22. LA GIUSTIZIA PENALE ITALIANA NELLA PROSPETTIVA INTERNAZIONALE
Atti del Convegno di studio svoltosi a Courmayeur, 8-10 ottobre 1999

23. SISTEMA SANZIONATORIO: EFFETTIVITÀ E CERTEZZA DELLA PENA
Atti del Convegno di studio svoltosi a Casarano-Gallipoli, 27-29 ottobre 2000

24. PER UNA GIUSTIZIA PENALE PIÙ SOLLECITA: OSTACOLI E RIMEDI RAGIONEVOLI
Atti del Convegno di studio svoltosi a Milano, 18 marzo 2005 e Lecce, 14-15 ottobre 2005

25. IMPRESA E GIUSTIZIA PENALE: TRA PASSATO E FUTURO
Atti del Convegno di studio svoltosi a Milano, 14-15 marzo 2008

26. RICICLAGGIO E CORRUZIONE: PREVENZIONE E CONTROLLO TRA FONTI INTERNE E INTERNAZIONALI
Atti del Convegno di studio svoltosi a Courmayeur, 28-29 settembre 2012

27. CIRCOLAZIONE DEI BENI CULTURALI MOBILI E TUTELA PENALE: UN'ANALISI DI DIRITTO INTERNO, COMPARATO E INTERNAZIONALE
Risultati di una ricerca e di un Seminario di studio svoltosi a Milano, 29 ottobre 2013

28. DEI DELITTI E DELLE PENE A 250 ANNI DALLA PUBBLICAZIONE. La lezione di Cesare Beccaria

29. MISURE PATRIMONIALI NEL SISTEMA PENALE: EFFETTIVITÀ E GARANZIE
Atti del Convegno di studio svoltosi a Milano, 27 novembre 2015.

30. CRIMINALITÀ D'IMPRESA E GIUSTIZIA NEGOZIATA: ESPERIENZE A CONFRONTO
Atti del Convegno di studio svoltosi a Milano, 28 ottobre 2016.

31. IL PROBLEMA DELL'INQUINAMENTO STORICO: ALLA RICERCA DEI RIMEDI GIURIDICI NELL'ORDINAMENTO ITALIANO
Atti del Convegno di studio svoltosi a Milano, 26 ottobre 2017.

32. IL FATTO ILLECITO NEL DIRITTO AMMINISTRATIVO E NEL DIRITTO PENALE: LA GARANZIA DELLA PREVEDIBILITÀ
Atti del Convegno di studio svoltosi a Milano, 29 novembre 2019.

33. GIURISDIZIONE PENALE, INTELLIGENZA ARTIFICIALE ED ETICA DEL GIUDIZIO
Atti del XXXIII Convegno di studio *online* "Enrico de Nicola", Milano, 15 ottobre 2020.

CENTRO NAZIONALE DI PREVENZIONE E DIFESA SOCIALE

Convegni di studio «Enrico de Nicola»
Problemi attuali di diritto e procedura penale

33

Giurisdizione penale, intelligenza artificiale ed etica del giudizio

UNIVERSITÀ DEGLI STUDI DI MILANO
DIPARTIMENTO DI SCIENZE GIURIDICHE "CESARE BECCARIA"

Fondazione CARIPLO

GIUFFRÈ
GIUFFRÈ FRANCIS LEFEBVRE

INTELLIGENZA ARTIFICIALE E DIRITTI FONDAMENTALI IN AMBITO PROBATORIO

Mitja Gialuz
ordinario di Diritto processuale penale
nell'Università degli Studi di Genova

Sommario: 1. La "marcia trionfale" dell'intelligenza artificiale nell'ambito della giustizia penale. — 2. Carte dei diritti "tradizionali" e fonti *ad hoc*. — 3. Un triplice insieme: prova scientifica, prova digitale e prova fondata sull'IA. — 4. La prova fondata sull'IA tra prove tipiche e innominate. — 5. Le specificità della prova fondata sull'IA. — 6. Conclusioni.

1. *La "marcia trionfale" dell'intelligenza artificiale nell'ambito della giustizia penale*

Vorrei partire da una precisazione terminologica. Come è stato detto, di definizioni di intelligenza artificiale [1] ve ne sono tante, ma credo ci si debba accordare su una stipulativa, che potrebbe essere quella posta dalla Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi [2]: secondo questa fonte l'intelligenza artificiale (d'ora innanzi anche IA) è costituita da un « insieme di metodi scientifici, teorie e tecniche finalizzate a riprodurre mediante le macchine le capacità cognitive degli esseri umani » [3]. Che cosa si intenda poi per "capacità cognitive" è tutto da verificare e non è indifferente ai fini della nostra trattazione; le intendiamo, com'è stato suggerito dal documento introduttivo a questo convegno, in senso lato. Come

[1] È noto, infatti, che non vi è una totale convergenza definitoria sulla locuzione di "intelligenza artificiale": v., per tutti, C. Burchard, *L'intelligenza artificiale come fine del diritto penale?*, in *Riv. it. dir. proc. pen.*, 2019, p. 1914; A. Santosuosso, *Sulla trasformazione algoritmica della società*, in *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Firenze, 2020, pp. 6-9; S. Signorato, *Giustizia penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo*, in *Riv. dir. proc.*, 2020, pp. 605-606. Per una recente panoramica al riguardo, cfr. Centro comune di ricerca della Commissione europea, *AI Watch Defining Artificial Intelligence, Towards an operational definition and taxonomy of artificial intelligence*, Lussemburgo, 2020, p. 17 e ss.

[2] Ci si riferisce alla *Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi*, adottata dalla Commissione per l'efficienza della giustizia (CEPEJ) nel 2018. Per un commento alla stessa, cfr. S. Quattrocolo, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *www.lalegislazionepenale.it*, 18 dicembre 2018.

[3] Così si legge nell'Appendice III della *Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia*, cit., p. 47.

vedremo, questa definizione ci consentirà anzitutto di distinguere la nozione di "prova digitale" da quella di "prova fondata sull'intelligenza artificiale" [4].

Detto questo, dobbiamo prendere atto che, negli ultimi lustri, vi è stata un'espansione sensibile dell'IA nella nostra quotidianità: dalle macchine a guida automatica all'uso del *machine learning* nei servizi di implementazione del sistema sanitario, dalla materia assicurativa alle applicazioni industriali, dai dispositivi finalizzati a individuare le truffe online, fino agli assistenti domotici come Google Home e Alexa [5]. In fondo, è esperienza di tutti quella di essere anticipati da *gmail* nella scrittura delle *e-mail*, nel senso che non siamo più liberi neanche di scrivere perché abbiamo un *software* che ci anticipa e ci suggerisce i nostri testi; ma, per quanto ci riguarda specificamente, in breve tempo l'intelligenza artificiale si è ritagliata, spesso in modo silenzioso, — e proprio per questo è assai importante il simposio odierno — un ruolo chiave anche nell'ambito della giustizia penale, intesa in senso lato [6]. Mi limito ad alcuni esempi non controversi e ovviamente non esaustivi.

Per quel che concerne la fase della prevenzione, segnalo i *software* di *predictive policing* [7], che vengono utilizzati anche in Italia [8]: penso al *KeyCrime*,

[4] Cfr., *infra*, § 3.

[5] In merito, cfr., tra i molti, S. Hénin, *AI. Intelligenza artificiale tra incubo e sogno*, Milano, 2019, p. 75 e ss.; J. Kaplan, *Intelligenza artificiale. Guida al prossimo futuro*, Roma, 2017. Sulle ragioni di questa rapida evoluzione, cfr. C. Cath, S. Wachter, B. Mittelstadt, M. Taddeo, L. Floridi, *Artificial Intelligence and the 'Good Society': the US, EU, and UK approach*, in *Science and Eng. Ethics*, 2018, p. 505.

