UNIVERSITÀ
DI TRENTO
Facoltà di
Giurisprudenza

INTELLIGENZA ARTIFICIALE E PROCESSO PENALE

INDAGINI, PROVE, GIUDIZIO

a cura di
GABRIELLA DI PAOLO
LUCA PRESSACCO

2022

UNIVERSITÀ
DI TRENTO
Facoltà di
Giurisprudenza

QUADERNI DELLA FACOLTÀ DI GIURISPRUDENZA

63

2022

Al fine di garantire la qualità scientifica della Collana di cui fa parte, il presente volume è stato valutato e approvato da un *Referee* interno alla Facoltà a seguito di una procedura che ha garantito trasparenza di criteri valutativi, autonomia dei giudizi, anonimato reciproco del *Referee* nei confronti di Autori e Curatori.

ISBN 978-88-8443-990-1
ISSN 2284-2810

Il presente volume è pubblicato anche in versione cartacea grazie al contributo della Struttura Dipartimentale Facoltà di Giurisprudenza dell'Università degli Studi di Trento nell'ambito dell'iniziativa "Dipartimenti di eccellenza - legge 232/2016 art. 1 commi da 314 a 338" – MUR per i tipi di Editoriale Scientifica - Napoli
con ISBN 979-12-5976-459-1

Dicembre 2022

INTELLIGENZA ARTIFICIALE E PROCESSO PENALE

INDAGINI, PROVE, GIUDIZIO

a cura di

GABRIELLA DI PAOLO

LUCA PRESSACCO

Università degli Studi di Trento 2022

INDICE

NOTIZIE SUGLI AUTORI

Jacopo Della Torre – Ricercatore a tempo determinato (RtdB) di Diritto processuale penale presso l'Università degli Studi di Genova

Gabriella Di Paolo – Professoressa ordinaria di Diritto processuale penale presso l'Università degli Studi di Trento

Giulia Lasagni – Ricercatrice a tempo determinato (RtdB) di Diritto processuale penale presso l'Alma Mater Studiorum, Università di Bologna

Lucia Maldonato – Assegnista di ricerca in Diritto penale presso l'Università Cattolica del Sacro Cuore di Milano

Luca Pressacco – Assegnista di ricerca in Diritto processuale penale presso l'Università degli Studi di Trento

Serena Quattrocolo – Professoressa ordinaria di Diritto processuale penale presso l'Università degli Studi del Piemonte Orientale "Amedeo Avogadro"

PREMESSA

L'utilizzo dei *software* fondati sull'intelligenza artificiale (IA) in ambito processuale rappresenta l'ultima evoluzione del complesso rapporto che lega nuove tecnologie e giurisdizione penale. L'IA, tuttavia, non si limita ad agevolare lo svolgimento di alcune attività processuali, bensì promette – come esprime il termine stesso – di imitare o di riprodurre le capacità cognitive degli esseri umani e, per quanto interessa in questa sede, dei soggetti del processo. Poiché l'umanità del giudizio affonda le sue radici nella dignità della persona, l'IA ha attirato sin da subito l'attenzione degli studiosi ed è stata oggetto di alcuni pionieristici tentativi di regolazione, maturati nel contesto istituzionale dell'Unione europea. Sono stati prontamente individuati i pericoli insiti nella tumultuosa rivoluzione in atto, sottolineando l'attitudine degli strumenti in questione a convertirsi in autentiche "tecnologie di controllo", idonee a conculcare gravemente le libertà individuali e, in particolar modo, le garanzie processuali. Affinché questa cupa profezia non si autoavveri, secondo ben noti meccanismi di psicologia sociale, è necessario compiere uno sforzo di immaginazione, riflettendo sui limiti e sulle potenzialità applicative degli strumenti in esame, per offrire un'alternativa credibile – anzitutto in prospettiva culturale e, nei limiti in cui ciò risulta possibile in sede scientifica, anche nella dimensione applicativa – ai soggetti che operano a vario titolo nel sistema di giustizia penale.

Da questa ispirazione di fondo, è nata l'idea di organizzare un seminario di approfondimento sul rapporto tra "*Intelligenza artificiale e processo penale*". Il compito di svolgere le relazioni principali è stato affidato ad alcuni giovani studiosi, provenienti da diversi Atenei italiani, che – nel medesimo arco temporale – hanno condotto ricerche dedicate proprio alle interferenze tra le tecnologie di *artificial intelligence* e le discipline penalistiche. L'iniziativa si è svolta in videoconferenza il 12 novembre 2021, con la partecipazione di un nutrito pubblico di accademici ed esponenti delle professioni legali, testimoniando la sensibilità delle tematiche in oggetto e suggerendo l'opportunità di dare un seguito

editoriale all'incontro realizzato in modalità virtuale. Il presente volume costituisce, pertanto, una raccolta ragionata delle riflessioni che sono state svolte in quella sede e vede la luce grazie alle risorse provenienti dal finanziamento del Dipartimento di eccellenza.

Considerata la varietà degli argomenti trattati, ogni capitolo contiene una bibliografia autonoma ma – per il lettore interessato a individuare i riferimenti utili per un primo approccio alla materia – in appendice al volume è stata inserita una bibliografia essenziale concernente il rapporto tra intelligenza artificiale e la dimensione giuridica, specialmente processuale.

Un ringraziamento sincero va a tutti coloro che hanno reso possibile lo svolgimento del convegno di cui si presentano gli atti, ai relatori per l'impegno profuso anche nella fase di redazione dei rispettivi contributi (nonostante innumerevoli incombenze accademiche) e a tutti coloro che hanno variamente contribuito alla pubblicazione del presente volume. Infine, desideriamo rivolgere un ringraziamento speciale alla Prof.ssa Serena Quattrocolo, autrice di uno studio pionieristico sui rapporti tra intelligenza artificiale e processo penale, per aver accettato di svolgere le conclusioni del convegno di cui si presentano gli atti, stilando in seguito anche la prefazione che il lettore può trovare nelle prime pagine di questo volume.

I curatori

PREFAZIONE

Serena Quattrocolo

Il volume rappresenta il risvolto editoriale di un interessante convegno svoltosi *on line*, nell'autunno del 2021, organizzato dal Dipartimento di Giurisprudenza dell'Università di Trento, sul tema dei rapporti tra "Intelligenza artificiale e processo penale", nell'ambito del progetto dei Dipartimenti di Eccellenza, finanziato dal Ministero dell'Università.

In quell'occasione, avevo ricevuto il graditissimo invito a presentare delle conclusioni, potenzialmente riassuntive, dei ricchi spunti emersi dal pomeriggio di lavori. E con altrettanto piacere provo, in questa sede, ad offrire una prefazione allo stimolante volume che ne è emerso.

Prendendo le mosse da un dato formale, non si può negare che anche negli studi giuridici, il tema delle interazioni con l'intelligenza artificiale (IA) stia ricevendo significativa attenzione. Incontri, seminari, scritti, raccolte stanno occupando molti studiosi delle scienze giuridiche, anche nel settore tradizionalmente meno elastico nella ricezione delle innovazioni tecnologiche, ovvero quello della giustizia penale. È invitabile, del resto, il fermento attorno ad un tema che suscita reazioni polarizzate, distopiche o utopiche, anche per via di alcune problematiche di fondo.

In primo luogo, la cultura giuridica europea, ma soprattutto italiana, ha lungamente ignorato un'area di ricerca computazionale da tempo sviluppatasi non solo oltreoceano, la cosiddetta *AI & Law*. Sin dagli albori, infatti, il ragionamento giuridico (si veda L. Pressacco, cap. III) ha rappresentato per l'intelligenza artificiale una sfida estremamente stimolante, essendo un dominio delle attività umane ispirato ma non determinato da regole prestabilite. In secondo luogo, e in diretta conseguenza con quanto appena osservato, nella maggior parte degli operatori del diritto è mancata una conoscenza anche solo superficiale delle caratteristiche essenziali dell'IA (si veda G. Lasagni, Cap. II), sostituita, piuttosto, da suggestioni per lo più letterarie e cinematografiche, ben lontane dalla realtà delle scienze computazionali. Il fermento di cui sopra, allora – pur caratterizzato dall'invitabile polarizzazione che circonda ogni fenome-

no ancora sconosciuto – ha il pregio di aver spinto anche gli operatori meno curiosi verso un contatto introduttivo con i temi che ci interessano, favorendo la possibilità di ampliare le conoscenze circa la consistenza e lo stato degli studi computazionali in materia e gettando le basi per la costruzione di un glossario comune, tra giuristi e informatici, essenziale per lo sviluppo di una intelligenza artificiale utile al diritto e, per quanto ci riguarda, utile al processo penale (tema, quello dell'utilità che riprenderò in conclusione).

Lasciando il dato formale per immergersi in quello di merito, si deve osservare come questo volume si ponga al di fuori – o meglio, al di sopra – del disordinato fermento di cui si è parlato, per offrire diversi approfondimenti che proiettano il lettore a un livello avanzato di riflessione.

I quattro capitoli che compongono l'opera, infatti, muovono opportunamente da un piano nel quale le caratteristiche essenziali, le principali modalità di funzionamento, i più evidenti limiti (si veda J. Della Torre, Cap. I) della *data driven AI* sono dati per conosciuti. Senza ripercorrere le ormai note 'stagioni' vissute, a partire dagli anni Cinquanta del secolo scorso dall'IA (con ripetute primavere e inverni), è utile premettere che il momento presente è caratterizzato da soluzioni computazionali e modelli che si basano sul trattamento di dati, di *big data* (si veda L. Maldonato, Cap. IV). La *data driven AI*, infatti, è una forma di intelligenza artificiale, oggi predominante, che sfrutta l'improvvisa e inarrestabile disponibilità di dati digitali, verificatasi con la cosiddetta 'Quarta Rivoluzione', innescata dall'inedita accessibilità, a costi contenuti, delle materie prime necessarie per produrre dispositivi digitali sempre più piccoli, potenti ed economicamente convenienti.

Ebbene, i pregi e le caratteristiche di questo tipo di IA sono ormai noti anche alla comunità giuridica, soprattutto per via delle esperienze filtrate per lo più da ordinamenti di *common law* e, soprattutto, sono stati attentamente studiati dalle principali istituzioni europee, con lo scopo di predisporre un'efficace governance dell'IA, individuata soprattutto dall'Unione europea come eccezionale volano di crescita per il continente europeo, che deve tuttavia essere convogliato all'interno di attente politiche di contemperamento con gli interessi sociali. Numerosissimi, ormai, gli interventi di *soft law*, sia dell'Unione europea, sia del Consiglio d'Europa (quest'ultimo con la Carta etica per l'uso dell'IA nei sistemi giudiziari, pubblicata nel 2018), ma anche i testi vincolanti, come la

direttiva 2016/680/UE, il regolamento 2016/679/UE e, in prospettiva, la Proposta di regolamento sull'intelligenza artificiale, denominata *AI Act*, ancora in fase di negoziazione tra Parlamento e Consiglio dell'Unione europea (giunta attualmente alla terza formulazione).

