L'identificazione della persona nei cui confronti vengono svolte le indagini attraverso l'intelligenza artificiale (IA)

di GIULIO ERRICO

SOMMARIO: 1. Introduzione. — 2. L'IA come sistema. — 3. Il riconoscimento facciale.

1. Introduzione.

Parafrasando l'*incipit* di un celebre scritto, si potrebbe dire che lo spettro dell'IA è alle porte del processo penale.

Gli sforzi profusi dal legislatore per evitare che la razionalizzazione delle applicazioni investigative di simili tecnologie sia devoluta all'elaborazione pretoria sembrerebbero cedere il passo all'inarrestabile forza della transizione digitale.

Si parla, non a caso, di quarta rivoluzione industriale (1). Vale a dire, di un fenomeno complesso che non potrà non dispiegare i propri effetti sul sistema processuale penale.

Se è certo, però, che l'IA, fulcro del moto rivoluzionario, obbligherà tutti gli attori del processo a misurarsi con essa, non è altrettanto chiaro quando l'interprete sarà chiamato a farlo.

Il quesito potrebbe trovare una risposta nell'iniziativa annunciata, lo scorso anno, all'esito dell'incontro tenutosi presso il Viminale, cui hanno preso parte i Ministri dell'Interno, dello Sport e i vertici del mondo del calcio e ribadita nel corso della recente con-

(1) A. RANGONE, *Comprendere e governare la quarta rivoluzione industriale*, Torino, 2022, 54.

ferenza organizzata dall'Associazione Stampa Estera in Italia (2).

È stata, infatti, resa nota l'intenzione di introdurre in tutti gli stadi italiani dei dispositivi di riconoscimento facciale per "assicurare alla giustizia" (3) i responsabili degli illeciti commessi durante le manifestazioni sportive.

Il sistema permetterebbe di risalire in tempo reale all'identità dei tifosi mediante algoritmi di *deep learning*: modelli di apprendimento non supervisionato (senza l'intervento umano) che, sfruttando numerosi livelli computazionali, sono in grado di analizzare dati, confrontali ed elaborare autonomi processi decisionali.

Una fitta trama di reti neurali che replica, sostanzialmente, i meccanismi di funzionamento dell'apprendimento e del ragionamento umano.

Volgendo lo sguardo alle possibili implicazioni processuali, si avrà che all'individuazione del tifoso al quale è attribuito un reato (4) potrà procedere una macchina dotata d'intelligenza, astrattamente in grado di sostituirsi alla polizia giudiziaria (5).

La prospettiva genera, tuttavia, sentimenti contrastanti.

Il dibattito sull'uso di tecnologie dotate di ragionamento vede, in effetti, contrapporsi tesi "oltranziste", il cui principale limite risiede nel trascurare un dato, ormai, inconfutabile: l'IA farà ingresso nel processo penale (6), indipendentemente dalle opinioni di chi ne intravede le enormi potenzialità e di chi, invece, ne avversa l'impiego.

(2) *https://www.radioradicale.it/scheda/748592/conferenza-stampa-con-il-ministro-per-lo-sport-e-i-giovani-andrea-abodi/stampa-e-regime* - Conferenza stampa del 10/10/2025.

(3) F. Bianchi, *Riconoscimento facciale, ecco come funzionerà (solo uno stadio è già pronto)*, in *Repubblica*, Spycalcio, art. *web* del 3 ottobre 2024.

(4) Non sembrerebbe essere d'ostacolo la disposizione di cui al primo capoverso dell'art. 349 c.p.p., nella parte v'è scritto che, oltre ai rilievi dattiloscopici, fotografici e antropometrici, sono ammessi «altri accertamenti».

(5) L. Algeri, *Cybercrime*, in *Omnia, Trattati giuridici*, IIª ed., diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano, 2023, 1766.

(6) R. Lopez, *Le indagini atipiche*, in *Leggi penali tra regole e prassi*, IIª ed., a cura di A. Scalfati, Torino, 2019, 256.