[6] Il dibattito sviluppatosi in materia è cresciuto in maniera significativa negli ultimi anni. Tra i diversi contributi pubblicati sul tema, cfr., di recente, F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Dir. pen. cont.*, 29 settembre 2019; M. Caianiello, *Criminal Process faced with the Challenges of Scientific and Technological Development*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2019, p. 267; G. Canzio, *Intelligenza artificiale e processo penale*, in *Cass. pen.*, 2021, p. 797; G. Contissa, G. Lasagni, *When it is (also) Algorithms and AI that decide on Criminal Matters: In Search of an Effective Remedy*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2020, p. 280; B. Galgani, *Considerazioni sui "precedenti" dell'imputato e del giudice al cospetto dell'IA nel processo penale*, in *Sist. pen.*, 2020, n. 4, p. 81; M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *Dir. pen. cont.*, 29 maggio 2019; V. Manes, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in Aa.Vv., *Intelligenza artificiale. Il diritto, i diritti e l'etica*, a cura di U. Ruffolo, Milano, 2020, p. 547; U. Pagallo, S. Quattrocolo, *The impact of AI on criminal law, and its twofold procedures*, in Aa.Vv., *Research Handbook on the Law of Artificial Intelligence*, a cura di W. Barfield e U. Pagallo, Cheltenham-Northampton, 2018, p. 385; D. Polidoro, *Tecnologie informatiche e procedimento penale: la giustizia penale "messa alla prova" dall'intelligenza artificiale*, in *Arch. pen.*, 2020, n. 3 (versione web); C. Piergallini, *Intelligenza artificiale: da "mezzo" ad "autore" del reato?*, in *Riv. it. dir. proc. pen.*, 2020, p. 1745; S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European legal Discussion*, Cham, 2020, *passim*; G. Riccio, *Ragionando su intelligenza artificiale e processo penale*, in *Arch. pen.*, 2019, n. 3 (versione web); P. Severino, *Intelligenza artificiale e diritto penale*, in Aa.Vv., *Intelligenza artificiale*, cit., p. 531; S. Signorato, *Il diritto a decisioni penali non basate esclusivamente su trattamenti automatizzati: un nuovo diritto derivante dal rispetto della dignità umana*, in *Riv. dir. proc.*, 2021, p. 101.

[7] In argomento, si vedano, per tutti, Aa.Vv., *Predictive Policing and Artificial Intelligence*, a cura di J. McDanie e K. Pease, Oxon-New York, 2021, *passim*; L. Bennet Moses, J. Chan, *Algorithmic prediction in policing: assumptions, evaluation, and accountability*, in *Policing and Society*, 2016, p. 1; P.J. Brantingham, *The Logic of Data Bias and Its Impact on Place-Based Predictive Policing*, in *Ohio State Journal of Criminal Law*, 2018, p. 473 e ss.; C. Burchard, *L'intelligenza artificiale come fine del diritto penale?*, cit., p. 1922 e ss. Degno di menzione è il *tool* statunitense

adottato dalla Questura di Milano, che ha portato a risultati assai significativi [9], oppure a *X-Law*, un *software* elaborato dalla Questura di Napoli e completato dal Dipartimento di Pubblica Sicurezza del Ministero dell'Interno e usato in diverse realtà del nostro Paese [10].

Nell'ambito del procedimento penale, con specifico riguardo alle dinamiche probatorie, possono essere individuati due ambiti nei quali gli strumenti di intelligenza artificiale si stanno affermando in maniera evidente.

Il primo riguarda le *digital evidence* di ultima generazione basate sull'IA [11]: nella fase delle indagini si fa un uso sempre più ampio di sistemi fondati sull'intelligenza artificiale; e questo impiego sarà destinato a crescere notevolmente con la diffusione dell'*Internet of Things* [12] e con la domotica, perché assisteremo a dispositivi presenti nelle nostre abitazioni che offriranno informazioni dirette sulla scena del crimine [13].

Ma si pensi già oggi ai captatori e agli strumenti di riconoscimento facciale: in particolare, in quest'ultimo caso, si è in presenza di un *tool* che consente, tramite un algoritmo basato sull'IA, « di associare alla foto o al video del volto di uno sconosciuto una o più immagini contenute in una banca dati di dimensioni variabili di soggetti le cui generalità siano già note » [14]. I cosiddetti *facial recognition systems* operano, più precisamente, mediante algoritmi, capaci di rilevare « le cosiddette impronte facciali (*faceprint*), ovvero un certo numero di tratti, quali la posizione degli occhi, del naso, delle narici, del mento e delle

PredPol, in grado di individuare zone ad "alto rischio" di criminalità (cfr. *https://www.predpol.com/*). Inoltre, per una recente disamina sui *predictive policing tools* olandesi Syri e CAS, v. L. Strikwerda, *Predictive policing: the risk associated with risk assessment*, in *The Police Journal: Theory, Practice and Principle*, 2020, p. 1 e ss.

[8] Cfr. M.B. Armiento, *La polizia predittiva come strumento di attuazione amministrativa delle regole*, in *Dir. amm.*, 2020, p. 990 e ss.; G. Contissa, G. Lasagni, G. Sartor, *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Diritto di internet*, 2019, p. 621.

[9] V. C. Morabito, *La chiave del crimine*, in *https://www.poliziadistato.it/statics/16/la-chiave-del-crimine.pdf*; M. Serra, *Rapinatore seriale catturato grazie al software "Key crime"*, in *https://www.lastampa.it/2018/01/05/milano/rapinatore-seriale-catturato-grazie-al-software-key-crime-ijoXB7yQTI4P0g5noFfteI/pagina.html*.

[10] Per indicazioni al riguardo cfr. *https://corrieredelveneto.corriere.it/venezia-mestre/cronaca/18_novembre_16/venezia-l-algoritmo-che-prevede-furti-avvisa-polizia-colpo-sventato-d62fe1fc-e9ab-11e8-9475-b8ef849c8bde.shtml*.

[11] Sul rapporto tra *artificial intelligence* e prova penale, si veda il lavoro pionieristico di L. Lupária, *Prova giudiziaria e ragionamento artificiale: alcune possibili chiavi di lettura*, in *Il concetto di prova alla luce dell'intelligenza artificiale*, Milano, 2005, p. XIV e ss. Sul tema, cfr., tra i molti, S. Lorusso, Digital evidence, *cybercrime e giustizia penale 2.0*, in *Proc. pen. giust.*, 2019, p. 821 e ss.; L. Lupária, G. Ziccardi, *Investigazione penale e tecnologia informatica*, Milano, 2007, *passim*; M. Pittiruti, Digital evidence *e procedimento penale*, Torino, 2017, *passim*; S. Quattrocolo, *Equità del processo penale e* automated evidence *alla luce della Convenzione europea dei diritti dell'uomo*, in *Revista Italo-Española de Derecho Procesal*, 2019, p. 2 e ss.; G. Vaciago, Digital evidence. *I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'imputato*, Torino, 2012, *passim*.

[12] V. U. Pagallo, S. Quattrocolo, *The impact of AI on criminal law*, cit., p. 385.

[13] Cfr. S. Quattrocolo, *Equo processo penale e sfide della società algoritmica*, in *BioLaw Journal*, 2019, 1, p. 138.

[14] Così, J. Della Torre, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della* High Court of Justice, in *Dir. pen. cont. — Riv. Trim.*, 1/2020, p. 232.

orecchie » [15] e, in questa maniera, di realizzare « un modello biometrico finalizzato al riconoscimento » [16]. Ciò, in particolare, può avvenire attraverso due modalità: la prima *real-time*; la seconda basata su immagini o video che sono già agli atti.

Negli Stati Uniti già dalla fine degli anni Novanta e nei primi anni Duemila si discuteva dell'utilizzo di tali dispositivi tecnologici nell'ambito del processo penale; tuttavia, il dibattito è divenuto particolarmente acceso nel 2020 con lo "scandalo *Clearview*", in cui la polizia americana usava una app di riconoscimento facciale che operava su un *database* contenente miliardi di dati rubati (ed ecco il punto fondamentale) da *social network* come Facebook, Twitter, Instagram e molti altri [17]. In sostanza, il *software* si basava su dati raccolti e trattati illegittimamente.

Quanto all'Italia, merita segnalare un sistema definito SARI (Sistema Automatico di Riconoscimenti Immagini) di cui si sa veramente poco [18]. Recentemente, vi è stata un'interrogazione parlamentare presentata alla Camera [19] e la risposta del Ministro dell'Interno ha dato atto che esistono due modalità in cui si articola il *tool* in questione [20]: per un verso, il cosiddetto SARI *Enterprise*, che opera « per la ricerca di volti a partire da immagini statiche su banche dati di grandi dimensioni » [21], e, per altro verso, il SARI *Real-Time*,

[15] In questo senso, R. Lopez, *La rappresentazione facciale tramite* software, in Aa.Vv., *Le indagini atipiche*, a cura di A. Scalfati, 2ª ed., Torino, 2019, p. 241.

[16] Cfr. R. Lopez, *La rappresentazione facciale*, cit., p. 241.