Gli scritti raccolti in questo volume – dedicati, rispettivamente, alle applicazioni investigative e probatorie del riconoscimento facciale (Cap. I, Jacopo Della Torre); all'impiego dell'IA anche a scopi difensivi (Cap. II, Giulia Lasagni); ai rapporti tra IA e ragionamento giuridico (Cap. III, Luca Pressacco); agli strumenti psico-criminologici di accertamento del rischio di recidivanza e di comportamento violento (Cap. IV, Lucia Maldonato) – muovono dai due capisaldi qui richiamati, ovvero la generalizzata conoscenza di base delle caratteristiche dell'IA e l'esistenza di un substrato normativo rilevante a livello europeo, per portare il lettore a una riflessione più approfondita. I temi percorrono tutto l'arco del procedimento penale, nella prospettiva di proiettare soluzioni tecniche ispirate alla miglior scienza computazionale, all'interno dell'esistente quadro normativo, europeo e nazionale.

La spinta che si percepisce in tutti i capitoli è quella di guidare la riflessione oltre la ricordata polarizzazione rispetto al fenomeno dell'IA, per avviare un dialogo consapevole e informato con gli esperti di scienze computazionali, al fine di sviluppare una IA utile al processo penale. Avendo conquistato un adeguato substrato di conoscenza, tocca oggi al processualista assumere l'iniziativa di creare, insieme agli esperti informatici, le soluzioni computazioni più avanzate che possano aiutare a circoscrivere, se non a risolvere, i principali problemi del processo penale italiano. E' innegabile che l'attuale condizione della giustizia penale italiana si avvicini molto ad uno scenario di denegata giustizia, per via delle estreme difficoltà in cui devono operare tutti gli attori del procedimento penale, i magistrati, gli avvocati, il personale amministrativo – ormai ridotto ai minimi termini – le forze che svolgono attività di polizia giudiziaria… Occorre dunque guardare con obiettività alle potenzialità dell'IA ed assumere con decisione un ruolo non più passivo, ma proattivo nella individuazione di soluzioni tecniche che, nel pieno rispetto del quadro normativo vigente, possano aiutare a restituire effettività alla giustizia penale italiana.

In questo volume, gli spunti certo non mancano.

Buona lettura,

SQ

QUALE SPAZIO PER I *TOOLS* DI RICONOSCIMENTO FACCIALE NELLA GIUSTIZIA PENALE?

Jacopo Della Torre

1. Premessa: i software *di riconoscimento facciale tra intelligenza artificiale e biometria*

In pochi decenni, l'intelligenza artificiale[1] (d'ora in avanti, IA) si è trasformata da materia fantascientifica in uno dei pilastri delle società contemporanee. A parte il mercato multimiliardario che si sta sviluppan-

[1] Com'è noto, al giorno d'oggi non esiste una definizione universalmente condivisa di "intelligenza artificiale": sul punto v., per tutti, L. FLORIDI, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Milano, 2022, p. 40. Per siffatta ragione è utile specificare che in questo lavoro si utilizzerà la spiegazione del concetto elaborata dalla «Carta etica sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli altri ambiti connessi», adottata dalla Commissione europea per l'efficienza della giustizia CEPEJ nel corso della sua XXXI riunione plenaria, Strasburgo, 3 dicembre 2018 [CEPEJ (2018) 14], che la intende come l'«insieme di metodi scientifici, teorie e tecniche finalizzate a riprodurre mediante le macchine le capacità cognitive degli esseri umani» (p. 47 versione italiana). Per un'analisi dell'atto, 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.eu*, 18 dicembre 2018.

do attorno a tale branca dell'informatica[2], è soprattutto l'impatto profondo che essa sta avendo sulla nostra quotidianità a rendere evidente tale mutamento epocale. Catalogare e riconoscere immagini, tradurre testi, compiere diagnosi o prognosi mediche, pilotare droni o automobili, scrivere canzoni, sono, d'altra parte, solo alcune delle attività che vengono oggigiorno compiute dagli «agenti artificiali»[3]. Ed è proprio la presa d'atto per cui l'IA, «*thanks to the Internet of Things, is constantly present in our lives*»[4] ad aver portato ad affermare che vivremmo già in «società algoritmiche», cioè organizzate intorno al processo decisionale automatizzato delle tecnologie digitali[5].

Naturalmente, il mondo del diritto non poteva rimanere estraneo a cambiamenti tanto radicali.

Da un lato, sempre più sistemi giuridici interni e sovranazionali, anche al fine di mantenersi competitivi a livello globale, hanno iniziato a predisporre articolate strategie di intervento in questo settore, tese a guidare gli investimenti e a gettare le basi per una sua prima normazione[6]. Al riguardo, basti solo pensare alla «*digital agenda*», fissata dall'Unione europea a partire dal 2018[7], culminata nella "storica" proposta di regolamento "generale" sull'IA dell'aprile 2021[8], in fase di negoziazione da parte del legislatore eurounitario.

---

[2] Secondo un recente studio (cfr. *IDC, Forecasts Companies to Increase Spend on AI Solutions by 19.6% in 2022*, in *www.idc.com*, 15 febbraio 2022), tale mercato si attesterà globalmente, nel 2022, oltre i 430 miliardi di dollari.

[3] Cfr. L. Floridi, J.W. Sanders, *On the Morality of Artificial Agents*, in *Minds and Machines*, 2004, p. 349.

[4] Sono parole di M. Caianiello, *Dangerous Liaisons. Potentialities and Risks Deriving from the Interaction between Artificial Intelligence and Preventive Justice*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2021, n. 1, p. 2.

[5] Si allude alla posizione espressa da M. Balkin, *The Three Laws of Robotics in the Age of Big Data*, in *Ohio State Law Journal*, 2017, p. 1219.

[6] Per un quadro europeo del fenomeno, v. *JRC, OECD report, AI Watch. National strategies on Artificial Intelligence. A European perspective*, 2021, in *www.publications.jrc.ec.europa.eu*.

[7] Cfr. comunicazione della Commissione europea, *L'intelligenza artificiale per l'Europa*, COM (2018) 237, del 25 aprile 2018.

[8] Ci si riferisce alla *Proposta di regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, COM (2021) 206, Bruxelles, 21 aprile 2021. Per un commento, cfr. G. Contissa, F. Galli, F. Godano, G. Sartor, *La nuova Proposta di Regolamento euro-*

Da un altro lato, l'ultimo decennio ha visto pure l'intensificarsi del dibattito circa l'impiego degli strumenti digitali, al fine di rendere più efficiente il lavoro degli operatori della giustizia, pubblici e privati[9].

Com'è noto, il sistema penale non sfugge al fenomeno, anzi[10]. La "lunga onda" dell'IA ha "travolto" a tal punto pure tale settore, da trovare già, in alcuni Paesi, possibili applicazioni trasversali dalla fase della prevenzione, al procedimento penale di cognizione, per arrivare al momento esecutivo[11].

Accanto al discusso settore degli algoritmi «predittivi»[12], uno dei

---

peo sull'intelligenza artificiale: questioni giuridiche e approcci regolatori, in R. Brighi (a cura di), *Nuove questioni di informatica forense*, Roma, 2022, p. 387.

[9] Cfr., solo per fare alcuni esempi, i volumi di G. Alpa (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020; S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020; J. Nieva-Fenoll, *Intelligenza artificiale e processo*, Torino, 2019; H.-W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, G. De Gregorio (a cura di), *Constitutional Challenges in the Algorithmic Society*, Cambridge, 2021; U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020.

[10] Per un quadro di sintesi del dibattito in materia, v. F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Diritto penale contemporaneo – Archivio web*, 29 settembre 2019; C. Burchard, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *Riv. it. dir. proc. pen.,* 2019, p. 1908; M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Diritto penale contemporaneo – Archivio web*, 29 maggio 2019; L. Lupária, *Artificial Intelligence in Criminal Courts. Opportunity or Threat?*, in A.M. Lopez Rodriguez, M.D. Green, M.K. Kubica (a cura di), *Legal Challenges in the New Digital Age*, Leiden, 2021, p. 160; V. Manes, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, cit., p. 547; P.P. Paulesu, *Intelligenza artificiale e giustizia penale. Una lettura attraverso i principi,* in *Archivio penale – Rivista web*, 2022, n. 1; S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Cham, 2020 e G. Ubertis, *Intelligenza artificiale e diritto penale*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2020, n. 4, p. 75. Cfr. anche il volume collettaneo *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021.

[11] Non a caso, negli Stati Uniti vengono già proposti "schemi circolari", volti a rappresentare il fatto che le tecnologie in esame operano non solo trasversalmente, ma si influenzano pure in modo reciproco, tramite i dati prodotti: cfr., ad esempio, EPIC, *AI in the Criminal Justice System*, in *www.epic.org*.

[12] All'interno di tale eterogeneo *genus* rientrano, tanto quei mezzi preventivi, come i

terreni d'elezione principali che l'IA ha attualmente in campo penale è quello degli applicativi biometrici digitali[13]. Con tale locuzione, ci si riferisce a un gruppo eterogeneo di *tools*, tesi ad automatizzare l'analisi di caratteristiche fisiologiche della persona (quali le impronte facciali o digitali, la forma della mano, dell'iride, e così via), oppure comportamentali (come la voce, la firma o l'andatura), acquisite da sensori elettronici, elaborate da specifici programmi «e, infine, trasformate in modelli matematici»[14]. La scienza biometrica ci mostra, insomma, come, a seguito del progresso tecnologico, i nostri corpi si siano trasformati «in una "miniera a cielo aperto" dalla quale attingere dati ininterrottamente»[15]; essi sono, infatti, «oggetto di un processo di de-composizione ove ogni aspetto viene raccolto, conservato e consegnato ad una macchina»[16].

Il presente contributo vuole concentrarsi su una delle tipologie di tecniche biometriche il cui impiego in ambito penale è più discusso: i *software* di riconoscimento facciale[17]. Si tratta di mezzi che, pur trovan-

---

software di *predictive policing*, che hanno il fine di identificare *ex ante* il tempo e il luogo di commissione di attività illecite, quanto quelli operanti in sede procedimentale, volti a compiere predizioni razionali su comportamenti futuri individuali (tipico esempio sono i *risk assessment tools*, tesi a calcolare il rischio di recidiva o di fuga di un prevenuto). V., sul punto, tra i molti, S. Signorato, *Giustizia penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo*, in *Riv. dir. process.*, 2020, p. 605. Per ulteriori approfondimenti al riguardo, v. *infra*, cap. IV.