Parrebbe, allora, più proficuo spostare l'attenzione del discorso sul tema delle garanzie (7), unico strumento per fronteggiare eventuali applicazioni dell'IA incompatibili coi valori del giusto ed equo processo (artt. 111 Cost. e 8 CEDU).

Così, nel caso di procedure di identificazione che avvengano secondo le modalità escogitate per la repressione della violenza negli stadi, potrebbero trovare applicazione gli artt. 189, 213 ss. e 361 c.p.p.

Si tratterebbe, del resto, di una prova non vietata, né disciplinata dalla legge che, conducendo all'individuazione dell'autore del fatto senza pregiudicarne la libertà morale, sembra ammissibile.

In ogni caso, non può trascurarsi la necessità (8) di risalire alla logica delle scelte compiute dalla macchina. Soltanto la trasparenza delle procedure non supervisionate può, in effetti, garantire un impiego dell'IA conforme ai valori che temprano l'ordinamento processuale (9).

Per tale ragione, qualora sia possibile ricostruire il percorso deduttivo seguito dalla macchina intelligente, la prova potrà essere assunta secondo lo schema previsto dall'art. 213 c.p.p.

S'imporrebbe, per la polizia giudiziaria, l'assolvimento di obblighi descrittivi, utili all'individuazione degli elementi conoscitivi sintetizzati dall'output e di tutte quelle circostanze che influiscono «sull'attendibilità del riconoscimento».

Un simile approccio contribuisce ad abbattere il rischio di errori, come quello verificatosi, il 13 aprile 2024, ai danni di un tifoso brasiliano: scambiato per un pericoloso criminale dagli scanner di riconoscimento facciale installati presso uno stadio del Sergipe e tratto in arresto durante lo svolgimento del *match* calcistico.

(7) D. Polidoro, *Tecnologie informatiche e procedimento penale: la giustizia penale "messa alla prova" dall'intelligenza artificiale*, in *Archivio Penale*, n. 3/2020, 33.

(8) F. Agrusti, *Educazione e intelligenza artificiale*, Roma, 2023, 22.

(9) G. Padula, *Intelligenza artificiale e giudizio penale: scenari, limiti e prospettive*, in *Processo Penale e Giustizia*, n. 6/2021, 4.

2. L'IA come sistema.

La scelta del legislatore del 1989, di optare per un compromesso nel prevedere l'ammissibilità di prove non disciplinate dalla legge, sebbene per molti aspetti sia stata lungimirante, per altri si è rivelata infelice (10).

È stato autorevolmente osservato (11) come l'art. 189 c.p.p. sia stato talvolta utilizzato per aggirare i requisiti delle prove tipiche, con conseguenti responsabilità da parte della giurisprudenza che, "*contrabbandando omissioni o irritualità come semplici profili di atipicità*", avrebbe svilito un prezioso strumento di integrazione del sistema probatorio.

Un simile pericolo sembrerebbe riguardare, da vicino, anche l'IA.

I risultati probatori ottenuti mediante sistemi dotati di questa tecnologia, che hanno trovato nel regolamento UE n. 1689 del 2024 un primo riconoscimento sostanziale, potrebbero far ingresso nel processo penale attraverso il disposto dell'art. 189 c.p.p., ancorché il codice di rito non contempli delle modalità che ne disciplinino l'assunzione.

Basti pensare alla possibilità di accertare l'identità di un soggetto con dispositivi di riconoscimento facciale.

Il dato conoscitivo acquisito tramite il sistema di IA, la cui attendibilità potrebbe finanche essere maggiore rispetto al processo (umano e, dunque, limitato) di percezione ed elaborazione delle informazioni apprese dalla realtà esterna (12), parrebbe rispondere ai criteri dettati dal legislatore per l'assunzione delle prove innominate.

D'alto canto, se la scansione di dati biometrici, a cui ogni giorno ci si sottopone per sbloccare uno *smartphone*, «non pregiu-

(10) O. Mazza, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *Dir. pen. contemp.*, n. 3/2013, 8.

