale*, in C. Conti-A. Marandola (a cura di), *La prova scientifica*, cit., 510 s.

immagini utilizzate – dello strumento sono avvolte da un’opacità, piuttosto ardua da contrastare, che non permette di conoscere questi elementi costitutivi<sup>71</sup>, considerando che la valutazione deve essere svolta *ex ante*<sup>72</sup>.

Questo insieme di profili critici rende, quindi, difficoltoso un possibile ricorso all’atipicità, in vista di una carenza di garanzie minime che assicurino l’affidabilità degli elementi probatori raccolti. Si rischierebbe, così, di cadere in un’inutilizzabilità dei risultati appresi, permettendo delle vere e proprie “scorciatoie probatorie”<sup>73</sup>.

Si pone su un terreno piuttosto scivoloso anche la prospettiva offerta dalle Forze di polizia<sup>74</sup>, in cui l’attività verrebbe qualificata come “accertamento tecnico”. Un’impostazione di tal tipo rischierebbe di far entrare suddetto “*genus*” di attività identificativa, come già evidenziato piuttosto opaca, nel processo penale.

In particolare, la tipologia di attività da eseguire, avendo prevalentemente carattere ripetibile, verrebbe ricompresa nell’alveo delle operazioni dell’art. 359 c.p.p. e, in casi particolari e residuali, nell’art. 354 c.p.p.

Così facendo, vengono meno le garanzie difensive e, come analizzato da alcuni<sup>75</sup>, queste norme non danno contezza dei limiti applicativi entro cui possono spingersi le Forze di polizia nell’applicazione dello strumento.

Inoltre, questo disposto normativo risulta anche carente, se applicato allo strumento in esame, di un vero e proprio controllo da parte dell’autorità giudiziaria.

## 6. Prospettive de *jure condendo*

Alla luce delle osservazioni svolte in sede investigativa e della ricostruzione delle possibili interpretazioni possono sicuramente trarsi alcune considerazioni sistematiche.

Innanzitutto, l’attuale panorama legislativo non pare offrire in questa delicata materia sufficienti garanzie all’utilizzo di moderni strumenti tecnici d’indagine, come quelli di tipo algoritmico. Si assiste a una realtà a doppia velocità, dove la tecnologia continua a fare numerosi passi in avanti e il diritto non riesce a svilupparsi di pari passo<sup>76</sup>.

---

<sup>71</sup> Sul punto, J. Della Torre, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?*, in G. Di Paolo-L. Pressacco (a cura di), *Intelligenza artificiale e processo penale. Indagini, prove e giudizio*, Trento, 2022, 38 s.; M. Gialuz, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA.VV., *Giurisprudenza penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, 64 s.

<sup>72</sup> In tal senso, E. Aprile, *La prova penale*, Milano, 2002, 60 s.

<sup>73</sup> Così, F.R. Dinacci, *Le regole generali delle parole*, in G. Spangher (a cura di), *Procedura penale. Teoria e pratica del processo*, I, Torino, 2015, 776; A. Scalfati-D. Servi, *Premesse sulle prove penali*, in A. Scalfati (a cura di), *Trattato di procedura penale*, II, I – *Le prove*, Torino 2008, 28 ss.

<sup>74</sup> In argomento, Ministero dell’Interno, *Sistema automatico di riconoscimento immagini: un futuro che diventa realtà*, in *interno.gov*, 19 settembre 2021.

<sup>75</sup> Tra gli altri, J. Della Torre, *Tecnologie di riconoscimento facciale e procedimento penale*, in *Riv. it. dir. proc. pen.*, 3, 2022, 1084 s.

<sup>76</sup> Su questo aspetto si rimanda all’analisi di D. Curtotti, *L’inadeguatezza delle norme al*

Sebbene una parte della dottrina<sup>77</sup> abbia tentato di colmare la lacuna legislativa con delle interpretazioni di sistema, queste soluzioni non sembrano molto praticabili. Infatti, al pari di quanto avvenuto in tema di prova scientifica<sup>78</sup>, il codice di rito risente ancora di un'obsolescenza delle sue norme – essendo ancora legato all'impianto originario di un procedimento penale ancora formalmente polarizzato sulla fase dibattimentale – che non permette un adattamento a “nuovi” strumenti come quelli algoritmici, non contemplando le garanzie minime che il procedimento penale contemporaneo richiede.