[17] Com'è noto, tale scandalo è emerso dopo un'inchiesta condotta dal New York Times: cfr. K. Hill, *The Secretive Company That Might End Privacy as We Know It*, in *www.nytimes.com*, 18 gennaio 2020. Per indicazioni in merito, cfr. J. Della Torre, *Novità dal Regno Unito*, cit., p. 234. Per una disamina del caso *Clearview*, secondo una prospettiva eurounitaria, v. I.N. Rezende, *Facial recognition in police hands: Assessing the "Clearview case" from a European perspective*, in *New Journal of European Criminal Law*, 2020, p. 375 e ss. Non va, peraltro, sottaciuto come la questione dell'utilizzo dei *facial recognition systems* risulti particolarmente spinosa: al riguardo, degna di menzione è la recente pronuncia della *Court of Appeal* dell'Inghilterra e Galles, *R (on the application of Edward Bridges) v. The Chief Constable of South Wales Police*, [2020] EWCA Civ 1058, la quale, disattendendo la pronuncia della *High Court of Justice*, ha considerato lesivo dell'art. 8 CEDU l'impiego degli strumenti di riconoscimento facciale. Sulla decisione di primo grado, si veda, ancora, l'analisi di J. Della Torre, *Novità dal Regno Unito*, cit., p. 236 e ss.

[18] Sul punto, cfr. J. Della Torre, *Novità dal Regno Unito*, cit., pp. 241-242; R. Lopez, *La rappresentazione facciale*, cit., p. 240 e ss.; E. Sacchetto, Face to face: *il complesso rapporto tra* automated facial recognition technology *e processo penale*, in www.lalegislazionepenale.eu, 16 ottobre 2020, p. 7 e ss.; R. Valli, *Sull'utilizzabilità processuale del SARI: il confronto automatizzato di volti rappresentati in immagini*, in *ilPenalista*, 16 gennaio 2019.

[19] Ci si riferisce all'interrogazione parlamentare n. 4-04528 formulata, dopo lo scoppio dello scandalo statunitense *Clearview*, dall'On. Sensi in ordine al funzionamento del *software* SARI. Da ultimo, occorre segnalare che in data 3 marzo 2021 è stata sollevata un'interrogazione a risposta immediata (n. 3-0274) da parte degli On. Sensi e altri, con riferimento agli *intendimenti in ordine all'utilizzo di sistemi di riconoscimento facciale, anche in relazione alla necessaria tutela dei diritti fondamentali della persona* (cfr., anche in merito alla risposta formulata dal Ministro dell'Interno, Camera dei deputati, XVIII Legislatura, Resoconto stenografico dell'Assemblea. Seduta n. 463 di mercoledì 3 marzo 2021).

[20] Il testo della risposta del Ministro dell'Interno all'interrogazione parlamentare è rinvenibile in *http://documenti.camera.it/leg18/resoconti/commissioni/bollettini/html/2020/02/05/01/allegato.htm*.

[21] Così, Ministero dell'Interno. Dipartimento della pubblica sicurezza, *Capitolato tecnico. Procedura volta alla fornitura della soluzione integrata per il sistema automatico di riconoscimento*

finalizzato al « riconoscimento in tempo reale di volti presenti in flussi video provenienti da telecamere » [22].

Più nel dettaglio, le immagini in cui viene applicato il SARI *Enterprise* sono confrontate con i profili facciali estratti dalla banca dati AFIS (*Automated Fingerprint Identification System*), la quale contiene, sempre secondo la risposta del Ministero dell'Interno, quasi 18 milioni di cartellini fotosegnaletici [23]. Il sistema SARI *Real-Time*, invece, confronta i volti presenti nei flussi video dinamici con quelli contenuti in una *watchlist* con una grandezza dell'ordine di 100.000 persone [24].

D'altra parte, accanto alle *digital evidence*, un'ulteriore frontiera per gli strumenti basati sull'IA, rilevabile nelle dinamiche probatorie, è rappresentata dalle cosiddette *machine evidence* o *e-evidence*, che saranno prodotte, per esempio, dalla stessa automobile a guida automatizzata in caso di incidenti generati da una cooperazione tra uomo e robot [25].

Quindi, in definitiva, per quanto riguarda l'utilizzo in ambito, *lato sensu*, probatorio, abbiamo, da un lato, la *digital evidence* di ultima generazione basata sull'intelligenza artificiale (e un *focus*, secondo me, va fatto proprio sui sistemi di riconoscimento facciale); dall'altro, le cosiddette *machine evidence* o *e-evidence*.

Con specifico riferimento alla fase decisoria, poi, nel procedimento penale — com'è stato ricordato — si utilizzano algoritmi per la valutazione della prova, che si fondano sulle reti bayesiane e reti neurali e che servono per ricostruire il passato attraverso una valutazione razionale, in particolare, delle prove scientifiche [26].

Ma non è tutto. Rilevano, inoltre, gli algoritmi predittivi: da un canto, quelli volti a formulare giudizi prognostici di pericolosità, i cosiddetti *risk assessment tools* [27]; dall'altro, quelli finalizzati a predire il contenuto della decisione [28].

Da ultimo, segnalo che si sta sviluppando un utilizzo dell'intelligenza artificiale anche nel settore della cooperazione internazionale. Al riguardo, è interessante un recente studio della Commissione intitolato "*Cross-border Digital Criminal Justice*", dove si propone l'uso dell'intelligenza artificiale per

immagini S.A.R.I., p. 7, consultabile in *https://www.poliziadistato.it/statics/06/20160627-ct-sari--4-.pdf*.

[22] In questi termini, di nuovo, Ministero dell'Interno. Dipartimento della pubblica sicurezza, *Capitolato tecnico*, cit., p. 7.

[23] Cfr., nuovamente, quanto si legge in *http://documenti.camera.it/leg18/resoconti/commissioni/bollettini/html/2020/02/05/01/allegato.htm*.

[24] Cfr. Ministero dell'Interno. Dipartimento della pubblica sicurezza, *Capitolato tecnico*, cit., p. 7.

[25] V. European Committee on Crime Problems, *Working Group of Experts on Artificial Intelligence and Criminal Law — Working Paper for the meeting of 27 March 2019*, p. 4.

[26] In merito, v., per tutti, F. Taroni, S. Bozza, J. Vuille, *Il ruolo della probabilità nella valutazione della prova scientifica*, in Aa.Vv., *Prova scientifica e processo penale*, a cura di G. Canzio e L. Lupária, Milano, 2017, p. 23 e ss.

[27] Sui quali si intratterrà, nella sua relazione, Serena Quattrocolo.

[28] Al riguardo, cfr. la relazione di Luca Lupária.

facilitare il lavoro di Eurojust [29]. Si tratterebbe, più nel dettaglio, di automatizzare la trasmissione di informazioni dai singoli *stakeholders* all'*Eurojust Case Management System*.

Fatta questa breve panoramica, il compito che mi è stato affidato riguarda la specifica analisi dell'ambito probatorio, e cioè delle prove fondate sull'IA — quali le videoriprese con riconoscimento facciale, la *Bloodstain Pattern Analyis* (BPA), o gli stessi captatori —, con l'obiettivo di inquadrare — come richiesto dal titolo della relazione — i diritti fondamentali dei soggetti coinvolti nel procedimento penale [30].

2. *Carte dei diritti "tradizionali" e fonti* ad hoc

A tal fine, prenderei le mosse da uno spunto interessante fornito dalla giurisprudenza del Consiglio di Stato, che, a partire dal 2019, ha avuto modo di occuparsi ampiamente dell'utilizzo di meccanismi automatici basati sull'intelligenza artificiale, sia pure nell'ambito di procedimenti amministrativi [31]. Ebbene, i supremi giudici amministrativi, nella pronuncia n. 8472 del 13 dicembre 2019, hanno cristallizzato quella che definirei "una regola d'oro", che bisogna sempre tenere a mente, quando ci si approccia all'intelligenza artificiale: « l'utilizzo di procedure informatizzate » — così ha detto il Consiglio di Stato — « non può essere motivo di elusione dei principi che conformano il nostro ordinamento » [32].

Quali sono, allora, questi principi?

Anzitutto, vanno richiamati quei principi classici, che richiedono dei semplici adattamenti quando viene in rilievo la prova basata sull'IA.

Per un verso, alludo ai diritti e alle garanzie che tutelano la sfera intima dell'individuo, erigendo una barriera, uno scudo protettivo rispetto alle intrusioni esterne. Vengono in mente gli artt. 14 e 15 Cost., a protezione dell'inviolabilità del domicilio e delle conversazioni e comunicazioni, l'art. 8 CEDU, nella parte in cui tutela la vita privata, l'art. 7 Carta di Nizza, sempre in tema di salvaguardia della *privacy*, e, ancora, il diritto di difesa e il corollario del *nemo tenetur se detegere*. Quest'ultimo, come ha accennato il professor Ubertis, dovrebbe essere interpretato in senso rigoroso e applicato non solo quando la persona dell'imputato è fonte di dichiarazioni, ma anche quando è oggetto di prova o, meglio, fonte di dati, sui quali opera poi l'intelligenza artificiale, anzitutto, attraverso la profilazione, ma non solo.