[13] Per due ampie ricerche in argomento, v. *Greens/EFA*, *Biometric & Behavioural Mass Surveillance in EU Member States*, in *www.greens-efa.eu*, 25 ottobre 2021, nonché C. Wendehorst, Y. Duller, *Biometric Recognition and Behavioural Detection. Study Requested by the JURI and PETI committees*, Bruxelles, 2021.

[14] La citazione è tratta da E. Sacchetto, *Spunti per una riflessione sul rapporto tra biometria e processo penale*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2019, n. 2, p. 476.

[15] Sono parole di S. Rodotà, *Trasformazioni del corpo*, in *Politica dir.*, 2006, p. 6.

[16] Cfr. F. Paolucci, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *Media Laws – Rivista di diritto dei Media*, 2021, n. 1, p. 208.

[17] Nella letteratura interna v., oltre al lavoro monografico di G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021, i saggi di G. Borgia, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, in *www.lalegislazionepenale.eu*, 11 dicembre 2021; E. Currao, *Il riconoscimento facciale e*

do le loro radici in studi pionieristici degli anni Sessanta[18], hanno subito un *boom* dirompente negli ultimi decenni. Proprio grazie ai grandi progressi assicurati dall'IA[19], che li ha resi molto più accurati e a buon mercato, essi hanno iniziato a venir utilizzati in una serie sempre più vasta di settori pubblici e privati[20], fino a entrare a far parte della nostra quotidianità, specie tramite *device* come *smartphone* o *tablet*.

In via preliminare, è il caso di ricordare che gli *automatic facial recognition systems* (d'ora in avanti *AFRS*) sono stati definiti, a livello europeo, come meccanismi che permettono di analizzare «immagini digitali contenenti volti di individui, per scopi di identificazione, autenticazione/verifica, o categorizzazione di suddetti individui»[21].

A livello tecnico, essi operano sulla base di alcuni passaggi susseguenti[22]. In prima battuta, acquisiscono il "dato grezzo" rappresentato

---

i diritti fondamentali: quale equilibrio?, in *Diritto penale e uomo*, 19 maggio 2021; R. Lopez, *La rappresentazione facciale tramite* software, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2019, p. 239; Ead., *Riconoscimento facciale tramite* software *e individuazione del sospettato*, in A. Scalfati (a cura di), *Pre-investigazioni (Espedienti e mezzi)*, Torino, 2020, p. 295; E. Sacchetto, Face to face: *il complesso rapporto tra* automated facial recognition technology *e processo penale*, in *www.lalegislazionepenale.eu*, 16 ottobre 2020; L. Saponaro, *Le nuove frontiere tecnologiche dell'individuazione personale*, in *Archivio penale – Rivista* web, 2022, n. 1; M. Torre, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Dir. pen. proc*., 2021, p. 1042; R.V.O. Valli, *Sull'utilizzabilità processuale di Sari: il confronto automatizzato di volti rappresentati in immagini*, in *ilPenalista*, 16 gennaio 2019. Cfr. volendo anche J. Della Torre, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della* High Court of Justice, in *Diritto penale contemporaneo – Rivista trimestrale*, 2020, n. 1, pp. 231 ss.

[18] Cfr., per una panoramica diacronica, l'articolo di T. Klosowski, *Facial Recognition is Everywhere. Here's What We Can Do About It*, in *www.nytimes.com*, 15 luglio 2020.

[19] Come ricorda S. Quattrocolo, *op. ult. cit*., pp. 65 s., «*the main techniques used in face recognition are the PCA (Principal Component Analysis), the LFA (Local Feature Analysis) and neural networks*».

[20] Tanto che il mercato del riconoscimento facciale, valutato in meno di 4 miliardi di dollari nel 2018, si stima supererà i 10 nel 2025: cfr. E. Li, *Europe's Next Steps in Regulating Facial Recognition Technology*, in *Columbia Journal of Transnational Law – Bullettin Blogposts*, 7 novembre 2021.

[21] La definizione è del Gruppo di lavoro "Articolo 29", parere 2/2012 – WP 192, adottato il 22 marzo 2012.

[22] Per una spiegazione del funzionamento dei *tools*, cfr. W. Crumpler, J.A. Lewis, *How Does Facial Recognition Work?. A primer*, in *www.csis.org*, 10 giugno 2021.

dall'immagine di un volto umano. In secondo luogo, dopo aver attenuato le variazioni di colore o di dimensione all'interno del *frame*, rilevano una serie di caratteristiche individualizzanti del viso – come la posizione degli occhi, del naso, delle narici, del mento e delle orecchie[23] – e, per il loro tramite, elaborano un "modello", detto *template*, il quale è passibile di confronto con le immagini (note) presenti in archivio. Infine, laddove all'esito di questa ricostruzione algoritmica dell'"architettura facciale" «emerga con una certa probabilità che le due immagini si riferiscono alla stessa persona, si avrà il c.d. "*matching*"»[24].

A ciò deve aggiungersi che gli algoritmi in questione possono essere impiegati, tanto in modalità «statica» (o *ex post*), quanto «dinamica» (o *real-time*)[25]. Nel primo caso, essi raffrontano l'immagine di un volto già acquisita in precedenza, con i profili contenuti in *database* di dimensioni variabili. Al contrario, laddove siano utilizzati *live*, i *software* consentono di esaminare "in diretta" i flussi provenienti da telecamere; di selezionare le "impronte facciali" delle persone riprese e di cercare, infine, una corrispondenza tra queste ultime e i volti contenuti in un archivio di partenza.

Allo stesso tempo, non va tralasciato che, negli ultimi anni, gli *AFRS* hanno acquisito importanza anche in ottica di *sentiment analysis*[26], ovvero quali tecnologie impiegate per studiare le emozioni degli individui, a partire dalle loro espressioni del volto[27]. Si tratta, evidentemente, di un'applicazione assai critica, posto che, in questa prospettiva, le macchine finiscono per impattare su quello che do-

[23] Sui cosiddetti "punti di repere" del viso, v. E. Sacchetto, *op. ult. cit*., p. 3.

[24] Così G. Borgia, *op. cit*., pp. 2 s.

[25] Al riguardo, v. *Greens/EFA*, *Biometric & Behavioural Mass Surveillance*, cit., p. 27.

[26] In argomento, cfr. A. McStay, *Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy*, in *Big Data & Society*, 2020, p. 1.

[27] Cfr., sul punto, lo studio dell'*European Parliamentary Research Service* (*EPRS*), *Regulating facial recognition in the EU*, settembre 2021, p. 4, nonché quello dell'*European Data Protection Supervisor*, *Facial Emotion Recognition*, in *www.edps.europea.eu*, *TechDispatch* 1/2021.

vrebbe essere un "giardino proibito": la libertà morale[28] o psichica[29] della persona.

Una volta fornite tali indicazioni di base, nelle prossime pagine si procederà a studiare, più da vicino, le problematiche sollevate dall'impiego dei *face detection systems* nel contesto, oltremodo delicato, in ragione dei principi fondamentali che lo permeano, costituito dalla giustizia penale. Più in particolare, dopo aver descritto le potenzialità e i numerosi rischi, che caratterizzano tali meccanismi, il *focus* sarà rivolto all'esperienza italiana. Come si avrà modo di vedere, gli *AFRS* sono oramai diffusi pure nel sistema processuale penale interno. Nondimeno, la mancata regolazione compiuta del fenomeno da parte del legislatore ha acuito il pericolo che gli stessi finiscano per tramutarsi, da strumenti potenzialmente utili in termini di efficienza, in autentiche "trappole" per i diritti fondamentali dell'individuo.

2. Le potenzialità dell'impiego dei facial recognition system *in campo penale*

L'esigenza di raccogliere i dati biometrici di imputati, arrestati o ricercati affonda, ovviamente, le sue radici «nella notte dei tempi»[30]. Onde avere un concreto esempio di ciò, basta ricordare come, già nel Seicento, un inquisitore del calibro di Eliseo Masini esortasse, nel suo «*Sacro*

[28] Da intendersi, per riprendere le parole di L. Scomparin, *La tutela del testimone nel processo penale*, Padova, 2000, p. 2, come il diritto «di formare senza costrizioni la propria volontà e di muovere il proprio comportamento esteriore in conformità delle spinte psichiche interne, senza intromissioni e senza la sottoposizione coatta ad introspezioni che ne svelino il concreto funzionamento». In argomento, cfr., *ex multis*, A. Bonomi, *Libertà morale e accertamenti neuroscientifici: profili costituzionali*, in *BioLaw Journal – Rivista di biodiritto*, 2017, n. 3, pp. 142 ss. e G. Vassalli, *Il diritto alla libertà morale. Contributo alla teoria dei diritti della personalità*, in Id., *Scritti giuridici*, III, *Il processo e le libertà*, Milano, 1997, pp. 253 ss.

[29] In proposito si parla anche di garanzia dell'*habeas mentem*: cfr. G. Di Paolo, *Tecnologie del controllo e prova penale. L'esperienza statunitense e spunti per la comparazione*, Padova, 2008 p. 169, la quale riprende la risalente posizione di A. Baldassarre, Privacy *e Costituzione: l'esperienza statunitense*, Roma, 1974, pp. 397 ss.

[30] Cfr. L. Garlati, *Alle origini della prova scientifica: la scuola di polizia di Salvatore Ottolenghi*, in *Revista brasileira de Direito processual penal*, 2021, p. 885.

arsenale», a prendere nota, nel modo più particolareggiato possibile, di tutte le informazioni circa i tratti somatici dei prevenuti, onde così poterli riconoscere in seguito più facilmente[31].

A ben vedere, neppure l'idea di individuare un metodo scientifico, volto a rendere più oggettiva ed efficiente l'attività di riconoscimento delle persone per finalità procedimentali, può dirsi una novità. È, del resto, risaputo che le prime iniziative in proposito risalgono già agli ultimi decenni dell'Ottocento[32], per opera di alcuni noti criminologi, come il francese Alphonse Bertillon, fondatore dell'«antropometria»[33].

Preso atto di ciò, ben si intuirà perché l'opportunità di affidare compiti "ricognitivi" a macchine di ultima generazione abbia suscitato vivo entusiasmo, specie tra le autorità di *law enforcement*. Un tanto ha, invero, esaudito l'«atavico desiderio» di mettere al servizio della giustizia penale tecnologie all'avanguardia, capaci – per parafrasare le parole di Salvatore Ottolenghi – di decifrare quel complesso e sfuggente alfabeto con cui sono scritti i tratti del «volto umano»[34].

Effettivamente, non si può negare che le potenzialità dischiuse dall'utilizzo degli *AFRS* in ambito penale siano davvero notevoli.