(11) P. Tonini, *Diritto processuale penale*, Milano, 2012, 183.

(12) Come per i reati commessi in occasione di manifestazioni sportive e non. La capacità di questi complessi strumenti *software* e *hardware* di sviluppare autonomi processi decisionali per risalire all'identità di uno o più facinorosi potrebbe rivelarsi molto più efficace del riconoscimento operato dal singolo agente di p.g.

dica la libertà morale della persona» (13), è indubbio che l'analisi, l'implementazione e il raffronto di tali caratteristiche dell'individuo possano rappresentare delle informazioni utili ad «assicurare l'accertamento dei fatti (art. 189 c.p.p.)».

Siffatta interpretazione, non condivisa da taluni (14), presta però il fianco a pratiche devianti (15).

Dietro la complessità dei processi decisionali attuati dalla macchina "addestrata" si cela, infatti, il rischio che gli elementi sintetizzati dall'IA vengano introdotti nel giudizio eludendo le regole poste a presidio del principio di legalità processuale (16).

Così, nel caso dell'individuazione di un soggetto avvenuta mediante scanner di riconoscimento facciale che, tra i dati elaborati per generare il risultato probatorio, abbia valorizzato scritti anonimi (art. 240 c.p.p.) o informazioni su voci correnti nel pubblico (art. 234, co. 3, c.p.p.), si finirebbe per legittimare una prova contraria ad espressi divieti normativi.

O, ancora, una prova irrituale.

Come nell'ipotesi in cui input ed output siano costituiti da *frames* estratti da videoregistrazioni avvenute in luoghi riservati (17), ove si assisterebbe ad un evidente aggiramento delle disposizioni dettate per le intercettazioni delle comunicazioni, che verrebbe dissimulato dagli algoritmi di *deep learning* (18).

Gli esempi addotti impongono di riflettere sue due questioni.

(13) A Bonomi, *Libertà morale e accertamenti neuroscientifici: profili costituzionali*, in *Biodiritto*, n. 3/2017, 148.

(14) J. Della Torre, *Intelligenza artificiale e processo penale*, in *Quaderni della Facoltà di Giurisprudenza*, Università di Trento, 2022, n. 63, 38.

(15) O. Mazza, *op. cit.*, 5.

(16) S. Moccia, *Massimo Nobili: il costume della legalità*, in *Rv. Penale Diritto e Procedura*, Commenti, opinioni, 14 settembre 2020.

(17) Intendendosi, come tale, unicamente il domicilio. Le critiche espresse in dottrina sul tema delle videoriprese non sono, infatti, state accolte favorevolmente dalla giurisprudenza di legittimità che, valorizzando il concetto di "comportamento non comunicativo", non ha mai posto in discussione l'indirizzo affermato dalle Sezioni Unite del 2006 (n. 26795, 28 marzo 2006).

(18) S. Quattroccolo, *Intelligenza artificiale e diritto*, in *Bioetica, Scienza e Società*, 2023, 271.

La prima attiene alla trasparenza (19), intesa come necessità di ricostruire le scelte compiute dalla macchina dotata di ragionamento o, perlomeno, setacciare gli elementi che ne costituiscono il patrimonio conoscitivo.

L'accessibilità dei dati (20) sembra rappresentare la *condicio sine qua non* per un utilizzo dell'IA rispondente ai principi che reggono il processo accusatorio, tra cui quello del contradditorio, che verrebbe conculcato nell'eventualità che un soggetto non sia posto nella condizione di verificare i presupposti in fatto su cui si fonda la prova (21).

La seconda, invece, concerne la tendenza, che si registra nella discussione sul tema, a confondere la causa per l'effetto.

Perché se i sistemi *software* ed *hardware* muniti di autonomo ragionamento vengono alimentati da input espressamente vietati dall'ordinamento (agli esempi sugli scritti anonimi o sulle informazioni apprese dal pubblico se ne potrebbero aggiungere altri), il problema non è l'IA in sé, ma chi ne governa le modalità applicative (22).