Per altro verso, mi riferisco a quelle garanzie che assicurano un confronto dialettico paritario e una verifica sull'attendibilità della fonte di prova: dall'art. 111, commi 2, 3 e 4 Cost. allo stesso diritto di difesa, nonché all'art. 6 CEDU [33]. Sicuramente, la prova fondata sull'IA pone sfide nuove (ci tornerò soprattutto in relazione al tema dell'opacità [34] del processo decisionale di tali strumenti, ossia della cosiddetta *black box* [35]); mi pare, però, che il portato di queste garanzie non muti significativamente, nel senso che si tratta di applicare le medesime al contesto specifico, ma senza la necessità di adattamenti concettuali.

Vi sono invece dei canoni "classici" che vanno ripensati *ab ovo*, alla luce della nuova frontiera dell'intelligenza artificiale.

Credo che il diritto fondamentale, quando si parla di intelligenza artificiale, sia anzitutto quello alla protezione dei dati di carattere personale, che viene estratto dalla giurisprudenza della Corte EDU dall'art. 8 CEDU [36], e che è, invece, cristallizzato nell'art. 8 Carta di Nizza come diritto all'autodeterminazione informativa e all'integrità del dato [37]. Evidentemente, c'è una valenza centrale, perché la caratteristica peculiare dell'intelligenza artificiale è quella di analizzare una quantità enorme — come ci è stato ricordato — di dati, che sono il vero e proprio "ossigeno" dell'IA [38].

Ebbene, mi pare che l'art. 8 CDFUE sia una cornice fondamentale, che prevede una protezione abbastanza avanzata, con un unico problema, però,

[29] Cfr. European Commission, *Cross-border Digital Criminal Justice. Final Report*, Lussemburgo, 2020.

[30] In ordine all'impatto dell'IA sui diritti fondamentali della persona, si veda, in termini generali, il recente studio pubblicato da FRA — European Union Agency for Fundamental Rights, *Getting the future right — Artificial intelligence and fundamental rights*, 14 dicembre 2020, consultabile in *https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights*. In dottrina, cfr., tra gli altri, J. Nieva-Fenol, *Intelligenza artificiale e processo*, Torino, 2019, p. 118 e ss.; A. Završnik, *Criminal justice, artificial intelligence systems, and human rights*, in *ERA Forum*, 2020, p. 567 e ss.

[31] In argomento, v., tra gli altri, E. Carloni, *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in *Dir. amm.*, 2020, p. 281 e ss.; S. Cristi, *Evoluzione tecnologica e trasparenza nei procedimenti "algoritmici"*, in *Diritto di internet*, 2019, p. 382 e ss.; M. Ferrari, *La complessità della digitalizzazione e dell'uso degli algoritmi nella PA*, ivi, 2020, p. 338 e ss.; A.G. Orofino, G. Gallone, *L'intelligenza artificiale al servizio delle funzioni amministrative: profili problematici e spunti di riflessione*, in *Giur. it.*, 2020, p. 1738; B. Raganelli, *Decisioni pubbliche e algoritmi: modelli alternativi di dialogo tra forme di intelligenza diverse nell'assunzione di decisioni amministrative*, in *www.federalismi.it*, 2020, p. 242 e ss.

[32] Cfr. Cons. Stato, sez. VI, 13 dicembre 2019, n. 8472, in *Giur. it.*, 2020, p. 1190, con nota di M. Timo, *Il procedimento di assunzione del personale scolastico al vaglio del Consiglio di Stato*.

[33] In merito, si veda, da ultimo, S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings*, cit., p. 91 e ss.

[34] Cfr. J. Burrell, *How machines think: Understanding opacity in machine-learning algorithms*, in *Big Data and Society*, 2016, vol. 1, p. 1.

[35] Cfr. F. Pasquale, *The black box society: The secret algorithms that control money and information*, Harvard University Press, 2015; nonché F. Palmiotto, *The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, in Aa.Vv., *Algorithmic Governance and Governance of Algorithms*, a cura di M. Ebers e M. Cantero Gamito, Cham, 2020, p. 49 e ss.

[36] Cfr. S. Quattrocolo, *Equità del processo penale*, cit., pp. 112-113; R. Sicurella, V. Scalia, *Data mining and profiling in the Area of Freedom, Security and Justice*, in *New Journal of European Criminal Law*, 2013, p. 409 e ss.

[37] V. O. Pollicino, M. Bassini, *Commento all'art. 8*, in Aa.Vv., *Carta dei diritti fondamentali dell'Unione europea*, a cura di R. Mastroianni, O. Pollicino, S. Allegrezza, F. Pappalardo, O. Razzolini, Milano, 2017, p. 134 e ss.

[38] Difatti, *« as a result of the need to learn by analysing vast amount of data, AI has become hungry for data, and this hunger has spurred data collection, in a self-reinforcing spiral. Thus, the development of AI systems based on machine learning presupposes and fosters the creation of vast data sets, i.e., big data »*: così, l'*European Parliamentary Research Service* (EPRS), *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, Brussels, 2020, p. 16.

(non piccolo) costituito dalla mancanza di una chiara riserva di giurisdizione. È ben vero che la Corte di giustizia ha ricollegato in vari casi all'art. 8 il necessario intervento di un'autorità giudiziaria — si pensi, ad esempio, alla sentenza della Grande Sezione *Digital Rights Ireland* [39] e al recente caso *H.K. c. Prokuratuur* [40] —, ma non ci si deve dimenticare che la giurisprudenza rappresenta un formante "fluido", che può mutare. Pertanto, sarebbe importante proporre un'interpretazione evolutiva che consenta di fornire una cornice garantistica più solida.

In quest'ottica, mi pare che, sul versante nazionale, si debba perseguire la strada della valorizzazione dell'art. 13 Cost. Credo che l'inviolabilità della libertà personale vada intesa come libertà di autodeterminarsi non solo nel mondo fisico, ma anche in quello virtuale [41]. Secondo molti, l'*habeas corpus* va riconfigurato come *habeas data*, ma ritengo sia necessario ragionare di una protezione integrale della persona nella dimensione elettronica, che adempie alla stessa funzione di garanzia che ha storicamente avuto la libertà con riferimento alle intrusioni fisiche [42]. « Non possiamo oggi non interrogarci sui riflessi connessi alle garanzie processuali di una nuova concezione "integrale" della persona » [43]; invero, è innegabile che alla proiezione di quest'ultima « nel mondo corrisponde il diritto al pieno rispetto di un corpo che, ormai, è al contempo "fisico" ed "elettronico" » [44]. Ed è un corpo che si estende naturalmente ai dispositivi tecnologici di uso comune: penso, in particolare, a quello "strumento degli strumenti" che per i filosofi antichi era la mano e per i contemporanei è lo *smartphone*, nel quale c'è l'intera nostra vita e che rappresenta una vera e propria estensione della nostra mente.

Pertanto, credo che l'art. 13 Cost. sia importante (e ci ritornerò) per il riconoscimento facciale, ma anche in relazione ai captatori, soprattutto con riguardo a quelle attività che si possono compiere attraverso questi ultimi strumenti, le quali sono rimaste estranee alla disciplina recente introdotta tra il 2019 e il 2020 [45]. Sono convinto che, anche prendendo spunto dall'introduzione del professor Ubertis, l'art. 13 Cost. ci consenta di garantire uno schermo più

[39] Cfr. Corte Giust. UE, Grande Sezione, 8 aprile 2014, C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a.*, punto 62. Su tale decisione, cfr., per tutti, L. Trucco, Data retention: *la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giur. it.*, 2014, p. 1850.

[40] Il riferimento è a Corte Giust. UE, Grande Sezione, 2 marzo 2021, C-746/18, *H.K. c. Prokuratuur*.

[41] In merito, cfr. i rilievi di L. Parlato, *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale*, in *Proc. pen. giust.*, 2020, p. 297 e ss.

[42] Cfr. S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma, 2014, p. 30.

[43] Cfr. L. Lupária, Privacy, *diritti della persona e processo penale*, in *Riv. dir. proc.*, 2019, p. 1464.

[44] Queste le parole di S. Rodotà, *Privacy, libertà, dignità. Discorso conclusivo*, 26ª Conferenza Internazionale sulla *Privacy* e sulla Protezione dei Dati Personali, Wroclaw (PL), 14, 15, 16 settembre 2004, reperibile in *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293#:~:text=Senza%20una%20forte%20tutela%20del,la%20costruzione%20di%20una%20soci et%C3%A0*.