Il pregio maggiore di simili mezzi sta nella loro velocità: essi sono in grado di ridurre, in modo esponenziale, i tempi di lavoro degli operatori, mettendoli nelle condizioni di raffrontare, in pochi secondi, il *template* elaborato dall'algoritmo con le foto anche di milioni di soggetti schedati e di verificare così un'eventuale corrispondenza. Si ha così un salto di qualità epocale rispetto solo a pochi anni fa, allorquando la ricerca informatizzata «imponeva che i connotati identificativi del soggetto, dati anagrafici e/o tratti somatici […] fossero indicati in forma descrittiva ed

[31] Si veda, in proposito, E. Masini, *Sacro arsenale ovvero Prattica dell'officio della Santa Inquisizione, Seconda Parte, Del modo di formare i processi, e essaminare Testimoni, e Rei*, Bologna, 1665, p. 51.

[32] V. al riguardo L. Garlati, *op. cit*., pp. 894 s.

[33] Cfr. A. Bertillon, *Identification anthropométrique. Instructions signalétiques*, Melun, 1892, nonché Id., *La photographie judiciaire. Avec un appendice sur la classification et l'identification anthropométriques*, Parigi, 1890.

[34] S. Ottolenghi, *Il segnalamento del delinquente in servizio della polizia giudiziaria*, Palermo, 1889, p. 16.

inseriti manualmente dall'operatore nei campi presenti nelle maschere di interrogazione»[35].

Peraltro, simili algoritmi presentano anche il vantaggio di compiere analisi tecniche oramai davvero molto accurate[36]. Come si è accennato, i *tools* prendono in considerazione una nutrita serie di criteri fisionomici e metrici, dotati di portata individualizzante, essendo persino in grado di estrarre caratteristiche fisionomiche non percepibili dall'occhio umano[37]. Siamo, pertanto, di fronte ad applicativi capaci di dar vita a un'indagine assai più avanzata rispetto alle operazioni di raffronto tra fotografie e/o *frame* di video, svolte, fino a oggi, in modo per lo più intuitivo, finanche dagli stessi giudici e, nondimeno, consentite dalla giurisprudenza[38].

Com'è ovvio, i *software* di *facial recognition* hanno pure l'indiscutibile pregio di non essere soggetti all'inevitabile degradazione mnestica tipica della mente umana[39]. Mentre, infatti, il riconoscimento compiuto da una persona fisica, oltre a perdere via via la propria efficacia dimostrativa con lo sfumare nel tempo dei ricordi, rappresenta anche un'attività psicologicamente irripetibile[40], le macchine, una volta registrata in modo adeguato l'immagine di un volto, sono – salvo perdite di dati o bachi del sistema – in grado di riprodurla e di analizzarla un numero indefinito di volte.

Non va neppure sottaciuto che i meccanismi di *face detection* rientrano indubbiamente tra le tecniche biometriche che meglio si adattano alle

---

[35] La citazione è tratta da R. Lopez, *La rappresentazione facciale*, cit., p. 243.

[36] Cfr., al riguardo, W. Crumpler, *How Accurate are Facial Recognition Systems – and Why Does It Matter?*, in *www.csis.org*, 14 aprile 2020, il quale afferma che «*Facial recognition has improved dramatically in only a few years. As of April 2020, the best face identification algorithm has an error rate of just 0.08% compared to 4.1% for the leading algorithm in 2014*».

[37] Cfr. N. Balossino, S. Siracusa, *L'identificazione basata sul volto: metodi fisionomici e metrici*, in *Security Forum*, Bergamo, 2004, reperibile in *www.docplayer.it*, p. 3.

[38] V., ad esempio, Cass. pen., sez. II, 2 ottobre 2009, n. 40731, in *DeJure*.

[39] Sulla quale cfr. A. Bernasconi, *La ricognizione di persone nel processo penale. Struttura e procedimento probatorio*, Torino, 2003, pp. 35 ss.

[40] Sulle problematiche psicologiche legate all'attività ricognitiva, cfr., per tutti, A. Bernasconi, *op. cit.*, pp. 8 ss.; A.M. Capitta, *Ricognizioni e individuazioni di persone nel diritto delle prove penali*, Milano, 2001, pp. 1 ss.; S. Cavini, *Le ricognizioni e i confronti*, Milano, 2015, pp. 1 ss.

moderne «società dell'informazione»[41], dominate da un flusso vorticoso di immagini virtuali, scattate, riprese e pubblicate continuamente da ognuno di noi. È fin troppo ovvio osservare come, oggigiorno, i volti, su cui applicare i *tools*, sono assai facilmente reperibili[42], potendosi sfruttare per ottenerli fonti estremamente ramificate e potenti, come la fitta rete di telecamere (fisse e mobili), dislocate nelle città, nonché quell'immensa mole di dati contenuta nei *device* tecnologici, oppure pubblicata su *internet*. In tale quadro, si può ben dire che «*today's selfie is tomorrow biometric profile*»[43]; scattare una foto significa, in altri termini, lasciare una traccia elettronica (difficilmente eliminabile) di sé nell'«infosfera»[44], passibile, in seguito, di raccolta e di profilazione, pure nell'ambito di un'indagine su di un fatto di reato.

Infine, va messo in rilievo che i sistemi di riconoscimento facciale hanno pure il vantaggio di prestarsi a una pluralità di impieghi procedimentali assai eterogenei. Simili tecnologie possono essere applicate, tanto per finalità di stretta identificazione (cioè per verificare la corrispondenza tra identità fisica e identità anagrafica di una persona[45]), quanto per riscostruire l'attività criminosa. Il fatto che un *software* riconosca il volto di una persona su una scena del crimine può, evidentemente, rappresentare un'informazione preziosa, sia per orientare le indagini, sia in chiave probatoria.

Né vanno sottovalutati i particolari vantaggi per la sicurezza, che possono conseguire dall'impiego *real-time* dei *software*: in questa modalità, essi permettono di monitorare, in modo penetrante, determinate "zone

---

[41] Cfr. L. Floridi, *La rivoluzione dell'informazione*, Torino, 2012, p. 3.

[42] Lo osservano, giustamente, G. Mobilio, *op. cit*., p. 11 e S. Quattrocolo, *op. ult. cit*., p. 66.

[43] Il riferimento va all'omonima opera d'arte del 2016 di A. Hervey.

[44] La terminologia è di L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017.

[45] Sull'istituto dell'"identificazione" in senso stretto, regolato a livello interno dall'art. 349 c.p.p., cfr., per tutti, D. Curtotti, *Rilievi ed accertamenti tecnici*, Padova, 2013, pp. 108 ss., la quale ricorda che lo scopo dello stesso non è l'individuazione del colpevole, ma del nome di un indagato di cui non si conoscano le generalità. Per quanto qui rileva, va osservato come l'impiego per fini identificativi di strumenti di riconoscimento facciale risulta particolarmente utile laddove la persona nei cui confronti si procede adotti lo stratagemma di provocarsi un'abrasione delle impronte digitali, onde impedire l'utilizzo delle classiche tecniche dattiloscopiche.

sensibili" (come aeroporti, confini, oppure luoghi in cui si svolgono manifestazioni), verificando la presenza di individui oggetto di ricerca (siano essi sospettati di un reato, condannati o anche vittime).

Quanto appena affermato non deve, tuttavia, far pensare che tali *device* siano utili solo per finalità repressive o per la ricerca di persone scomparse/rapite. Se è pur vero, infatti, che gli applicativi di *face detection* sono stati finora impiegati soprattutto dalle autorità di *law enforcement*, è indubbio che potrebbero idealmente giovare anche alle difese, laddove potessero avvalersene[46]. Un'esigenza di questo tipo potrebbe, ad esempio, verificarsi nei casi in cui l'algoritmo servisse per avvalorare una prova d'alibi (si pensi all'ipotesi in cui il sospettato fosse ripreso *aliunde* nell'ora di commissione di un reato), oppure comunque per argomentare la tesi dell'estraneità dell'indagato/imputato dall'illecito (ciò potrebbe accadere laddove la macchina non riconoscesse il volto della persona tra quelli presenti sulla scena del crimine). Sulla scorta di queste considerazioni, ben si comprenderà come, onde evitare il determinarsi di uno scottante problema di parità delle armi[47], risulti importante che, allorquando un ordinamento penale decida di dotarsi di siffatti meccanismi, ne consenta poi l'accesso anche ai prevenuti, che lo richiedano per finalità difensive[48].

3. Il "volto oscuro" dei sistemi automatici di riconoscimento facciale

Già quanto osservato da ultimo farà intuire come gli *AFRS* non pre-

[46] Cfr. G. Lasagni, G. Contissa, *Making Criminal Procedure Rights Computable*, in Contissa, G. Lasagni, M. Caianiello, G. Sartor (a cura di), *Effective Protection of the Rights of the Accused in the EU Directives. A Computable Approach to Criminal Procedure Law*, Leiden-Boston, 2022, p. 43, nt. 6. Al riguardo, v. anche *infra*, cap. II, spec. § 2.

[47] Sui problemi rispetto alla parità delle armi, suscitati dagli strumenti computazionali, cfr., per tutti, S. Quattrocolo, *Equità del processo penale e* automated evidence *alla luce della Convenzione europea dei diritti dell'uomo, in Revista ítalo-española de Derecho Procesal,* 2019, n. 2, pp. 118 ss.

[48] Ciò potrebbe, ad esempio, avvenire consentendo alle difese di avvalersi, a richiesta, dell'applicativo in dotazione dell'Autorità; oppure anche di *tools* diversi, la cui affidabilità sia stata pubblicamente certificata.

sentino solo vantaggi, ma anche molteplici rischi, messi in rilievo da tempo dalla dottrina straniera[49] e italiana[50].

Il primo e principale pericolo è legato alla loro fallibilità: sebbene, come accennato, i *software* più moderni garantiscano, in condizioni ideali, un livello di *performance* assai elevato[51], va posto in rilievo che, nell'applicazione pratica, essi possono essere indotti in errore da molteplici fattori[52], tanto esogeni (quali, ad esempio, la scarsa qualità delle immagini, oppure la tipologia di luce), quanto endogeni (come, ad esempio, un non adeguato "allenamento" dell'algoritmo da parte degli sviluppatori).