Ma voler impedire l'avvento nel processo penale di strumenti informatici dotati di intelligenza propria equivarrebbe a voler bandire l'inoculazione del *trojan* (art. 266, comma 2-*bis*, c.p.p.), senza considerarne la straordinaria efficacia investigativa, in ragione dell'uso discutibile che se n'è fatto in passato (23).

Forse è possibile immaginare un impiego di questo genere di risorse che sia in linea coi valori sanciti dall'art. 111 Cost. spostando l'attenzione del discorso dall'IA — quale mezzo tecnolo-

(19) G. Canzio, *Ai act e processo penale: sfide e opportunità*, in *Sistema Penale*, 20 ottobre 2024, 4.

(20) E. Currao, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?,* in *Diritto Penale e Uomo*, n. 5, 19 maggio 2021.

(21) F. M. Griffantini, *Attività preparatorie del contraddittorio dibattimentale*, II^a ed., Torino, 2010, 164.

(22) A. Craviotto - L. Vitali - L. Egitto - C. Canepa, *Per un uso responsabile dell'IA nel processo (penale)*, in *Giurisprudenza Penale Web*, 2024, n. 3, 6.

(23) M. Griffo, *Il trojan e le derive del terzo binario*, in *Sistema Penale*, 7 febbraio 2020, n. 2, 65.

gico — all'IA quale «sistema» (24).

La definizione, contenuta all'art. 3 del Regolamento UE n. 1689/2024 (25), permette di ridurre la complessità del tema ai seguenti termini: a) obiettivi espliciti od impliciti perseguiti dalla macchina; b) caratteristiche degli input dedotti; c) affidabilità degli output generati.

Il vantaggio che si trae dall'analisi di ogni singolo profilo consiste nell'escludere l'utilizzo di macchine provviste di IA per finalità non compatibili coi divieti probatori stabiliti dal Codice (26).

Nonché nel discernere, tra «previsioni, contenuti, raccomandazioni o decisioni» generati dal sistema, quelli attendibili da quelli che non lo sono (27); o, ancora, quelli ottenuti a partire da input "leciti" da quelli che, al contrario, sono stati assunti in violazione della legge (28).

Nell'impossibilità di prevedere gli esiti della sfida che si appresta ad affrontare la giustizia penale, l'apprezzamento dell'IA come sistema e la sottoposizione dei suoi output ai limiti di legalità in materia probatoria (29) sembrerebbe rappresentare l'unico modo per scongiurare che le garanzie processuali arretrino di fronte all'impeto della transizione digitale.

(24) A. Altieri, *L'artificial intelligence come organizzazione*, Iª ed.,Torino, 2024, 6.

(25) Art. 3, co. 1, n. 1), Reg. UE del 13 giugno 2024, n. 1689: «sistema di IA: 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».

(26) Accertare, tramite l'IA, la rispondenza del comportamento di una determinata persona ai valori morali generalmente accettati si tradurrebbe nel perseguimento di un obiettivo, sia esso esplicito od implicito, in contrasto col disposto dell'art. 194 c.p.p., che circoscrive il perimetro tracciato dall'art. 187 c.p.p., impedendo che la «moralità dell'imputato», salvo tassative eccezioni, formi oggetto di prova.

(27) A. Fonsi, *Prevenzione dei reati e riconoscimento facciale: il parere sfavorevole del Garante privacy sul sistema SARI Real Time*, in *Penale Diritto e Procedura*.

(28) F. Consulich, *Il diritto penale al tempo dell'intelligenza artificiale prospettive punitive nazionali dopo l'ai act*, in *Diritto e difesa*, 17 dicembre 2024, 2.

(29) P. Ferrua, *Ammissibilità della prova e divieti probatori*, in *Revista Brasileira de Direito Processual Penal*, Vol. 7, n. 1, n. 7/2021, 238 (*https://doi.org/10.22197/rbdpp.v7i1.53*).