[45] Ci si riferisce al d.l. 30 dicembre 2019, n. 161, convertito, con modificazioni, dalla l. 28 febbraio 2020, n. 7. Per una disamina sul tema del captatore alla luce della riforma, v. L. Agostino, M. Peraldo, *Le intercettazioni con captatore informatico: ambito di applicazione e garanzie procedurali*, in *Le nuove intercettazioni. Legge 28 febbraio 2020, n. 7*, a cura di M. Gialuz, in *Diritto di internet*, suppl. al fascolo 3/2020, p. 44 e ss.

solido rispetto a quello dell'art. 24, comma 2, Cost.; e ciò se solo si considera che nel nostro ordinamento, com'è ben noto, la categoria della prova incostituzionale non si è consolidata [46].

Quindi, volendo riassumere quanto finora delineato, si ergono, da un canto, principi classici che vanno semplicemente adattati alla frontiera dell'IA e, dall'altro, principi classici che vanno completamente ripensati (alludo in particolare alla libertà personale).

Infine, vanno segnalate le fonti dedicate all'intelligenza artificiale — vincolanti o atti di *soft law* —, in parte, basate proprio sulla garanzia fondamentale del diritto alla protezione del dato e, in parte, finalizzate ad adattare canoni tradizionali all'IA.

Da questo punto di vista, credo che a livello europeo si sia approcciata la tematica dell'intelligenza artificiale in modo corretto. Dinnanzi alla diffusione di tali strumenti, il tema non è e non può essere se si è a favore o contro di essi, perché le dinamiche, anche economiche, che ci sono state ricordate sono prorompenti [47]. Quindi, occorre stare dentro il processo e governarlo, come sta cercando di fare l'Unione europea e come ha tentato di fare anche il Consiglio d'Europa. In definitiva, il dibattito deve avere ad oggetto il come i sistemi giudiziari saranno in grado, nel prossimo futuro, di far fronte a questi sviluppi tecnologici, senza divenirne vittime, e di inquadrare il loro utilizzo per assicurare il rispetto dei diritti fondamentali.

In tal senso, le fonti vincolanti sono sicuramente il cosiddetto « *data protection reform package* » [48] del 2016, costituito dal regolamento 2016/679/UE (GDPR) e dalla direttiva 2016/680/UE [49]. Quest'ultima, a ben guardare, rappresenta una *lex specialis* in materia di repressione dei reati rispetto al regolamento [50], in quanto mira a stabilire norme minime relative alla « protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la

[46] Sulla dibattuta questione della "prova incostituzionale", cfr., per tutti, P. Tonini, C. Conti, *Il diritto delle prove penali*, 2ª ed., 2014, p. 104 e ss.

[47] Per un quadro sulle potenzialità e sui pericoli dell'IA, si vedano A. Carratta, *Decisione robotica e valori del processo*, in *Riv. dir. proc.*, 2020, pp. 493-497; L. Floridi, J. Cowls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum, C. Luetge, R. Madelin, U. Pagallo, F. Rossi, B. Schafer, P. Valcke, E. Vayena, *An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, in *https://www.researchgate.net/publication/328699738*, 2018, p. 2 e ss.

[48] Cfr. The European Commission's high-level expert group on artificial intelligence, *Draft Ethics Guidelines for Trustworthy AI*, in *https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai*, p. 13.

[49] Com'è noto, la direttiva 2016/680/UE è stata attuata nell'ordinamento italiano dal d.lgs. 18 maggio 2018, n. 51, sul quale v. C. Pansini, *Novità legislative interne*, in *Proc. pen. giust.*, 2018, p. 690 e ss.

[50] Cfr. A. Ripoll Servent, *Protecting or Processing?*, in Aa.Vv., *Privacy, Data Protection and Cybersecurity in Europe*, a cura di W.J. Shünemann e M.O. Baumann, Cham, 2017, p. 125.

prevenzione di minacce alla sicurezza pubblica » [51]. Tale atto racchiude diversi principi rilevanti, ma la norma fondamentale per la materia che ci interessa è senz'altro l'art. 11 della direttiva, che vieta le decisioni basate unicamente sui trattamenti automatizzati [52]. Questa previsione stabilisce infatti che « gli Stati membri dispongono che una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici negativi o incida significativamente sull'interessato sia vietata salvo che sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che preveda garanzie adeguate per i diritti e le libertà dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento ».

Dall'altro lato, per quanto concerne invece le fonti di *soft law*, sul versante della Grande Europa, vi è un'attenzione straordinaria per il crescente impiego di strumenti digitali anche in sede giudiziaria [53]. Al riguardo, è stata già ricordata la Carta etica europea [54], la quale, a sua volta, poggia su un importante studio in tema di *Algorithms and Human Rights*, pubblicato nel marzo 2018 [55]. A ciò si aggiunga la risoluzione dell'Assemblea parlamentare del Consiglio d'Europa *Justice by algorithm — the role of artificial intelligence in policing and criminal justice systems* [56]. A livello eurounitario, vanno menzionati il Libro bianco della Commissione UE sull'intelligenza artificiale del febbraio 2020 [57] e la Carta della robotica del Parlamento europeo del 2017 [58], la quale costituisce « un primo tentativo di codice etico » [59] in materia. Per di più, degne di nota sono le recenti risoluzioni del Parlamento europeo [60], nonché le conclusioni della presidenza

[51] Cfr. art. 1, par. 1, direttiva 2016/680/UE.

[52] Sulla portata dell'art. 11 direttiva 2016/680/UE, si rinvia a M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., p. 16 e ss. Più di recente, per un'analisi di tale previsione, dal punto di vista del rispetto della dignità umana, cfr. S. Signorato, *Il diritto a decisioni penali non basate esclusivamente su trattamenti automatizzati*, cit., p. 107 e ss.

[53] Si veda, di recente, quanto affermato in FRA — European Union Agency for Fundamental Rights, *Getting the future right*, cit., p. 23.

[54] V., *supra*, nota 2.

[55] Ci si riferisce ad *Algorithms and Human Rights — Study on the human rights dimension of automated data processing techniques and possible regulatory implications*, disponibile all'indirizzo: *https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5*.

[56] V. Risoluzione dell'Assemblea parlamentare del Consiglio d'Europa, 2342 (2020), *Justice by algorithm — the role of artificial intelligence in policing and criminal justice systems*, 22 ottobre 2020.

[57] Cfr. Libro bianco della Commissione UE, sull'intelligenza artificiale — Un approccio europeo all'eccellenza e alla fiducia, COM (2020) 65 final, 19 febbraio 2020.

[58] V. Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, P8_TA(2017)0051, 16 febbraio 2017.

[59] In questo senso, A. Adinolfi, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali*, in Aa.Vv., *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, a cura di S. Dorigo, Pisa, 2020, p. 31.

[60] Cfr. Risoluzione del Parlamento europeo, recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate, P9_TA-PROV (2020)0275, 20 ottobre 2020; Risoluzione del Parlamento europeo, recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale, P9_TA-PROV (2020)0276, 20 ottobre 2020; Risoluzione del Parlamento europeo, sui diritti di proprietà intellettuale per lo sviluppo di tecnologie di intelligenza artificiale, P9_TA-PROV(2020)0277, 20 ottobre 2020; nonché, da ultimo, Risoluzione del Parlamento europeo del 20 gennaio 2021 sull'intelligenza artificiale: questioni relative all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE è interessata relativamente agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale, P9_TA(2021)0009, 20 gennaio 2021. Merita osservare che in quest'ultimo atto il Parlamento europeo ha invitato la Commissione « a valutare le conseguenze di una moratoria sull'utilizzo dei sistemi di riconoscimento facciale e, in funzione dell'esito di tale valutazione, a prendere in considerazione l'introduzione di una moratoria sull'utilizzo di tali sistemi da parte delle autorità dello Stato nei luoghi pubblici e nei locali destinati all'istruzione e all'assistenza sanitaria, come pure di una moratoria sull'utilizzo dei sistemi di riconoscimento facciale da parte delle autorità di contrasto in spazi semi-pubblici come gli aeroporti ». Per un primo commento a tale atto, dal punto di vista della sua rilevanza anche nel settore penale, cfr. T. Wahl, *EP Input on AI*, in *Eucrim*, 20 marzo 2021.

del Consiglio UE, *The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change* [61]. Per concludere, sul piano internazionale, va ricordata la raccomandazione del Consiglio dell'OCSE del maggio 2019 [62].

Ora, individuate le fonti, prima di applicarle specificamente alle prove basate sull'IA, vorrei fare un passo avanti per analizzare quelle che sono le peculiarità che l'intelligenza artificiale pone rispetto all'attività probatoria.

3. *Un triplice insieme: prova scientifica, prova digitale e prova fondata sull'IA*

A tale proposito, conviene fissare alcuni punti fermi sul piano concettuale e definitorio, e, in particolare, nel rapporto tra le diverse categorie di prova, quali la prova scientifica e quella informatica.