Al contempo, proprio sul fronte delle nuove tecnologie – specialmente nel caso del riconoscimento facciale – non sembra auspicabile neppure un adattamento *tout court* a impostazioni dottrinali per cui tutte le attività non espressamente vietate dalla legge sono da considerarsi pienamente lecite<sup>79</sup>, per via delle potenzialità dello strumento biometrico e dell'alta invasività sui diritti e sulle libertà dei soggetti interessati. In questo modo, infatti, si rischia di far entrare nel procedimento (o peggio ancora nel processo) elementi provenienti da uno strumento opaco, ancora poco controllato, connotandoli di un'utilizzabilità intrinseca con l'*escamotage* dell'art. 189 c.p.p. Emerge chiaramente, come auspicato da parte della dottrina, l'esigenza di introdurre una disposizione normativa che fissi l'*an* e il *quomodo* di utilizzo di queste moderne strumentazioni<sup>80</sup>.

Anche il legislatore è conscio di questa necessità<sup>81</sup>.

---

*cospetto della nuova realtà investigativa e le soluzioni giuridiche percorribili*, in D. Curtotti-L. Saravo (a cura di), *Manuale delle investigazioni sulla scena del crimine*, II ed., Torino 2022, 171 ss.; M. Tallacchini, *Scienza e tecnologia: paradigmi normativi e nuove tecnologie*, in P. Tincani (a cura di), *Diritto e futuro dell'Europa*, Colle di Val d'Elsa, 2021, 135 ss.

<sup>77</sup> V., tra gli altri, R. Lopez, *La rappresentazione facciale tramite software*, cit., 253; M. Torre, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, cit., 1052 ss.

<sup>78</sup> Si v., fra gli altri, E. Aprile, *Le indagini tecnico-scientifiche: problematiche giuridiche sulla formazione della prova penale*, in *Cass. pen.*, 2003, 4034; C. Bonzano, *Prova “scientifica”: le garanzie difensive tra progresso tecnologico e stasi del sistema*, in C. Conti (a cura di), *Scienza e processo penale. Nuove frontiere e vecchi pregiudizi*, Milano 2011, 116; A. Camon, *La fase che “non conta e non pesa”: indagini governate dalla legge?*, in *Dir. pen. proc.*, 2017, 425 s.; D. Curtotti, *Rilievi e accertamenti tecnici*, cit., 161 s.; P. Felicioni, *La prova del DNA nel procedimento penale*, Torino 2018, 11; A. Scalfati, *La deriva scienziata dell'accertamento penale*, in *Proc. pen. giust.*, 2011, 148.

<sup>79</sup> Su questa impostazione, F. Cordero, *Tre studi sulle prove penali*, Milano, 1963, 157 ss.

<sup>80</sup> In tal senso, J. Della Torre, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., 1093; W. Nocerino, *Sulle modalità di acquisizione delle immagini provenienti dalle videocamere di sorveglianza*, cit., 2425; C. Pallante, *Identità e identificazione: uno scopo, tante normative*, cit., in *press*; A. Scalfati, *LA e processo penale: prospettive d'impiego e livelli di rischio*, cit., 1409; M. Torre, *Il Regolamento europeo sull'intelligenza artificiale: i profili processuali*, in *Proc. pen. giust.*, 6, 2024, 1544.

<sup>81</sup> Sulla necessità di una normativa, si sono registrate alcune piccole aperture anche da parte del legislatore. Infatti, in un primo momento è stata approntata una prima proposta di legge che bloccasse temporaneamente l'installazione e l'uso di impianti di videosorveglianza che utilizzano sistemi di riconoscimento facciale, nell'attesa di una normativa che ne disciplinasse i relativi limiti, senza tuttavia riuscire nell'intento (Proposta n. 3009/2021). Successivamente, con la L. n. 205 del 3 dicembre 2021, di conversione del D.lgs. n. 139 dell'8 ottobre 2021 recante “*Disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali*”, il Parlamento ha previsto nell'art. 9, co. 9, un blocco dell'installazione

Inoltre, sul fronte dei diritti solo l'esplicitazione dei limiti<sup>82</sup> può fornire un effettivo contemperamento tra i fini securitari e i diritti dei cittadini coinvolti. Non bisogna, infatti, trascurare che libertà e sicurezza rappresentano due facce di una stessa medaglia<sup>83</sup> e non più degli interessi totalmente contrapposti tra loro.