Esistono, del resto, oramai molteplici riprove di come i sistemi in esame, fornendo risultati di matrice soltanto statistico-probabilistica, non siano affatto sempre efficaci. In proposito, basti pensare all'esperienza della finale di UEFA *Champions League* di Cardiff del 2017, nel corso della quale oltre 2.000 persone innocenti sono state identificate quali possibili criminali da un *tool* di *facial recognition*[53]. Ma le cose non sono andate meglio negli USA, dove le cronache hanno già registrato molteplici casi di persone arrestate ingiustamente, a causa di *alert* degli *AFRS*, non controllati in modo adeguato dagli operatori "umani"[54]. Quanto appena affermato rende evidente come gli strumenti in esame, laddove non siano maneggiati con cautela, possano trasformarsi in macchine idonee a

[49] Pare utile precisare che il tema dei "lati oscuri" delle tecnologie di *facial recognition* è dibattuto da decenni soprattutto nei Paesi di *common law*, dove le stesse sono da più tempo radicate. Per i dovuti riferimenti dottrinali in proposito, si consenta il rinvio a J. Della Torre, *op. cit*., p. 233, nt. 10.

[50] Si veda, ad esempio, il pioneristico studio di G. Di Paolo, *op. cit.*, nonché, più di recente, G. Mobilio, *op. cit.*, pp. 57 ss.

[51] Cfr. W. Crumpler, *op. cit*.

[52] Secondo quanto riportato da W. Crumpler, *op. cit.*, «*the error rate for one leading algorithm climbed from 0.1% when matching against high-quality mugshots to 9.3% when matching instead to pictures of individuals captured "in the wild"*».

[53] In proposito, v. BBC, *2,000 wrongly matched with possible criminals at Champions League*, in *www.bbc.com*, 4 maggio 2018.

[54] Cfr. D. Harwell, *Wrongfully arrested man sues Detroit police over false facial recognition match*, in *www.washingtonpost.com*, 13 aprile 2021; K. Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, in *www.nytimes.com*, 6 gennaio 2021.

favorire il verificarsi di *miscarriages of justice*[55], ovvero l'esito peggiore per ogni sistema di giustizia penale.

A tali considerazioni di fondo, deve aggiungersi che i *facial recognition systems* sono affetti, tanto da molteplici problematiche "traversali", che caratterizzano le eterogenee forme di IA impiegate in campo giuridico, quanto da una serie di criticità peculiari, legate al loro funzionamento specifico.

Dalla prima prospettiva, si consideri, ad esempio, il fatto che pure i *software* di riconoscimento facciale, così come altre forme di IA, sono una potenziale "*black box*"[56], ovvero «sistemi in cui *input* e *output* sono osservabili, mentre il funzionamento interno [del sistema] rimane oscuro persino ai suoi stessi programmatori»[57]; con tutto ciò che ne consegue in termini di contrasto con pilastri del *fair trial*, nelle sue articolazioni del contraddittorio e della parità delle armi[58]. È, infatti, evidente che solo conoscendo i processi di funzionamento di un determinato *tool* sarà poi possibile controllarne in modo effettivo il risultato. Per non dire poi che i requisiti dell'*intepretability*[59] e della *transparency* dell'algoritmo[60] sono essenziali anche per il giudice, onde poter, da un lato, valutarne l'idoneità dei risultati ad assicurare l'accertamento dei fatti e, da un altro lato, motivare *ex post* razionalmente la propria decisione basata sull'IA.

---

[55] Al riguardo, J. Robins, *Former regulator warns of miscarriages of justice as a result of poor quality CCTV facial comparisons*, in *www.thejusticegap.com*, 10 febbraio 2022.

[56] Sul punto, v. A. Adensamer, L.D. Klausner, "*Part Man, Part Machine, All Cop": Automation in Policing*, in *Frontiers in Artificial Intelligence*, 23 giugno 2021, p. 4.

[57] La citazione è tratta da 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, n. 4, p. 620.

[58] In proposito, v. S. Quattrocolo, *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *Media Laws – Rivista di diritto dei Media*, 2020, n. 3, p. 127.

[59] Come ricordato da E. Sacchetto, *op. ult. cit*., p. 11, nt. 52 «l'interpretabilità è la qualità di un sistema di intelligenza artificiale avente ad oggetto la capacità di comprendere quali modelli vengono utilizzati per effettuare (nel caso della disciplina biometrica) identificazioni o riconoscimenti tra i soggetti».

[60] Non a caso, tale canone è ritenuto uno dei principi essenziali per l'utilizzo equo degli algoritmi in campo giuridico: cfr., per tutti, C. Blacklaws, *Algorithms: transparency and accountability*, in *Philosophical Transactions of the Royal Society*, 2018, pp. 1 ss.; U. Pagallo, *Algoritmi e conoscibilità*, in *Rivista di filosofia del diritto*, 2020, n. 1, pp. 93 ss.

Allo stesso tempo, molteplici ricerche hanno denunciato pure gli effetti potenzialmente discriminatori determinati da tali tecnologie[61]. A quest'ultimo riguardo, vale la pena di menzionare uno studio del *National Institute of Standards and Technology* degli Stati Uniti, che ha dimostrato come molti algoritmi di riconoscimento facciale finiscano per causare una quantità più elevata di errori nei confronti delle persone afro-americane (specie se donne) e asiatiche rispetto ai caucasici[62].

Un tanto ci permette di osservare come anche queste macchine corrano il rischio di veder ridotta la loro affidabilità dalla presenza di *bias* cognitivi, i quali sono spesso favoriti da una non sufficiente attenzione prestata dagli sviluppatori per la qualità dei dati che le alimentano[63]. Vi è, in altre parole, sempre il pericolo che i creatori degli algoritmi, non selezionando in modo sufficientemente attento i volti con cui "allenare" gli applicativi, finiscano per "trasmettere" al sistema pregiudizi umani, determinando così quell'esiziale fenomeno del "*garbage in*" e "*garbage out*", oramai ben noto alla letteratura sul tema[64].

Quanto ai pericoli "specifici", causati dal funzionamento dei mezzi in esame, va segnalata, in prima battuta, l'interferenza notevole che essi determinano nei confronti del diritto alla *privacy*[65], nella sua duplice

---

[61] Cfr. A. Najibi, *Racial Discrimination in Face Recognition Technology*, in *www.sitn.hms.harvard.edu*, 24 ottobre 2020; R.A. Waelen, *The struggle for recognition in the age of facial recognition technology*, in *AI and Ethics*, 2022, p. 4.

[62] Ci si riferisce allo studio del dicembre del 2019 di P. Grother, M. Ngan, K. Hanaoka, *Face Recognition Vendor Test (FVRT). Part 3: Demographic Effects*, in *www.nvlpubs.nist.gov*.

[63] S. Quattrocolo, *op. ult.cit.*, p. 67.

[64] Cfr. C. Garvie, *Garbage in, garbage out. Face recognition on flawed data*, in *www.flawedfacedata.com*, 16 maggio 2019.

[65] Siffatta interferenza è stata riconosciuta, in modo espresso, da C. edu, 11 giugno 2020, *P.N. c. Germania*, § 56 e da C. edu, 13 febbraio 2020, *Gaughran v. Regno Unito*, §§ 65-70. Nello stesso senso, v. anche, *ex multis*: a) le *Guidelines on facial recognition* del *Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data*, giugno 2021, p. 5; b) il *report* del 13 settembre 2021 dell'Alto rappresentante ONU per i Diritti umani, A/HRC/48/31, § 27; c) la risoluzione sull'utilizzo del riconoscimento facciale, approvata nell'ottobre 2020, dalla *Global Privacy Assembly*, in *www.edps.europa.eu*; d) il libro bianco della Commissione europea, *sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*, COM (2020) 65, 19 febbraio 2020, p. 24, nt., 57; e) il documento dell'Agenzia UE per i diritti fondamentali (d'ora in avanti *FRA*), *Facial recognition technology: fundamental rights*

declinazione di diritto «al rispetto della vita privata» e alla «protezione dei dati personali», il quale – com'è ben noto – è oramai disciplinato da un cospicuo reticolo di fonti interne ed europee[66], tra cui spiccano, oltre all'art. 8 CEDU, gli artt. 7 e 8 della Carta di Nizza.

Ciò si deve, in prima battuta, al fatto che tali tecnologie operano, come si è visto, estraendo, in modo coattivo, le "impronte facciali", ovvero dati biometrici che, in ossequio all'art. 10 della direttiva 2016/680/UE, in materia di trattamenti di dati compiuti dalle autorità di *law enforcement*[67], sono particolarmente sensibili, in quanto idonei a identificare in modo univoco un individuo[68]. Il che fa comprendere come gli *AFRS* impattino, allo stesso tempo, sia sul diritto all'"identità personale"[69], sia sul cosiddetto *habeas data*[70] – da intendersi come prerogativa dell'individuo di mantenere il controllo sulle informazioni concernenti il proprio corpo *virtuale* e di opporsi alle interferenze altrui sulle stesse – elaborato dalla migliore dottrina[71], in chiave evolutiva, dal canone tradizionale dell'*habeas corpus*[72].

---

considerations in the context of law enforcement, in *www.fra.europa.eu,* 21 novembre 2019, p. 23; f) l'articolo dell'*European Data Protection Supervisor*, *Facial recognition: A solution in search of a problem?*, in *www.edps.europa.eu*, 28 ottobre 2019.

[66] Per una sintesi, v. l'analisi, in chiave penalistica, di L. Lupária, Privacy, *diritti della persona e processo penale*, in *Riv. dir. process.*, 2019, pp. 1448 ss.

[67] Sulla quale, cfr. S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, pp. 87 ss.

[68] Non a caso la Corte europea dei diritti dell'uomo ha, per parte sua, affermato che l'immagine di un soggetto «*constitutes one of the chief attributes of his or her personality, as it reveals the per-son's unique characteristics and distinguishes the person from his or her peers*». Cfr. *ex multis*, C. edu, GC, 17 ottobre 2019, *López Ribalda e altri c. Spagna*, § 89. Sul versante eurounitario, v. CGUE, Sez. IV, 17 ottobre 2013, C-291/12, *Micheal Schwarz,* § 48, dove i giudici di Lussemburgo hanno riconosciuto che la raccolta dell'immagine facciale può provocare imbarazzo fisico o psichico.

[69] Sul quale cfr., per tutti, G. Pino, *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Bologna, 2003.

[70] Cfr. M. Gialuz, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in *Giurisdizione penale*, cit., pp. 58 e 64.

[71] Com'è noto, uno dei principali sostenitori del canone dell'*habeas data* è S. Rodotà, del quale si veda, il volume *Il mondo nella rete. Quali i dritti, quali i vincoli*, Roma, 2014, *passim*. Nel dibattito processualpenalistico, cfr., in proposito, B. Galgani, *Giudizio penale,* habeas data *e garanzie fondamentali*, in *Archivio penale – Rivista web*, 2019, n. 1 e L. Lupária, *op. cit*., pp. 1464 s.