Mi pare che si possa individuare una macrocategoria, che è, per l'appunto, quella della prova scientifica o, secondo un lessico meno puntuale, della prova tecnica o tecnologica. Com'è noto, in virtù delle categorie tradizionali, la prova scientifica è quella in cui l'inferenza probatoria, che è alla base dell'accertamento del fatto, si fonda su una legge scientifica, che non può essere articolata sulla base delle conoscenze ordinarie [63]. Ebbene, se è così, ritengo che la prova fondata sull'intelligenza artificiale (si pensi alla videoripresa con il riconoscimento facciale, oppure alla stessa BPA) rientri indubitabilmente in tale definizione. Anche questa, infatti, rappresenta una prova tecnica, fondata sull'applicazione della scienza a fini forensi.

A questo punto, ci si dovrebbe porre una seconda domanda: la prova fondata sull'IA è una prova informatica?

All'interno della macrocategoria della prova scientifica, vi è, invero, un sottoinsieme rappresentato dalla prova informatica o prova digitale o prova elettronica — appunto, da *electronic evidence* —, che si riferisce ai casi in cui la

[61] V. Conclusioni della presidenza del Consiglio UE, *The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change*, doc. Consiglio UE n. 11481/20, 21 ottobre 2020.

[62] Cfr. Raccomandazione del Consiglio dell'OCSE sull'intelligenza artificiale, OECD/LEGAL/0449, 22 maggio 2019.

[63] V. Cass., sez. IV, 17 settembre 2010, Cozzini, in *Cass. pen.*, 2011, p. 1679, sulla quale, cfr., tra gli altri, P. Tonini, *La Cassazione accoglie i criteri* Daubert *sulla prova scientifica. Riflessi sulla verifica delle massime di esperienza*, in *Dir. pen. proc.*, 2011, p. 1345.

legge scientifica applicata è quella propria dell'informatica [64]. Pertanto, credo che la prova basata sull'IA appartenga a questo sottoinsieme della prova informatica, proprio perché l'intelligenza artificiale si basa su programmi informatici.

Allora, in ultima analisi, la prova fondata sull'IA è un ulteriore sottoinsieme della prova informatica: secondo la definizione fornita in apertura e acquisita in chiave stipulativa, la tecnologia digitale diventa intelligenza artificiale solo se è programmata per riprodurre almeno una delle capacità cognitive degli esseri umani.

L'impiego del dispositivo basato sull'intelligenza artificiale, quindi, può servire sostanzialmente in due fasi della dinamica probatoria: da un lato, può essere impiegato per la ricerca dell'elemento di prova o della fonte di prova (pensiamo alla videoripresa con riconoscimento facciale *live*, che serve per identificare l'indagato, oppure allo stesso captatore informatico); dall'altro lato, può essere utilizzato nella fase della valutazione dell'elemento di prova. L'esempio è quello di una videoripresa con riconoscimento facciale differita, finalizzata a dare un nome a un volto ripreso in un *frame* statico a disposizione dell'autorità giudiziaria oppure ad analizzare dei reperti (penso, in quest'ultimo caso, alla BPA).

Il fatto che la prova fondata sull'intelligenza artificiale sia un sottoinsieme della prova scientifica e informatica ha un'ovvia, ma significativa, conseguenza. Mi riferisco alla circostanza che anche per la prova fondata sull'IA si ripropongono questioni che sono già state affrontate con riferimento alle prime due.

In primo luogo, questa non è una prova certa, esattamente come quella scientifica. Per quanto essa possa essere affidabile, si può ragionare solo in termini di probabilità, perché, anche se la prova è una videoripresa con riconoscimento facciale che rappresenta, ad esempio, l'omicidio o la rapina, sarà sempre una prova sulla quale bisogna ragionare in termini di probabilità. Non vi è dubbio, infatti, che il frammento di realtà catturato dalla telecamera intelligente andrà contestualizzato, se non altro per esaminare l'elemento soggettivo del reato.

Secondariamente, vi è un problema della catena di custodia del dato e della sua genuinità.

In terza battuta, non deve sfuggire l'ulteriore criticità collegata alla cosiddetta "nuova prova scientifica". Il riferimento è ai celebri criteri Cozzini, vale a dire all'autorità scientifica dell'esperto e alla generale accettazione nella comunità scientifica degli enunciati proposti [65]. In questo punto si colloca la questione fondamentale con riguardo all'intelligenza artificiale, posto che spesso non si conosce il metodo scientifico che sta al fondo dell'algoritmo: accade che que-

[64] Sul punto, v., per tutti, L. Cuomo, *La prova digitale*, in Aa.Vv., *Prova scientifica*, cit., p. 669 e ss.

[65] Cfr. Cass., sez. IV, 17 settembre 2010, Cozzini, cit., p. 1679.

st'ultimo sia segreto [66], oppure che i sistemi di IA si sviluppino autonomamente rispetto a quella che era la programmazione iniziale [67].

Per concludere, l'ultimo aspetto problematico ben noto è quello delle modalità del contraddittorio sulla prova scientifica [68].

4. *La prova fondata sull'IA tra prove tipiche e innominate*

La qualificazione come prova scientifica consente anche di affrontare il tema del canale attraverso il quale si acquisiscono nel processo penale le prove fondate sull'intelligenza artificiale. Viene da chiedersi se queste ultime siano riconducibili *tout court* alla disciplina della prova atipica di cui all'art. 189 c.p.p.

La risposta è ovviamente negativa: dipende dalla singola prova basata sull'IA che viene in rilievo. La Cassazione ci ha insegnato fin dalla sentenza *Franzoni* [69] che quasi tutte le nuove tecniche di accertamento dei fatti offerte dallo sviluppo tecnologico — come, ad esempio, la BPA ormai diversi anni fa — non forniscono prove atipiche, ma sono modalità peculiari di espletamento di prove tipiche, come la perizia o l'esperimento giudiziale. Pertanto, un ragionamento analogo dovrà valere anche — solo per fare un esempio — per le videoriprese con riconoscimento facciale, che possono avere un inquadramento diverso a seconda delle modalità e del contesto.

Più nel dettaglio, laddove la videoripresa con riconoscimento facciale abbia una finalità di mera identificazione, rientrerà nell'art. 4 T.U.L.P.S. oppure nell'art. 349 del codice di rito [70].

Per contro, SARI *Enterprise* — per citare questo metodo italiano —, qualora sia applicato a un'immagine già esistente a fini investigativi e/o probatori, svolge una funzione riconducibile al *genus* rispettivamente dell'individuazione oppure delle ricognizioni fotografiche atipiche, perché in questo caso il riconoscitore non è un uomo, ma è una macchina [71].

Infine, laddove SARI sia applicato in modalità *real-time*, c'è un ulteriore profilo problematico, poiché la macchina fa una ricerca a tappeto su un numero non predeterminato, né (tendenzialmente) predeterminabile di individui. Vista la contestualità, si potrebbe anche pensare alla disciplina delle intercettazioni,

[66] Come esempio significativo può essere menzionato il celebre *tool* statunitense COMPAS (*Correctional Offender Management Profiling for Alternative Sanction*), il quale si basa su un algoritmo brevettato e segreto: per le considerazioni critiche sorte in proposito, v. D. Kehl, P. Guo, S. Kessler, *Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing, Responsive Communities Initiative*, in *Berkman Klein Center for Internet & Society, Harvard Law School*, 2017, p. 11.

[67] Cfr. S. Quattrocolo, *Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi vs rischi e paure della giustizia digitale "predittiva"*, in *Cass. pen.*, 2019, p. 1759.

[68] In merito, v., per tutti, P.P. Rivello, *La prova scientifica*, Milano, 2014, p. 163 e ss.

[69] V. Cass., sez. I, 21 maggio 2008, Franzoni, in *Cass. pen.*, 2009, p. 1840, con nota di F. Caprioli, Scientific evidence, *logiche del probabile nel processo per il "delitto di Cogne"*.

[70] Cfr. J. Della Torre, *Novità dal Regno Unito*, cit., p. 242, nota 112.

[71] V. J. Della Torre, *Novità dal Regno Unito*, cit., p. 242, nota 112; nonché le considerazioni di R. Lopez, *La rappresentazione facciale*, cit., p. 255.

dato che la giurisprudenza tende a utilizzare quel modello per le captazioni: ma, evidentemente, alla videoripresa con riconoscimento facciale manca del tutto la captazione di una comunicazione e, dunque, sulla base delle Sezioni Unite *Prisco* [72], non si può applicare per analogia la normativa sulle intercettazioni. Chiara la conseguenza: si è, nuovamente, in presenza di una prova atipica.