Al contrario, uno scenario privo di limiti espliciti – in cui l'uso di queste strumentazioni sia permesso *tout court* e dove i risultati possono fornire una base per l'accertamento dei fatti – rischia di formare la base di un controllo massivo sui cittadini<sup>84</sup>.

Analizzando le vicissitudini del sistema francese appare piuttosto ovvia questa considerazione di sistema. Infatti, il rischio di un aggiramento della normativa e, quindi, di un utilizzo incontrollato degli strumenti algoritmici è sempre presente.

Le esperienze internazionali insegnano proprio questi aspetti.

Sebbene possa sembrare potenzialmente «illusorio»<sup>85</sup>, unicamente la predisposizione di peculiari normative può contribuire a rendere maggiormente trasparenti gli strumenti investigativi, mirando a fornire le opportune garanzie per i soggetti coinvolti.

Con ciò non si vuole limitare l'attività investigativa con un eccessivo formalismo giuridico ma si intende garantire che quest'ultima sia conforme ai principi di uno Stato di diritto, all'interno di un ordinamento che, al giorno d'oggi, risulta essere ancora orfano di regole<sup>86</sup>.

Come già accaduto per alcuni ritrovati della tecnica<sup>87</sup>, anche in questo fran-

---

e dell'utilizzazione di impianti di tal tipo in luoghi pubblici o aperti al pubblico fino all'emanazione di una disciplina legislativa *ad hoc*, fornendo come termine ultimo il 31 dicembre 2023. Allo stato, non risulta ancora pronta un'effettiva normativa in materia ma il legislatore, mediante l'art. 8-ter della L. n. 87 del 3 luglio 2023 di conversione del D. l. n. 51 del 10 maggio 2023 “*recante disposizioni urgenti in materia di amministrazione di enti pubblici, di termini legislativi e di iniziative di solidarietà sociale*”, ha preferito prorogare il termine previsto al successivo 31 dicembre 2025. Su questa ricostruzione, F. Di Matteo, *La riservatezza dei dati biometrici nello spazio europeo dei diritti fondamentali: sui limiti all'utilizzo delle tecnologie di riconoscimento facciale*, in *Freedom, security & justice: European legal studies*, 2023, 1, 110; A. Procaccino, *Soft law e giustizia penale*, Pisa, 2023, 56 s.

<sup>82</sup> In tema, J. Della Torre, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in *Dir. pen. cont.*, 2020, 1, 243 s.; E. Sacchetto, *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, in *Legisl. pen.*, 16 ottobre 2020, 13 s.; *Ead.*, *Spunti per una riflessione sul rapporto tra biometria e processo penale*, in *Dir. pen. cont.*, 2, 2019, 477.

<sup>83</sup> Su questo peculiare concetto, W. Nocerino, *Le intercettazioni e i controlli preventivi*, cit., 393 s.

<sup>84</sup> In tal senso, M. Colacurci, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in G. Balbi-F. De Simone-A. Esposito-S. Manacorda (a cura di), *Diritto penale e intelligenza artificiale*, Torino, 2022, 126; W. Nocerino, *Le intercettazioni e i controlli preventivi*, cit., 384.

<sup>85</sup> Così, G.M. Baccari-C. Conti, *La corsa tecnologica tra Costituzione, codice di rito e norme sulla privacy: uno sguardo d'insieme*, in *Dir. pen. proc.*, 2021, 721 s.

<sup>86</sup> In questo senso, D. Curtotti, *L'inadeguatezza delle norme al cospetto della nuova realtà investigativa e le soluzioni giuridiche percorribili*, in D. Curtotti-L. Saravo (a cura di), *Manuale delle investigazioni sulla scena del crimine*, II ed., Torino, 2022, 171 ss.; *Ead.*, *Procedimento penale e intelligence in Italia: un'osmosi inevitabile, ancora orfana di regole*, in *Proc. pen. giust.*, 2018, 435 ss.