[72] In questo senso, si riesce a cogliere, sul piano interno, «uno stretto collegamento

Ma la circostanza per cui gli algoritmi di riconoscimento facciale sono delle «idrovore di dati»[73] estremamente potenti prova come esse determinino rischi ancora più gravi, potendosi trasformare persino in esiziali strumenti di «sorveglianza di massa»[74]. Difatti, applicando un *tool* di riconoscimento facciale *ex post* o *live* alla rete di telecamere (fisse e mobili), collocate in ogni angolo delle nostre città, e/o alle immagini reperibili sul *web*, diventa possibile controllare, in modo capillare, la nostra vita privata[75]. Né – è bene precisarlo – si deve ritenere che un pericolo di questo tipo valga unicamente per Stati autoritari: il recente scandalo "*Clearview*"[76], che ha travolto gli Stati Uniti e l'Europa, dimostra, del resto, quanto, anche nelle democrazie occidentali, il rischio del verificarsi di scenari orwelliani sia oltremodo concreto[77].

---

tra il "diritto alla riservatezza" riconducibile all'art. 2 Cost., con l'art. 3 Cost., quale fonte di tutela della dignità sociale, nonché con l'art. 13 Cost.» (cfr. L. Parlato, *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale*, in *Processo penale e giustizia*, 2020, p. 298).

[73] Si riprende qui l'immagine dei mezzi tecnologici come "idrovore", utilizzata, con riguardo alle intercettazioni, da G. Giostra, *I mali della libertà di stampa si curano solo con più libertà*, in *DDl Alfano: se lo conosci lo eviti*, Roma, 2009, p. 102.

[74] V., in proposito, la già citata risoluzione sulla tecnologia di riconoscimento facciale, adottata nell'ottobre 2020, dalla *Global Privacy Assembly*, nonché il nutrito gruppo di atti e di documenti ufficiali pubblicati da *EDRi*, *Facial Recognition & Biometric Mass Surveillance: Document Pool*, in *www.edri.org*, 5 luglio 2021. Nella letteratura italiana, il pericolo che le tecnologie in esame finiscano per trasformarsi in "mezzi di controllo di massa" era già stato lucidamente segnalato da G. Di Paolo, *op. cit.*, p. 5. Più di recente, v. A. Pin, "*A novel and controversial technology". Artificial face recognition, privacy protection and algorithm bias in Europe,* in *William & Mary Bill of Rights Journal*, 2021, p. 293.

[75] Come ricorda G. Di Paolo, *op. cit*., p. 146, il monitoraggio sistematico tramite immagini rappresenta «l'equivalente di migliaia di poliziotti intenti a spiare le persone in ogni singolo attimo della loro vita quotidiana, anche mentre si spostano per fare la spesa o andare al ristorante».

[76] Denunciato da K. Hill, *The Secretive Company That Might End Privacy as We Know It*, in *www.nytimes.com*, 18 gennaio 2020.

[77] Il riferimento corre a quell'applicazione di riconoscimento facciale – creata dall'azienda nord-americana Clearview e impiegata, almeno per un periodo, anche da forze dell'ordine europee – che utilizza quale *database* di partenza un'immensa mole di oltre 10 miliardi di immagini di volti di persone di svariati Paesi, tratti, senza il consenso degli interessati, da *social-networks* e dal *web*. In argomento, cfr. I. Neroni Rezende, *Facial recognition in police hands: Assessing the "Clearview case" from a European*

Va ancora ricordato che le macchine in esame sono tra quelle in grado di provocare un più marcato "effetto inibitore" (o "*chilling effect*") sulla vita delle persone[78]. Con tale locuzione si fa riferimento al pericolo che gli individui, proprio per timore di essere soggetti al trattamento biometrico dei *tools*, modifichino le proprie abitudini, finendo per autolimitarsi nell'esercizio di loro diritti fondamentali, come quello all'associazione o alla libera manifestazione del pensiero[79].

Ed è anche la presenza di tale criticità ad aver portato ad affermare che i *software* di riconoscimento sarebbero, in determinati casi, in grado di incidere negativamente pure sulla libertà morale (o di autodeterminazione) della persona[80], ovvero una garanzia che, secondo una linea di pensiero oramai sempre più radicata, andrebbe, a sua volta, ricondotta nella sfera protettiva dell'art. 13 Cost.[81]. Una tesi di questo tipo ci pare

---

perspective, in *New Journal of European Criminal Law*, 2020, n. 3, pp. 375 ss. Alla luce di un'invasione così marcata nella sfera di riservatezza dei singoli, non stupisce se le autorità garanti della *privacy* di vari Stati – tra cui l'Italia (cfr. Garante della privacy, *Riconoscimento facciale: il Garante privacy sanziona Clearview per 20 milioni di euro. Vietato l'uso dei dati biometrici e il monitoraggio degli italiani*, in *www.garanteprivacy.it*, 9 marzo 2022) – siano corse ai ripari, condannando Clearview a pagare ingenti somme di denaro.

[78] Cfr., in questo senso, le conclusioni della presidenza del Consiglio UE, doc. Consiglio UE n. 11481/20, 21 ottobre 2020, § 18. Nonché, *amplius*, la ricerca di *FRA*, *Facial recognition technology*, cit., pp. 4 e 30. In dottrina, v. G. Di Paolo, *op. cit*., p. 147 e G. Mobilio, *op. cit.*, p. 59.

[79] V., ancora, *FRA*, *Facial recognition technology*, cit., pp. 29 s. Nella dottrina nordamericana si è sviluppata da tempo l'idea per cui anche nei luoghi pubblici gli individui godrebbero di un diritto, di rango costituzionale, "*all'anonimato*", funzionale proprio alla tutela di libertà fondamentali come quella di parola: cfr., al riguardo, C. Slogobin, *Public privacy: camera surveillance of public places and the right to anonymity*, in *Mississippi Law Journal*, 2002, pp. 237 ss. Nella dottrina italiana, v., in proposito, G. Di Paolo, *op. cit*., pp. 17 e 149 ss.

[80] In questo senso v. M. Gialuz, *op. ult. cit*., p. 64, nonché, in precedenza, G. Di Paolo, *op. cit*., p. 146, la quale afferma che «il monitoraggio generalizzato e continuo degli individui esercita […] sulla psiche umana una sottile forma di coercizione, che va ad incidere negativamente […] sulle libertà fondamentali».

[81] Al riguardo v. la recente analisi – riferita proprio alle tecnologie digitali del controllo – di L. Parlato, *op. cit*., pp. 297 s. Nello stesso senso, v. anche, tra i molti, T. Alesci, *Corpo dell'imputato (fonte di prova nel processo penale)*, in *Digesto Pen. – Agg*., X, Torino, 2018, p. 78; P. Barile, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984, p. 112; C. Fanuele, *La libertà personale*, in F.R. Dinacci (a cura di), *Processo penale e Costituzione*,

condivisibile, perlomeno nel caso in cui i *tools* vengano applicati per finalità investigative e/o probatorie: in tale evenienza, infatti, l'impiego coattivo della tecnologia in esame sembra in grado di provocare un'ingerenza di tale entità su una porzione del corpo "virtuale" della persona da determinare un suo *assoggettamento totale al potere dell'autorità*, concretizzandosi così una delle (rare) ipotesi in cui lo stesso giudice delle leggi ha ammesso, sin dagli anni Cinquanta[82], che anche atti non fisicamente coercitivi siano idonei a limitare la libertà personale[83].

Milano, 2010, pp. 213 s.; P. Felicioni, *Il riconoscimento del parlante tra prassi e modelli normativi*, in A. Scalfati (a cura di), *Le indagini atipiche*, cit., p. 282; P.F. Grossi, *Libertà personale, libertà di circolazione ed obbligo di residenza dell'imprenditore fallito*, in *Giur. cost*., 1962, p. 205; F. Modugno, *I nuovi diritti nella giurisprudenza costituzionale*, Torino, 1995, pp. 11 ss.; R. Nania, *Appunti per un bilancio sulla libertà individuale nella esperienza costituzionale italiana*, in R. Nania (a cura di), *L'evoluzione costituzionale delle libertà e dei diritti fondamentali. Saggi e casi di studio*, Torino, 2012, pp. 6 s.

[82] Si allude a C. cost., 3 luglio 1956, n. 11, in *www.cortecostituzionale.it* sull'istituto dell'ammonizione. In seguito, v. anche C. cost., 31 maggio 1995, n. 210, *ivi*, C. cost., 24 novembre 1994, n. 419, *ivi*; C. cost., 30 giugno 1964, n. 68, *ivi*.

[83] Tale conclusione non pare smentita da una sentenza, in cui la Corte ha negato che i rilievi segnaletici "extracorporei", compiuti *ex* art. 4 t.u.l.p.s., siano idonei a limitare la libertà personale (cfr. C. cost., 27 marzo 1962, n. 30, in *www.cortecostituzionale.it*). Al riguardo, preme osservare come siffatta pronuncia non sembri conferente nel caso di specie, non solo perché i moderni *tools* di riconoscimento facciale sono in grado di estrarre da un'immagine un vero e proprio campione virtuale del corpo (l'"impronta facciale"), che, in quanto composto anche da dettagli non percepibili dall'essere umano, contiene informazioni intime e affatto esternalizzate al pubblico, ma soprattutto dal momento che il giudizio della Consulta ha avuto a oggetto l'istituto dei rilievi "identificativi" di sicurezza e non atti strettamente "investigativi" o "probatori". A quest'ultimo riguardo, non sfuggirà, del resto, come esista una notevole differenza di grado tra gli effetti negativi sull'individuo determinati dall'uso coattivo di un algoritmo per fini di identificazione o per obiettivi di ricostruzione dell'illecito: mentre nella prima ipotesi il mezzo serve solo per verificare le generalità di un soggetto (avendo, in ultima analisi, anche lo scopo, a lui favorevole, di evitare errori di persona), nel secondo esso viene usato per attività, a lui di certo avverse, quali l'esercizio dell'azione o anche la dimostrazione della sua responsabilità penale. Un tanto porta a dire che, quand'anche ci si potesse accontentare di ricomprendere le forme di applicazione coattiva di un *AFRS*, idonee a incidere in modo meno marcato nella sfera giuridica del singolo (come proprio quelle compiute per finalità identificative), tra i meri "obblighi personali", di cui all'art. 23 Cost. (cfr., al riguardo, G. Mobilio, *op. cit.*, p. 84), le cose stanno diversamente nel caso ci si avvalga dello strumento per obiettivi investigativi e/o probatori: in tale fattispecie la tecnologia pare determinare un sacrificio di tale entità di una parte del proprio corpo virtuale da ricadere nella sfera di

A "coronare" queste problematiche sta la circostanza per cui, secondo un'opinione diffusa, gli algoritmi di *face detection* metterebbero in pericolo pure il principio "super-primario" della dignità umana"[84]. Tale rischio pare essere particolarmente intenso laddove essi vengano impiegati quali mezzi di *sentiment analysis*[85]: il fatto di sottoporre l'individuo a un controllo tanto incisivo delle sue espressioni facciali, finalizzato a scandagliarne le emozioni interne, potrebbe, invero, indurlo a sentirsi «*in a weak and potentially humiliating position*»[86], in spregio al perno dei valori fondanti dei moderni Stati di diritto[87].