3. Il riconoscimento facciale.

L'attendismo del legislatore italiano, che mal si concilia con l'opposta frenesia della società digitale[30], obbligherà la giurisprudenza ad assumersi il delicato compito di razionalizzazione le applicazioni investigative dell'IA.

Se è lecito pensare che l'ingresso nel processo di macchine dotate di ragionamento possa costituire l'occasione per una riflessione, ad ampio spettro, sulla prova informatica[31], è verosimile credere che lo sfruttamento di simili tecnologie sarà sottoposto al vaglio, *prima facie*, del diritto pretorio.

Nonostante, quindi, si sia cercato di dare una risposta approssimativa al "se" e al "quando" l'IA obbligherà gli attori del processo a misurarsi con essa, l'interrogativo cogente parrebbe essere il "come".

Essendo, infatti, sottile il confine che divide la prova atipica da quella irrituale ([32]), il pericolo che gli output generati da questa nuova tecnologia, una volta fatti entrare nel tessuto processuale, possano destrutturare le prove nominate è alto ([33]).

Per arginarlo, si potrebbe, allora, pensare di ricondurre i dati conoscitivi acquisiti tramite l'IA entro gli schemi della prova tipica, cosi da assicurare il rispetto del principio di non sostituibilità ([34]).

La tutela dell'identità legale del sistema, che implica il riferimento al disposto normativo quando un'acquisizione trovi nel codice la sua disciplina, è degradata dall'apporto di componenti atipiche, all'interno di un mezzo tipico, allorché esse stridano con

([30]) G. Corasaniti, *Il diritto nella società digitale*, I^a ed., Milano, 2018, 84.

([31]) Esigenza già da tempo segnalata in dottrina, essendo numerosi gli studiosi che hanno sottolineato l'importanza di "*Uno statuto dei nuovi mezzi di ricerca della prova di fronte alla società digitale*" - Roma, 22 settembre 2023 - UnitelmaSapienza - *https://www.youtube.com/watch?v=zszwb6brpqw*.

([32]) O. Mazza, *op. cit.*, 8.

([33]) A. M. Buzura, *Nuove forme di atipicità probatoria in materia di videoregistrazioni investigative,* in *Archivio Penale*, n. 1/2022, 15.

([34]) L. Tombelli, *La tutela della corrispondenza tra atipicità della prova e tentativi di riforma*, in *Penale Diritto e Procedura*, 16 gennaio 2025, 5.

gli elementi propri del paradigma probatorio (35).

Al contrario, l'inserimento di un elemento atipico (purché rispondente ai criteri di legalità) all'interno di un mezzo tipico, che non si risolva nell'aggiramento dei connotati dell'istituto, sembrerebbe in linea con l'approccio esegetico delineato dalla Consulta (36).

Si consideri, ad esempio, lo *screenshot*.

Nel caso in cui esso sia utilizzato per estrapolare da un supporto informatico tracce pertinenti al reato senza l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione si eluderebbe il disposto del comma 1-*bis* dell'art. 247 c.p.p. (37).

La giurisprudenza di legittimità ha censurato a più riprese tale prassi, chiarendo che non è consentito, in un sistema ispirato al principio di legalità, «scostarsi dalle previsioni legislative per compiere atti atipici i quali, permettendo di conseguire risultati identici o analoghi a quelli conseguibili con gli atti tipici, eludano tuttavia le garanzie costituzionali dettate dalla legge per questi ultimi» (38).

Qualora, invece, attraverso detto strumento si realizzi una fotografia istantanea dello schermo di un apparato elettronico, con la finalità di incorporare su un documento informatico la rappresentazione di «fatti, persone o cose», la "cattura" sarà conforme al modello tracciato dall'art. 234 c.p.p. (39).

(35) P. Tonini, *op. cit.*, 284.