Quindi, per le ultime due prove basate sull'intelligenza artificiale alle quali ho fatto cenno, si pone lo stesso problema: possono entrare nel procedimento sulla base del canale, del *passepartout*, dell'art. 189 c.p.p.?

A me pare che la risposta debba essere negativa per diverse ragioni.

Da un lato, vi è un problema di trasparenza sul funzionamento dell'algoritmo, che non mi permette di sapere se la prova basata su di esso sia effettivamente « idonea ad assicurare l'accertamento dei fatti », come richiesto dall'art. 189 c.p.p.

Dall'altro lato, l'"algoritmo ricognitore" pregiudica la libertà morale in senso ampio, almeno se si interpreta in maniera estensiva quello stesso art. 13 Cost. al quale ho fatto cenno in precedenza. Vengono, infatti, utilizzati dati personali sensibili per individuare o identificare il soggetto il cui volto sia stato "rubato" in una piazza piuttosto che in uno stadio: si tratta insomma di dati biometrici che, ai sensi dell'art. 10 direttiva 2016/680/UE, sono da considerarsi sensibili, che vengono impiegati senza una copertura normativa *ad hoc* e senza consenso, posto che SARI è regolato solo in via amministrativa e non è previsto alcun consenso. Inoltre, si pone un problema di rispetto del principio di proporzionalità tutelato dall'art. 52 Carta di Nizza, dal momento che non vi è alcun bilanciamento in astratto che porti a limitare il diritto fondamentale alla protezione del dato solo laddove le limitazioni « siano necessarie e rispondano effettivamente a finalità di interesse generale », ossia, come ha insegnato la Corte di giustizia, solo per la repressione di forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica.

Insomma, si potrebbe concludere provvisoriamente che quella norma definita "inservibile e inutile" [73] dell'art. 189 c.p.p. potrebbe fare da filtro, se interpretata rigorosamente, almeno rispetto ad alcune prove basate sull'intelligenza artificiale.

Probabilmente, la trincea garantistica rispetto alle prove basate sull'IA coincide con quella vera e propria "linea Maginot" eretta dal codice del 1988, rispetto agli esperimenti gnoseologici che rischiano di pregiudicare la libertà morale: mi riferisco all'art. 64, comma 2, c.p.p., all'art. 188 c.p.p. e allo stesso art. 220, comma 2, c.p.p.

Ma, a ben considerare, non è tutto. Per esigenze di completezza, non si può omettere di dar conto della recente e significativa presa di posizione del garante per la *privacy* nostrano in ordine al sistema SARI *Real-Time*, la quale aggiunge un ulteriore tassello al panorama sin qui tratteggiato. Tale autorità, a differenza

[72] Cfr. Cass., Sez. Un., 28 marzo 2006, Prisco, in *Riv. it. dir. proc. pen.*, 2006, p. 1537.

[73] In questo senso, A. Camon, *La fase che non conta e che pesa: indagini governate dalla legge?*, in *Dir. pen. proc.*, 2017, p. 433.

del vaglio positivo adottato nel 2018 riguardo al meccanismo SARI *Enterprise* [74], ha formulato il 25 marzo 2021 un parere nettamente sfavorevole per quanto concerne l'altra modalità più invasiva di captazione [75], accogliendo così le sollecitazioni della dottrina [76]. Il garante per la protezione dei dati personali, infatti, dopo aver considerato come parametro normativo di riferimento l'art. 7 d.lgs. 18 maggio 2018, n. 51, emanato — lo si rammenti — in attuazione della direttiva 2016/680/UE [77], ha escluso qualsiasi possibilità di utilizzo dello strumento SARI *Real-Time*. E ciò alla luce del condivisibile rilievo secondo cui « allo stato non sussiste una base giuridica idonea [...] a consentire il trattamento dei dati biometrici in argomento » [78].

5. *Le specificità della prova fondata sull'IA*

Giunti a questo punto vi è da dire che la prova basata sull'intelligenza artificiale non è soltanto una prova scientifica, una prova informatica, ma presenta delle peculiarità ulteriori, sulle quali bisogna soffermarsi.

Il primo problema riguarda l'origine dei dati con cui alleno l'algoritmo; gli strumenti basati sull'IA vanno, infatti, "allenati" sulla base di dati, che servono per costruire il sistema [79]. Bisogna pertanto capire da dove provengono questi dati, che devono essere raccolti in modo trasparente e legittimo. Il problema, come vi ho detto, si è posto recentemente negli Stati Uniti per il caso *Clearview*, ma è venuto in rilievo anche con riguardo al *risk assessment tool* noto con il nome di HART (*Harm Assessment Risk Tool*) in Inghilterra, dove erano stati utilizzati dati acquisiti sempre dai *social network* [80].

Il secondo punto critico sorge non appena ci si chiede chi decide sulla scelta dei dati. Questa è una opzione fondamentale, perché incide sull'affidabilità [81]: evidentemente, se si parte da dati spuri o viziati, il risultato sarà una moltiplicazione di *bias* [82].

[74] Cfr. Garante per la protezione dei dati personali, *Sistema automatico di ricerca dell'identità di un volto*, 26 luglio 2018, n. 440.

[75] V. Garante per la protezione dei dati personali, *Parere sul sistema Sari* Real Time, 25 marzo 2021, n. 127.

[76] Cfr. J. Della Torre, *Novità dal Regno Unito*, cit., p. 242 e ss.

[77] V., *supra*, nota 49.

[78] Così, ancora, Garante per la protezione dei dati personali, *Parere sul sistema Sari* Real Time, cit.

[79] Cfr. le indicazioni contenute in Gruppo di Esperti MISE sull'intelligenza artificiale, *Proposte per una Strategia italiana per l'intelligenza artificiale*, 2 luglio 2020, p. 11, reperibili in *https://www.mise.gov.it/index.php/it/per-i-media/notizie/2041246-intelligenza-artificiale-online-la-strategia*.

[80] In argomento, sia consentito rinviare a M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., p. 10 e ss.

[81] Sul punto, cfr. V. Manes, *L'oracolo algoritmico e la giustizia penale*, cit., p. 561.

[82] Cfr., da ultimo, i rilievi formulati dal Gruppo di Esperti MISE sull'intelligenza artificiale, *Proposte per una Strategia italiana per l'intelligenza artificiale*, cit., p. 17. È noto, peraltro, che l'amplificazione delle forme di discriminazione è uno degli aspetti maggiormente criticati nell'utilizzo di *tools* basati sull'IA. A titolo emblematico, si veda il famoso studio realizzato con riferimento

Il terzo profilo problematico attiene alla conoscenza e alla trasparenza del modo in cui funziona l'intelligenza artificiale in ambito probatorio [83]. Questo è essenziale per rispettare il canone del contraddittorio e il diritto di difesa. Invero, dovrebbero essere esclusi a priori sistemi di cui non si conosce il funzionamento.

Da ultimo, la quarta criticità: non possono darsi decisioni totalmente automatizzate. La norma di riferimento — la richiamo ancora una volta — è quella dell'art. 11 della direttiva n. 680 del 2016 [84]: si tratta di un divieto che ricalca sostanzialmente quello dell'art. 22 GDPR [85].

Ebbene, a fronte di questi problemi, mi sembra interessante una decisione del Consiglio di Stato — la sentenza n. 881 del 2020 —, che in qualche modo introduce delle garanzie [86]. Essa si colloca sulla scia di un vero e proprio filone pretorio, iniziato alla fine del 2019 in materia amministrativa [87], dal quale si può estrapolare un compendio di principi che mi paiono estensibili alla materia penale.

In particolare, la pronuncia in esame, concernente un utilizzo in chiave decisoria di un sistema basato sull'intelligenza artificiale ai fini di un concorso pubblico, parte dall'importante presa d'atto secondo cui il ricorso a tale procedura informatica « non deve essere stigmatizzata, ma anzi, in linea di massima, incoraggiata » [88]. E questo, in quanto essa implica « numerosi vantaggi quali, ad esempio, la notevole riduzione della tempistica procedimentale per operazioni

al *risk assessment tool* COMPAS; da tale ricerca è emerso, in particolare, che il *software* in questione sarebbe « *biased against blacks* »: così, J. Angwin, J. Larson, S. Mattu, L. Kirchner, *Machine Bias*, in *www.propublica.org*, 23 maggio 2016. Sul punto, cfr., volendo, M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., p. 7. In aggiunta, tra i molti contributi pubblicati in argomento, v., recentemente, J. Kleinberga, J. Ludwigb, S. Mullainathan, C.R. Sunsteind, *Algorithms as discrimination detectors*, in *https://doi.org/10.1073/pnas.1912790117*, 2020; F.J. Zuiderveen Borgesius, *Strengthening legal protection against discrimination by algorithms and artificial intelligence*, in *The International Journal of Human Rights*, 2020, p. 1572 e ss. Si consideri, da ultimo, quanto emerso nella discussione della Commissione LIBE su *Artificial Intelligence in Criminal Law and its Use by the Police and Judicial Authorities in Criminal Matters*, in relazione ai potenziali effetti discriminatori dei *facial recognition systems*: in proposito, cfr. T. Wahl, *EP LIBE: AI in Criminal Law*, in *Eucrim*, 1° aprile 2020.