<sup>87</sup> Sul punto, si v., fra gli altri, W. Nocerino, *Il tramonto dei mezzi di ricerca della prova nell'era*

gente ci si trova di fronte a un problema tipicamente normativo. In questi casi, infatti, la giurisprudenza ha cercato di sopperire alle carenze legislative, fornendo agli interpreti possibili coordinate sistemiche nelle categorie probatorie esistenti<sup>88</sup>.

Nel contempo, anche le Corti sovranazionali hanno tentato di fornire possibili risposte<sup>89</sup>.

Sicuramente, un legislatore assente che si affida alle “cure” costanti della giurisprudenza non sembra essere una soluzione appagante, con il pericolo di generare nuove “zone grigie” e di non regolare una materia connotata da profili critici e da continue opacità<sup>90</sup>.

Non sembra neppure sostenibile una posizione di totale chiusura verso queste nuove potenzialità investigative, con il rischio di indebolire l’efficienza investigativa in ragione delle prerogative individuali<sup>91</sup>.

Guardando al modello francese, anche con riferimento ad altri strumenti tecnici<sup>92</sup>, è probabilmente giunto il momento di riflettere su possibili interventi normativi che ne riescano a fornire un’organicità e una precisa

---

2.0, in *Dir. pen. proc.*, 2021, 1029 s.

<sup>88</sup> Si pensi, più recentemente, a quanto avvenuto in materia di indagini su piattaforme criptate e di trojan, in cui si sono susseguite molteplici sentenze della Corte di Cassazione. Su questo profilo, si v., tra gli altri, W. Nocerino, *Ancora in tema di criptofonini: nuovi arresti giurisprudenziali in attesa delle Sezioni Unite*, in *Pen. DP*, 3, 2023, 485 ss.; *Ead.*, *Le Sezioni Unite risolvono l’enigma: l’utilizzabilità del “catturatore informatico” nel processo penale*, in *Cass. pen.*, 2016, 3546 ss.; V. Rizzi-D. Curtotti-A.M. Russitto-G. Giliberti-G. Scarpa-W. Nocerino, *Piattaforme criptate e prova penale. L’etere digitale alla sfida del codice di rito*, in *Polizia moderna*, 8, 2023, 50 ss.

<sup>89</sup> Si pensi alla sentenza *Glukhin vs. Russia* del 2023, con cui la Corte Europea dei diritti dell’uomo arriva a riconoscere, per la prima volta, il pieno utilizzo in sede investigativa del riconoscimento facciale, pur in mancanza di atti investigativi che ne “testimonino” l’effettivo uso. Questa conclusione viene suffragata dall’identificazione di un cittadino moscovita in sole 48 ore e dalle attività di estrazione dei filmati dalle videocamere della metropolitana di Mosca da parte delle forze di polizia. Sulla base di questi elementi, la Corte si trova a sviluppare il ragionamento già intrapreso con la sentenza *Gaughran vs. United Kingdom* del 2020, in cui aveva riconosciuto un potenziale rischio per le libertà nella conservazione delle immagini da parte delle forze di polizia – le quali possono razionalmente confluire in futuri *database* investigativi –, sino a introdurre il riconoscimento facciale nell’alveo dell’art. 8 CEDU, richiamando l’esigenza di una riserva di legge che perimetri l’uso di tale strumento. Cfr. CEDU, *Glukhin c. Russia*, ric. 11519/20 (2023), in *Proc. pen. giust.*, 2024, 413, con nota di O. Bruno, *La condanna per manifestazione pacifica (non preavvisata) e con riconoscimento facciale viola i diritti fondamentali*; G. Gallo, *Tecnologie di riconoscimento facciale e diritti fondamentali a rischio: il caso Glukhin c. Russia dinanzi alla Corte europea dei diritti dell’uomo*, in questa *Rivista*, 3, 2023, 195 ss.; G. Mobilio, *La Corte EDU condanna il ricorso alle tecnologie di riconoscimento facciale per reprimere il dissenso politico: osservazioni a partire dal caso Glukhin c. Russia*, in *DPCE online*, 2024, 1, 695 ss.; C. Nardocci, *Il riconoscimento facciale sul “banco” degli imputati. Riflessioni a partire, e oltre, Corte EDU Glukhin c. Russia*, in *Biolum journal*, 2024, 1, 279 ss.