(36) C. Conti, *Il principio di non sostituibilità: il sistema probatorio tra Costituzione e legge ordinaria*, in *Cassazione Penale*, Vol. 64, n. 2/2024, 459.

(37) Nonché del primo capoverso dell'art. 244 c.p.p., nella parte in cui prevede che «l'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

(38) Cass. pen., Sez. VI, 20/11/2024, (ud. 20/11/2024, dep. 13/01/2025) n. 1269, Rv. Diritto e Giustizia 2025, 14 gennaio 2025; Cass. pen., Sez. VI, 24/02/2003, n. 623, Ventre, Rv. 224741, in *DeJure*.

(39) Cass. Pen., Sez. V, 05/02/2021, (ud. 05/02/2021, dep. 30/03/2021), n. 12062, in *CED*, Cass. pen., 2021. Meno lineare è, invece, la questione relativa l'acquisizione di *file*

L'elemento col quale si ricava l'informazione è atipico in entrambe le ipotesi.

Nella prima, però, si traduce in un espediente, che svilisce le garanzie introdotte con la ratifica della Convenzione di Budapest del 2001 (40); nella seconda, l'innesto della componente atipica sul solco del binario codicistico non reca alcun pregiudizio al principio di non sostituibilità.

La questione del riconoscimento facciale potrebbe, allora, essere affrontata seguendo la direttrice degli artt. 213 ss. c.p.p. o nelle forme di cui all'art. 361 c.p.p. quando l'individuazione di una persona sia necessaria per la «prosecuzione delle indagini».

Si tratterebbe, in effetti, di aggregare un fattore atipico (IA), implementato da dati (input ed output) in linea con i divieti probatori stabiliti dal Codice, ad un mezzo giudicato idoneo, dallo stesso legislatore, ad assicurare l'accertamento dell'identità della persona (41).

La costruzione di un modello ibrido (42), sulla falsariga delle disposizioni previste per la ricognizione personale, non parrebbe, del resto, determinare l'erosione delle cautele apprestate dall'ordinamento per permettere alle parti e al giudice di valutare la credibilità della fonte di prova e di saggiarne l'attendibilità del risultato.

A condizione, tuttavia, che si assolvano, a pena di nullità, gli obblighi preveduti dall'art. 213 c.p.p.

Le operazioni preliminari descritte dalla norma appaiono, infatti, preminenti allorché il riconoscimento di un soggetto venga

in corso di redazione su personal computer mediante *screenshot* eseguito da un captatore informatico, ricondotto dalla giurisprudenza di legittimità nel concetto di comportamento comunicativo che, in quanto tale, non può formare oggetto di perquisizione informatica (Cass. pen., Sez. I, 07/10/2021, n. 3591, in *CED*, Cass. pen. 2022).

(40) Legge 18 marzo 2008, n. 48, di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, tenutasi a Budapest, il 23 novembre 2001.

(41) P. Tonini, *op. cit.*, Milano, 2012, 341.

(42) P. Rivello, *La prova penale*, in *Argomenti del Diritto*, a cura di P. Ferrua - E. Marzaduri - G. Spangher, Torino, 2013, 417.

demandato ad una macchina piuttosto che ad una persona (43).

Pertanto, come il ricognitore dovrà, per quel che ricorda, «descrivere la persona», riferire «se sia stato in precedenza chiamato a eseguire il riconoscimento» o visto il soggetto «prima e dopo il fatto per cui si procede» e indicare «se vi siano altre circostanze che possano influire sull'attendibilità del riconoscimento», così sarà necessario verificare, preventivamente, se il sistema dotato d'IA, impiegato per l'individuazione, possegga determinati requisiti tecnici (44), comprovanti un certo grado di affidabilità.

Tra le attività preliminari s'imporrà, dunque, l'indicazione dei dispositivi a cui si ricorre per eseguire la ricognizione, dei componenti *hardware* e del *software* in uso all'apparato intelligente, del suo sviluppatore (45) e del responsabile della procedura.