[83] Sul problema della trasparenza dei *tools* fondati sull'IA, si vedano, tra i molti, M. Loi, A. Ferrario, E. Viganò, *Transparency as design publicity: explaining and justifying inscrutable algorithms*, in *Ethics and Information Technology*, 2020; V. Manes, *L'oracolo algoritmico e la giustizia penale*, cit., p. 558 e ss.; S. Quattrocolo, *Artificial Intelligence*, cit., p. 17 e ss.

[84] In merito, cfr., *supra*, nota 52.

[85] Sulla disposizione di cui all'art. 22 GDPR, v. G.N. La Diega, *Against the Dehumanisation of decision-Making. Algorithmic decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information*, in *JIPITEC*, 31 maggio 2018, pp. 18-19; nonché, da ultimo, F. Peluso, M. Saporito, *Profilazione e privacy: un confronto fra i modelli Google, Amazon e Facebook*, in *Diritto di internet*, 2021, pp. 210-211; D. Sancho, *Automated Decision-Making under Article 22 GDPR*, in Aa.Vv., *Algorithms and Law*, a cura di M. Ebers e S. Navas, Cambridge, 2020, p. 136 e ss.

[86] Cfr. Cons. Stato, sez. VI, 4 febbraio 2020, n. 881, in *www.pa.leggiditalia.it*. Su tale pronuncia, v. J. Della Torre, *Verso uno statuto delle decisioni algoritmiche: dal Consiglio di Stato spunti estensibili anche alla giustizia penale*, in *Riv. dir. proc.*, in corso di pubblicazione; nonché A.G. Orofino, G. Gallone, *L'intelligenza artificiale al servizio delle funzioni amministrative*, cit.

[87] V., *supra*, nota 31.

[88] Cfr. Cons. Stato, sez. VI, 4 febbraio 2020, n. 881, cit.

meramente ripetitive e prive di discrezionalità, l'esclusione di interferenze dovute a negligenza (o peggio dolo) del funzionario (essere umano) e la conseguente maggior garanzia di imparzialità della decisione automatizzata » [89].

Al contempo, però, la Corte di Palazzo Spada ribadisce che « l'utilizzo di procedure informatizzate non può essere motivo di elusione dei principi che conformano il nostro ordinamento » [90], e, nel fare ciò, fissa alcuni canoni fondamentali.

In primo luogo, si staglia il principio di trasparenza, che va inteso in senso ampio e rafforzato. A detta del Consiglio di Stato, « la conoscibilità dell'algoritmo deve essere garantita in tutti gli aspetti » [91], nel senso che devo conoscerne gli autori, il procedimento usato per la creazione dell'algoritmo e il meccanismo di decisione. Per di più, « non può assumere rilievo l'invocata riservatezza delle imprese produttrici dei meccanismi informatici utilizzati » [92]. In altre parole, nel momento in cui l'impresa mette a disposizione dell'autorità lo strumento informatizzato, accetta le relative conseguenze in termini di *discovery*.

In seconda battuta, per quanto concerne la gestione dei dati, si richiamano i principi fondamentali della direttiva 2016/680/UE.

Rilievo centrale assume, inoltre, il principio di conoscibilità « per cui ognuno ha diritto a conoscere l'esistenza di processi decisionali automatizzati ed in questo caso a ricevere informazioni significative sulla logica utilizzata » [93].

Il quarto canone fondamentale è il cosiddetto "principio di non esclusività della decisione algoritmica", avente, secondo le significative parole dei supremi giudici amministrativi, « rilievo [...] globale in quanto ad esempio utilizzato nella nota decisione *Loomis vs. Wisconsin* » [94]. Più nel dettaglio, nel caso in cui vi sia una decisione automatizzata, bisogna configurare comunque un contributo umano capace di controllare, validare ovvero smentire la decisione automatica. Si tratta di quello che il professor Ubertis ha indicato come « controllo umano significativo » [95].

Il quinto ed ultimo principio è quello di non discriminazione algoritmica, in base al quale il titolare del trattamento dovrebbe, in ogni caso, utilizzare « procedure matematiche o statistiche appropriate per la profilazione » [96], attraverso la predisposizione di misure volte a impedire il verificarsi di effetti discriminatori « nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali,

[89] V. Cons. Stato, sez. VI, 4 febbraio 2020, n. 881, cit.

[90] Cfr. Cons. Stato, sez. VI, 4 febbraio 2020, n. 881, cit.

[91] Cfr. Cons. Stato, sez. VI, 4 febbraio 2020, n. 881, cit.

[92] Cfr. Cons. Stato, sez. VI, 4 febbraio 2020, n. 881, cit.

[93] V. Cons. Stato, sez. VI, 4 febbraio 2020, n. 881, cit.

[94] V. Cons. Stato, sez. VI, 4 febbraio 2020, n. 881, cit. La celebre pronuncia richiamata dall'arresto è la decisione della Corte suprema del Wisconsin del 31 luglio 2016 *State v. Loomis*, 881 NW 2d749 (WIS 2016), sulla quale si veda, da ultimo, S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings*, cit., p. 156 e ss.

[95] V. G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Dir. pen. cont. — Riv. trim.*, 4/2020, p. 83.

[96] Cfr. Cons. Stato, sez. VI, 4 febbraio 2020, n. 881, cit.

dell'appartenenza sindacale, dello *status* genetico, dello stato di salute o dell'orientamento sessuale » [97].

6. *Conclusioni*

Alla luce di ciò, non si può fare a meno di concludere dicendo che occorre ancorare questi canoni, soprattutto a livello interno, perché la decisione del Consiglio di Stato fa riferimento a fonti, anche di *soft law*, e io credo che sul versante europeo vengano in gioco l'art. 8 CEDU, nonché l'art. 8 della Carta di Nizza. Viceversa, nell'ordinamento italiano paghiamo ancora la carente tutela costituzionale del diritto alla protezione del dato, con tutti i suoi corollari che assumono rilevanza per la prova basata sull'IA.

Riprendo quindi lo spunto che ho lanciato poc'anzi, rispetto alla necessità di valorizzare l'inviolabilità della libertà personale di cui all'art. 13 Cost., intesa come *habeas data*. Mi sembra che, dinnanzi alle sfide poste in materia probatoria dall'intelligenza artificiale, sia ancora più stringente l'ammonimento di Stefano Rodotà, secondo il quale « senza una forte tutela del "corpo elettronico", dell'insieme delle informazioni raccolte sul nostro conto, la stessa libertà personale è in pericolo » [98]. Occorre insomma valorizzare le classiche garanzie poste dall'art. 13 Cost.: pertanto deve essere il legislatore — solo per fare un esempio — a disciplinare il riconoscimento facciale [99], nelle sue diverse varianti, e dovrà essere il giudice o il pubblico ministero, ossia persone umane, ad avere la responsabilità della valutazione, sulla scorta di quel modello che, in ambito matematico ed informatico, viene definito come HITL (*human in the loop*), in cui per produrre il suo risultato di prova è necessario che la macchina probatoria interagisca con l'essere umano.

[97] Cfr. Cons. Stato, sez. VI, 4 febbraio 2020, n. 881, cit.

[98] Così, S. Rodotà, *Privacy, libertà, dignità*, cit.

[99] A tale riguardo, si veda, peraltro, la recente proposta di legge (p.d.l. n. 3009, Atti Camera, XVIII Legislatura) d'iniziativa degli On. Sensi, Borghi, Madia, Quartapelle Procopio, Serrachiani e Verini, presentata il 12 aprile 2021 e volta a prevedere una sospensione dell'installazione e dell'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso di dati biometrici in luoghi pubblici o aperti al pubblico, in attesa dell'« entrata in vigore di una disciplina legislativa della materia e comunque non oltre il 31 dicembre 2021 ». Tale proposta di legge, secondo la relazione di accompagnamento, accoglie così « l'invito del Parlamento europeo » (v., *supra*, nota 60), nonché di diverse organizzazioni per i diritti civili a prevedere una moratoria per l'utilizzo di tali strumenti fino all'adozione di « una normativa che assicuri il pieno rispetto dei diritti costituzionali dei cittadini ».