4. Segue: *la reazione internazionale ai pericoli determinati dalle "tecnologie del controllo"*

I rilievi appena svolti fanno ben intuire il perché abbia preso piede un ampio ed eterogeneo movimento di pensiero, teso a frenare l'avanzata delle "tecnologie del controllo" in ambito penale[88].

---

tutela dell'art. 13 Cost. Nondimeno, non va sottaciuto il rischio che l'accertamento originariamente connotato da semplici esigenze identificative finisca poi per essere immesso nel circuito delle indagini. Si tratta, evidentemente, di un'«esondazione teleologica» (per riprendere le parole di D. Curtotti, *op. cit*., p. 110) da evitare, pena altrimenti il sorgere di ulteriori dubbi di legittimità costituzionale nei confronti dell'art. 349 c.p.p., vista la mancata fissazione da parte dello stesso di presupposti adeguati a soddisfare i parametri di cui all'art. 13 Cost. (cfr., per una sintesi delle criticità costituzionali che classicamente affliggono la regola *de qua*, v. T. Alesci, *op. cit.,* pp. 81 s.).

[84] In questi termini, v. il libro bianco della Commissione europea, *sull'intelligenza artificiale*, cit., p. 24, nt., 57, nonché la ricerca di *FRA*, *Facial recognition technology*, cit., p. 20 e le *Guidelines on facial recognition* del *Consultative Committee* della cd. "Convenzione 108", cit. p. 8.

[85] Sui rischi per la dignità umana determinati dai *tools* di indagine delle emozioni, cfr. P. Valcke, D. Clifford, V.K. Dessers, *Constitutional Challenges in the Emotional AI Era*, in H.-W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, G. De Gregorio (a cura di), *op. cit*., p. 67 s.

[86] La citazione è tratta da *FRA*, *Facial recognition technology*, cit., p. 20.

[87] Come osservava F. Cordero, *Procedura penale*, Milano, 1987, p. 472, «per nostra fortuna l'imputato è ancora considerato una persona e, quindi, gli compete il diritto all'inviolabilità dell'anima; appena questo privilegio cadesse, dovremmo rassegnarci a una condizione subumana».

[88] Per un quadro di sintesi, cfr. *EPRS*, *Regulating facial recognition*, cit., pp. 29 s. In

In quest'ottica si sono mosse, anzitutto, una serie di istituzioni europee che, pur non ritenendo necessario bloccare del tutto le porte agli strumenti di identificazione biometrica, in generale, e al *facial recognition*, in particolare, hanno espresso l'opinione per cui, onde poterli utilizzare, sarebbe indispensabile dettare salvaguardie minime *ad hoc* contro il rischio di compressione dei diritti fondamentali dell'individuo[89].

Un'opinione di questo tipo è stata, ad esempio, espressa dalla Commissione europea. All'interno della già richiamata proposta di regolamento UE sull'IA, essa ha stabilito un (discusso) divieto generale di avvalersi per finalità di *law enforcement* di sistemi di analisi biometrica *in tempo reale*, derogabile solo a fronte di determinati requisiti[90]. Nello specifico, all'art. 5 dell'iniziativa si è, non solo previsto che siffatti strumenti possano essere applicati soltanto in una serie ristretta di casi[91], ma anche che ogni utilizzo degli stessi debba essere autorizzato *ex ante* (o, in casi di urgenza, convalidato *ex post*) da parte di un giudice o di un'autorità amministrativa indipendente[92].

---

merito alle problematiche costituzionali sorte "nell'era dei controlli", oltre al già citato volume di G. Di Paolo (*supra* nt. 29), v. il recente studio di F. Nicolicchia, *I controlli occulti e continuativi come categoria probatoria*, Milano, 2020, pp. 39 ss.

[89] Cfr., in questo senso, oltre ai testi citati di seguito, la risoluzione 2342 (2020) dell'Assemblea parlamentare del Consiglio d'Europa.

[90] In argomento, v. G. Borgia, *op. cit*., p. 20.

[91] Più nello specifico, si prevede che tali tecnologie possano essere impiegate laddove sia strettamente necessario per: a) individuare vittime di reato; b) prevenire un'imminente minaccia alla vita o all'incolumità fisica degli individui o un attacco terroristico; c) individuare, localizzare o esercitare l'azione penale nei confronti delle persone sospettate di uno dei reati di cui all'art. 2, par. 2, della d.q. 2002/584/GAI, a patto che essi siano punibili nello Stato membro interessato con una pena della durata massima di almeno tre anni.

[92] Vale la pena di precisare che tale proposta è stata ritenuta troppo poco garantista, a fronte dei rischi determinati dagli strumenti di sorveglianza di massa, tanto da parte di un gruppo di parlamentari europei (cfr. *MEPs' Letter to the European Commission*, *www.patrich-breyer.de*, 15 aprile 2021), quanto da parte dalle autorità garanti della *privacy* UE (cfr. oltre al documento dell'*European Data Protection Supervisor* e dell'*European Data Protection Board*, *Joint Opinion* 5/2021, del 18 aprile 2021, il comunicato stampa dell'*European Data Protection Supervisor*, *Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary*, in *www.edps.europa.eu*, 23 aprile 2021). Anche un gruppo di oltre 60 associazioni per i diritti umani (la *Reclaim Your Face advocacy coalition*) ha sollevato numerose obiezioni in

Una prospettiva analoga è stata espressa anche da altri organi – come l'Agenzia europea per i diritti fondamentali[93] e *l'European Parliamentery Research Service* – i quali hanno, più in generale, insistito sulla necessità di compiere un rigido vaglio di proporzionalità[94], in astratto e in concreto, per ogni possibile impiego – *ex post* o *live* – di sistemi di *facial recognition*. Queste iniziative testimoniano come il riconoscimento facciale automatico sia ritenuto in grado di determinare, in certi casi, un'intrusione significativa nel diritto alla *privacy*[95], che, in quanto tale, stando all'insegnamento della Corte di giustizia UE, deve essere, da un lato, circoscritta soltanto alla sfera di criminalità più grave e, da un altro lato, accompagnata dall'autorizzazione di un giudice o di un'entità amministrativa indipendente[96].

Vista la posta in gioco, non stupisce che pure la Corte di Strasburgo abbia, per parte sua, già fissato alcuni paletti specifici in tema di *data retention* delle immagini facciali. Nella loro giurisprudenza, oltre ad aver

---

proposito, tra cui quella per cui la proposta presenterebbe il difetto di occuparsi soltanto dei sistemi *live* di identificazione biometrica, ma non di quelli che operano *ex post*: cfr. *European Commission proposal for new AI Regulation shows exaclty why we are fighting to ban BMS*, in *www.reclaimyorface.eu*, 21 aprile 2021.

[93] Cfr. *FRA*, *Facial recognition technology*, cit., pp. 20 s.

[94] In merito a tale canone cfr., tra gli altri, D. Negri, *Compressione dei diritti di libertà e principio di proporzionalità*, in *Diritti della persona e nuove sfide del processo penale*, Milano, 2019, pp. 55 ss.; F. Nicolicchia, *op. cit.,* pp. 57 ss.; S. Signorato, *op. ult. cit.*, pp. 262 ss.

[95] Tale considerazione pare tanto più fondata, una volta osservato che il riconoscimento del volto di un individuo costituisce un'informazione di partenza da cui è spesso possibile acquisire dati ulteriori di natura privata di cruciale importanza, tra cui, *in primis*, il luogo in cui egli si trova (v. *FRA*, *Facial recognition technology*, cit., p. 8).

[96] Ci si riferisce, in particolare, alle numerose pronunce della Corte di giustizia in materia di tabulati. Si vedano, tra le molte, CGUE, GS, 5 aprile 2022, C-140/20, *G.D.*, §§ 59 e 106; CGUE, GS, 2 marzo 2021, C-746/18, *H.K*, §§ 33 e 53; CGUE, GS, 6 ottobre 2020, C-511/18, *La Quadrature du Net*, § 139; CGUE, GS, 21 dicembre 2016, C-2013/15, *Tele2 Sverige AB*, conclusione n. 2; CGUE, GS, 8 aprile 2014, C-293/12 e C-594/12, *Digital Rights Ireland*, § 62. Per un'efficace sintesi della tematica, anche in chiave interna, v., per tutti, F.R. Dinacci, *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia: luci europee e ombre legislative*, in *Processo penale e giustizia*, 2022, n. 2, pp. 310 s.; L. Lupária, Data retention e *processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Diritto di internet*, 2019, pp. 758 ss.; T. Rafaraci, *Verso una* law of evidence *dei dati*, in *Dir. pen. proc*., 2021, pp. 853 ss.

affermato che «*the right to the protection of one's image presupposes the individual's right to control the use of that image*»[97], i giudici convenzionali hanno precisato che la conservazione della foto di un soggetto da parte delle forze di polizia, per un periodo di tempo indeterminato, «*without reference to the seriousness of the offence or the need for indefinite retention and in the absence of any real possibility of review*»[98], onde sottoporla, in seguito, a trattamenti automatici di riconoscimento facciale, viola l'art. 8 CEDU. Per contro, in un'altra occasione la Corte ha ritenuto che la custodia per cinque anni di una fotografia di un recidivo non avesse provocato una lesione delle garanzie europee, proprio perché di durata limitata e in quanto nel diritto nazionale esistevano salvaguardie procedimentali sufficienti «*against abuse (such as unauthorised access to or dissemination) of the data*»[99]. Un tanto testimonia come, anche a livello della grande Europa, il vaglio sulla stretta necessità e sulla proporzionalità dell'interferenza nella sfera privata del singolo, nonché sulle garanzie poste a protezione dei suoi diritti (quali quella di chiederne una revisione e/o cancellazione dal *database* nazionale), siano le "chiavi di volta" nella valutazione della legittimità dell'applicazione degli apparati tecnologici di controllo[100].

Sotto altro profilo, va posto in rilievo come molte istituzioni, partendo dalla convinzione per cui le tutele procedimentali sarebbero insufficienti a controbilanciare i pericoli derivanti dagli *AFRS*, abbiano adottato approcci ancora più rigidi, esortando ad approvare moratorie o divieti d'uso permanenti nei loro confronti[101].

In una prospettiva di questo tipo si è posto, ad esempio, il Parlamento

[97] Cfr. C. edu, sez. V, 11 giugno 2020, *P.N. c. Germania*, § 56.