In questo modo, è possibile escludere — a monte (46) — dal processo quegli applicativi che, per le loro caratteristiche, non siano in grado di generare «previsioni, contenuti, raccomandazioni o decisioni» conformi agli standard probatori (art. 192 c.p.p.) o, ancora, che perseguano obiettivi, «espliciti od impliciti», incompatibili coi valori stabiliti dall'art. 111 Cost. (47).

Inoltre, nello svolgimento della ricognizione potrà osservarsi una procedura di tipo bifasica.

Dapprima, sarà necessario setacciare gli input valorizzati dal sistema d'IA per pervenire ad un determinato output, capire quali dati biometrici abbia esaminato la macchina ed accertare i margini di errore associati agli algoritmi di *deep* o *machine learning* (48).

(43) J. Della Torre, *Intelligenza artificiale e processo penale*, cit., 41.

(44) A. Fonsi, *Prevenzione dei reati e riconoscimento facciale: il parere sfavorevole del Garante privacy sul sistema SARI Real Time*, in *Penale Diritto e Procedura*, Commenti, 8.

(45) C. Teresi, *L'ai act nell'ottica del processualpenalista: uno sguardo preliminare*, in *Penale Diritto e Procedura*, 20 giugno 2024, 4.

(46) M. Colacurci, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema Penale*, 12 settembre 2022, 36.

(47) L. Palazzani, *Tecnologie dell'informazione e intelligenza artificiale*, Roma, 2020, 74.

(48) R. Angelini, *Intelligenza artificiale, protezione dei dati personali e regolazione*,

Così da risalire a quei dati assunti in violazione dei limiti di legalità in materia probatoria e, al tempo stesso, recuperare trasparenza sull'insidioso terreno (49) delle procedure non supervisionate.

Per avere, poi, un riconoscimento quanto più possibile scevro da condizionamenti e suggestioni (50), è essenziale testare la credibilità della macchina dotata di intelligenza propria.

Ed il metodo più efficace sembrerebbe quello descritto dall'art. 214 c.p.p.

Percorrendo lo schema che il legislatore del 1989 ha ideato per la persona che è chiamata a compiere la ricognizione, alla quale si chiede di riconoscere un certo individuo — che ha percepito coi propri sensi — tra simili (51), si cercherà di ingannare il dispositivo di riconoscimento facciale per comprendere se al variare di input — «il più possibile somiglianti» tra loro — si avrà un risultato differente.

La logica sottesa alla scelta di distrattori aventi le medesime fattezze e finanche abbigliati identicamente, che mira ad affinare la qualità del risultato probatorio (52), può certamente trovare applicazione anche nell'ipotesi in cui l'individuazione di una persona sia eseguita "artificialmente".

Ritornando all'esempio del tifoso, si sottopone alla macchina l'immagine di uno spettatore somigliante al soggetto del quale, in prima battuta, è stata riconosciuta l'identità; se alla modifica dell'input (dati biometrici) si ottiene il medesimo output (ovvero la macchina continua ad associare allo spettatore somigliante l'identità del tifoso riconosciuto in precedenza), si avrà un elemento di prova verosimilmente non attendibile (53).

a cura di F. Pizzetti, Torino, 2018, 314.

(49) B. Fragrasso, *La responsabilità penale del produttore di sistemi di intelligenza artificiale*, p. 4, in *Sistema Penale*, 12 giugno 2023, 36.

(50) G. Spangher, *La pratica del processo penale*, Milano, Vol. II, 2012, 82.

(51) G. Illuminati, *La prova nel dibattimento penale*, IVª ed., a cura di P. Ferrua - F. M. Grifantini - G. Illuminati - R. Orlandi, 2010, Torino, 141.

(52) A. Nappi, *Codice di procedura penale. Rassegna di giurisprudenza e di dottrina*, in *Atti e prove*, Vol. II, a cura di R. Aprati - G. Ariolli - L. De Matteis - M. Gambardella - R. Mendoza - A. Nappi - P. Palladino, Milano, 2008, 609.