<sup>90</sup> F. Paolucci, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in questa *Rivista*, 2021, 1, 216.

<sup>91</sup> In questo senso, L. Camaldo, *Intelligenza artificiale e investigazione penale predittiva*, in *Riv. it. dir. proc. pen.*, 2024, 1, 249 s.

<sup>92</sup> Sul punto, S. Guinchard-J. Buisson, *Procédure pénale*, cit., 557 s.; W. Nocerino, *Ancora in tema di criptofonini: nuovi arresti giurisprudenziali in attesa delle sezioni unite*, cit., 487 ss.; E. Vergès, *La procédure pénale technicienne (ou l’asphyxie procédurale)*, in *Revue de sciences criminelles*, 3, 2019, 673 ss.

collocazione nel codice di rito.

Si potrebbe pensare a una norma aperta che punti a circoscrivere l'attività apprensiva e non il singolo strumento. Una sorta di "acquisizione di immagini biometriche", ossia un nuovo mezzo di ricerca della prova la cui titolarità (in termini di atti autorizzativi) potrebbe spettare alla giurisdizione e, in casi urgenti, all'organo inquirente.

In questo modo si potrebbero prevenire eventuali rischi di obsolescenza normativa, permettendo gli appositi adattamenti del testo legislativo ai mutamenti della società e della tecnica.

La norma, inoltre, potrebbe fungere da base anche per disciplinare la Banca dati SARI, inserendo le garanzie minime (tecniche e giuridiche) per connotare il risultato comparativo di un'elevata affidabilità processuale.

Così, si scongiurerebbe il rischio paventato dal Garante privacy di utilizzi massivi degli strumenti di riconoscimento biometrico<sup>93</sup>, restituendo una dimensione investigativa a strumenti nati in sede preventiva.

Allo stesso modo – senza sacrificare eccessivamente le prerogative individuali – si individuerebbero l'*an* e il *quomodo* di attività di tal tipo, perimetrando e rispettando il principio di proporzionalità.

Dunque, se quest'ultimo appare essere il più nobile obiettivo, non resta che attendere che i singoli legislatori nazionali e, più nello specifico quello italiano, forniscano indicazioni volte a perimetrare queste nuove potenzialità investigative e, soprattutto, a far comprendere i possibili utilizzi in sede probatoria.

---

<sup>93</sup> In tema, Garante privacy, *Parere sul sistema Sari Real Time*, 25 marzo 2021 (doc. web 9575877), cit.

### **Abstract**

Negli ultimi anni, le nuove tecnologie dotate di intelligenza artificiale (IA) hanno iniziato a permeare ogni aspetto della vita quotidiana, trasformando radicalmente il modo in cui ogni persona si relaziona con il mondo. A partire da queste semplici applicazioni, l'IA sta progressivamente potenziando il suo raggio d'azione, entrando a pieno titolo anche nelle dinamiche dell'investigazione penale. Ne costituisce un classico esempio l'impiego dell'IA a fini di riconoscimento facciale che consente di eseguire analisi sui tratti biometrici del volto per confrontarli con le caratteristiche inserite in un apposito *database*, nonché di conservarli all'interno della banca dati. Partendo da queste considerazioni preliminari, lo scritto analizza l'uso crescente dell'IA nel procedimento penale con particolare riferimento al riconoscimento facciale, ponendo l'attenzione sulle sue principali applicazioni investigative all'interno della legislazione nazionale ed eurounitaria.

In recent years, new technologies equipped with artificial intelligence (AI) have begun to permeate every aspect of daily life, radically transforming the way in which each person relates to the world. Starting with these simple applications, AI is gradually expanding its scope, becoming an integral part of criminal investigation. A classic example of this evolution is the use of AI for facial recognition, which allows biometric facial features to be analyzed and compared with characteristics stored in a specific database, as well as stored within the database itself. Starting from these preliminary considerations, this paper analyzes the growing use of AI in criminal proceedings, with particular reference to facial recognition technologies, focusing on its main investigative applications within national and EU legislations

### **Keywords**

intelligenza artificiale – riconoscimento facciale – indagini preliminari – Prüm II – giustizia penale