(53) D. Polidoro, *op*. cit., 20.

In tale prospettiva, si consegue l'indubbio vantaggio di sfruttare le opportunità che offrono i sistemi d'IA senza svilire l'identità legale del sistema probatorio, da cui dipende l'esercizio pieno ed effettivo del diritto di difesa (54).

Nella consapevolezza che questo complesso fenomeno non potrà non dispiegare i propri effetti sul sistema processuale penale, osservare la razionalità (55) delle scelte compiute dal legislatore sul finire dello scorso secolo può rivelarsi particolarmente utile.

Perché la strada per evitare quanto accaduto nell'aprile dello scorso anno ai danni dell'innocente tifoso brasiliano (56) parrebbe essere stata tracciata, dal nostro Codice, con molti anni d'anticipo.

L'importante è non prendere scorciatoie.

ABSTRACT: Molto presto, il processo penale italiano dovrà affrontare la sfida dell'intelligenza artificiale. Le riflessioni che seguono si concentrano sulle possibili implicazioni derivanti dall'introduzione negli stadi dei dispositivi di riconoscimento facciale. Nel silenzio del legislatore, l'interprete dovrà misurarsi col tessuto codicistico e tentare di risolvere, preliminarmente, due questioni. Quella dell'ammissibilità dei *facial recognition systems*, in ragione del disposto dell'art. 189 c.p.p (il dato conoscitivo acquisito tramite il sistema di IA sembrerebbe rispondere ai criteri dettati per l'assunzione delle prove innominate) e quella della legalità, che impone l'esclusione dei dati conoscitivi ottenuti in violazione dei limiti in materia probatoria. Essendo, però, sottile il confine che divide la prova atipica da quella irrituale, è necessario immaginare un paradigma che permetta di ricondurre gli elementi acquisiti tramite l'IA entro gli schemi della prova tipica, così da garantire il rispetto del principio di non sostituibilità senza rinunciare ai vantaggi del progresso tecnologico. La proposta è quella di costruire un modello probatorio ibrido, in grado di subordinare il riconoscimento facciale alle disposizioni previste dagli artt. 213 e ss. sulla ricognizione personale.

ABSTRACT: *Very soon, the italian criminal process will have to face the challenge of artificial intelligence. The following reflections focus on the possible implications arising*

(54) C. CONTI - M. TORRE, *Le indagini atipiche*, a cura di A. SCALFATI, Torino, 2019, 543.

(55) A. GAITO - E.N. LA ROCCA, *Vent'anni di "giusto processo" e trent'anni di "codice Vassalli": quel (poco) che rimane...*, in *Archivio Penale*, n. 3/2019, 7.

(56) D. MASTROGIACOMO, *Brasile, l'Intelligenza artificiale sbaglia ancora: tifoso scambiato per un ricercato dal riconoscimento facciale e arrestato allo stadio*, in *La Repubblica*, 30 aprile 2024, (*https://www.repubblica.it/esteri/2024/04/30/news/brasile_riconoscimento_facciale_arresto_sbagliato_intelligenza_artificiale-422776385/*).

from the introduction of facial recognition devices in stadiums. In the silence of the legislator, the interpreter will have to deal with the fabric of the code and try to resolve, preliminarily, two issues. That of the admissibility of facial recognition systems, potentially supported by the provisions of art. 189 c.p.p (the cognitive data acquired through the AI system would seem to meet the criteria dictated for the assumption of unnamed evidence) and that of legality, which requires the exclusion of cognitive data obtained in violation of the limits in evidentiary matters. However, since the line that divides atypical evidence from irregular evidence is thin, it is necessary to imagine a paradigm that allows the elements acquired through AI to be brought back within the schemes of typical evidence, so as to guarantee compliance with the principle of non-substitutability without giving up the advantages of technological progress. The proposal is to build a hybrid evidentiary model, capable of subordinating facial recognition to the provisions set forth in art. 213 et seq. on personal recognition.