[98] C. edu, sez. I, 13 febbraio 2020, *Gaughran c. Regno Unito*, § 96.

[99] Ci si riferisce ancora a C. edu, sez. V, 11 giugno 2020, *P.N. c. Germania*, § 74. V. in precedenza già C. edu, GC, 28 ottobre 1994, *Murray c. Regno Unito*, § 101 s.

[100] Cfr. anche la nota sentenza C. edu, GC, 25 maggio 2021, *Big Brother Watch e altri c. Regno Unito*, § 350.

[101] Ad esempio, un gruppo di oltre 100 membri del Parlamento europeo ha esortato la Commissione a vietare del tutto gli strumenti biometrici di sorveglianza di massa in spazi pubblici in Europa: cfr. *MEPs' Letter to the European Commission*, in *www.edri.org*, 8 marzo 2021. Sono innumerevoli le iniziative in proposito di associazioni a tutela dei diritti umani: cfr., ad esempio, *EDRi*, *Ban Biometric Mass Surveillance*, in *www.edri.org*, 13 maggio 2020; *Reclaimyourface*, *Letter to EU Commissioner for Justice*, in *www.reclaimyourface.eu*, 1° aprile 2021.

europeo, il quale, oltre a chiedere «una moratoria sulla diffusione dei sistemi di riconoscimento facciale per le attività di contrasto con funzione di identificazione, a meno che non siano usate strettamente ai fini dell'identificazione delle vittime di reati, finché le norme tecniche non possano essere considerate pienamente conformi con i diritti fondamentali», ha anche esortato a vietare del tutto «l'utilizzo dei sistemi di analisi e/o riconoscimento automatici negli spazi pubblici di altre caratteristiche umane quali l'andatura, le impronte digitali, il DNA, la voce e altri segnali biometrici e comportamentali»[102].

Particolarmente garantista è stata anche la posizione espressa in proposito dalle Autorità europee a tutela della *privacy*. All'interno di un'opinione congiunta sulla proposta di regolamento UE in tema di IA, l'*European Data Protection Board* e l'*European Data protection Supervisor* hanno sostenuto la necessità di adottare «a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces – such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioral signals – in any context»[103].

Sennonché, va a questo punto preso atto che i frutti concreti di questi tentativi di arginare l'avanzata dirompente delle tecnologie del controllo nei sistemi penali sono stati, finora, piuttosto modesti[104]. Nonostante tutte le esortazioni dottrinali, giurisprudenziali e politiche, esse stanno continuando a prosperare sempre più anche a livello europeo. Onde rendersi

---

[102] Cfr. *la Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale*, P9_TA (2021) 0405, rispettivamente §§ 25 e 26. Per un commento, cfr. G. Barone, *Intelligenza artificiale e processo penale: la linea dura del Parlamento europeo. Considerazioni a margine della risoluzione del Parlamento europeo del 6 ottobre 2021*, in *Cass. pen*., 2022, n. 3, pp. 1180 ss.

[103] V. *European Data Protection Supervisor* e dell'*European Data Protection Board*, *Joint Opinion* 5/2021, cit., § 32. Per di più, tali istituzioni hanno anche affermato «*that the use of AI to infer emotions of a natural person is highly undesirable and should be prohibited*» (§ 35).

[104] A riprova di ciò, si vedano le analisi di respiro europeo di *EDRi, EIJI*, *The rise and rise of biometric mass surveillance in the EU*, in *www.edri.org*, 7 luglio 2021; *Greens/EFA*, *Biometric & Behavioural Mass Surveillance,* cit. Per contro, va segnalato come negli USA un numero sempre maggiore di città e di Stati stiano approvando moratorie o divieti di impiego della tecnologia in esame: per un quadro aggiornato del fenomeno, cfr. la mappa interattiva pubblicata in *www.banfacialrecognition.com*.

conto della dimensione del fenomeno, basti, ad esempio, pensare alla circostanza per cui, da una recente ricerca, si ricava che, nella UE, «*11 out of 27 member states […]are already using facial recognition against biometric databases for forensic purposes and 7 additional countries are expected to acquire such capabilities in the near future*»[105].

Ciò posto, è il caso di segnalare che siffatta "marcia trionfale" del riconoscimento facciale automatico negli ordinamenti giuridici contemporanei è resa particolarmente problematica da una circostanza specifica. Si allude al fatto che, in diversi Stati, l'impiego della tecnologia *de qua* è stato avviato per la sola iniziativa delle autorità di pubblica sicurezza, in assenza di uno specifico intervento regolativo del legislatore[106]. Come è facile intuire, la mancata cristallizzazione di un compendio di garanzie processuali, idonee quantomeno a bilanciare i pericoli derivanti dall'impiego delle nuove tecnologie, ha conseguenze davvero esiziali: un tanto aumenta esponenzialmente il rischio che le stesse finiscano per comprimere alcuni tra i più basilari diritti fondamentali dell'individuo. Purtroppo, considerazioni di questo tipo valgono anche per l'esperienza italiana in materia, sulla quale è arrivato il momento di focalizzare l'attenzione.

---

[105] La citazione è tratta da *Greens/EFA*, *Biometric & Behavioural Mass Surveillance,* cit., pp. 19 s. Vale, inoltre, la pena di ricordare che l'utilizzo già massiccio della tecnologia in esame nello spazio di libertà, sicurezza e giustizia incrementerà ancora di più laddove venisse approvata la proposta di regolamento UE, *sullo scambio automatizzato di dati per la cooperazione di polizia ("Prüm II")*, COM (2021) 784, 8 dicembre 2021, la quale ha, tra l'altro, il fine di consentire il trasferimento e la consultazione automatizzata di immagini facciali da parte delle autorità di contrasto dei Paesi UE (e di Europol), rendendo comunicanti le banche dati nazionali (ed europee). Per un'analisi critica di siffatta iniziativa: cfr. l'*opinion* 4/2022 del 2 marzo 2022 dell'*European Data Protection Supervisor*.

[106] Ciò vale, ad esempio, per l'Inghilterra e il Galles (come è stato espressamente riconosciuto dalla *Court of Appeal*, nella nota sentenza *R (Bridges) – v – CC South Wales*, [2020] EWCA Civ 1058, §§ 90-94; sulla quale cfr. B. Keenan, *Automatic Facial Recognition and the Intensification of Police Surveillance*, in *Modern Law Review*, 2021, p. 886; A. Pin, *op. cit*., p. 291; J. Purshouse, L. Campbell, *Automated facial recognition and policing: A Bridge too far?*, in *Legal Studies*, 2022, p. 209; M. Zalnieriute, *Burning* Bridges: *The Automated Facial Recognition Technology and Public Space Surveillance in The Modern State*, in *The Columbia Science & Technology Law Review*, 2021, p. 243), oppure per la Germania (in questo senso v. la decisione del garante della *privacy* di Amburgo*, Antrag auf Zulassung der Berufung §§ 124, 124° VwGO,* 13 marzo 2020, pp. 8 s.).

5. L'esperienza italiana: il "sistema automatico di riconoscimento delle immagini"

Non è un mistero che, in Italia, gli istituti volti a consentire il riconoscimento di persone o di cose sono tradizionalmente soggetti a forti tendenze "antiformalistiche"[107]. Sebbene la consapevolezza circa i problemi di affidabilità, che affliggono (pure) l'attività ricognitiva umana, abbia portato il legislatore a dettare una nutrita serie di regole sul punto, è indiscutibile che l'impianto codicistico non abbia retto all'"urto" della prassi. È cosa nota, d'altra parte, che accanto agli strumenti "tipici" tradizionali della ricognizione (artt. 213 ss. c.p.p.) e dell'individuazione (art. 361 c.p.p.), il diritto pretorio ne abbia creati altri, privi di una puntuale disciplina, tra cui spicca il cd. "riconoscimento informale" dell'imputato, compiuto dai testimoni nel corso del dibattimento[108]. Vale la pena di rammentare che tale scenario si è potuto concretizzare soprattutto grazie all'atteggiamento "bulimico" della giurisprudenza[109]: è stata, in particolare, la Cassazione ad aver avallato le operazioni esegetiche creative degli operatori del diritto, confermandone la validità per il tramite di discutibili *caveat*, come il principio del libero convincimento del giudice[110], ancora una volta, inquisitoriamente trasfigurato in «vorace potenza superlogica, che trae il proprio

[107] In argomento, v. A. Bernasconi, *op. cit*., pp. 195 ss.; M. Bontempelli, *La ricognizione nel processo penale*, Torino, 2012; G. Cecanese, *Confronto, ricognizione ed esperimento giudiziale nella logica dei mezzi di prova*, Napoli, 2013, p. 145; A. Marandola, *L'identificazione fotografica*, in A. Scalfati (a cura di), *Le indagini atipiche*, cit., p. 209; N. Pascucci, *La natura controversa della ricognizione fotografica*, in *Riv. it. dir. proc. pen*., 2017, p. 287.

[108] Sul punto cfr., tra i molti, G. Cecanese, *Aspetti problematici e snodi interpretativi dell'individuazione di persone e di cose*, in *Archivio penale – Rivista web*, 2018, n. 1, pp. 12 ss.; N. Pascucci, *Un nodo ancora da sciogliere nel processo penale: il riconoscimento informale di persona in udienza*, in *Dir. pen. proc*., 2018, p. 721.

[109] Parla di «"bulimia logica" della giurisprudenza» A. Bernasconi, *Il riconoscimento fotografico curato dalla polizia giudiziaria*, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2014, p. 184.

[110] Cfr., solo per fare qualche esempio, Cass., sez. fer., 8 agosto 2019, n. 43285, in *Cass. pen*., 2020, p. 2073; Cass. pen., sez. V, 1° ottobre 2015, n. 6546, in *C.E.D. Cass*., n. 266023; Cass. pen., sez. V, 10 febbraio 2009, n. 22612, in *Cass. pen*., 2010, p. 1590.

alimento da tutto ciò che anche per un solo istante sia comparso sulla scena del processo»[111].

In un quadro già affetto da una così marcata «tendenza alla destrutturazione del sistema delle prove penali»[112], non stupisce se, a seguito del diffondersi delle tecnologie di *facial recognition* e della presa d'atto delle loro indubitabili potenzialità, si sia cercato di attribuire loro uno spazio, pur in assenza di un previo intervento regolativo da parte del legislatore.

I primi passi in proposito sono stati mossi già più di un quinquennio fa, per iniziativa del Ministero dell'Interni: è stata, in particolare, tale amministrazione ad avviare, nel 2016, una procedura a evidenza pubblica, finalizzata a dotare le forze di polizia[113] di una macro-infrastruttura informatica, denominata «sistema automatico di riconoscimento delle immagini» e, più comunemente, nota con l'acronimo SARI[114].

La fonte principale delle (scarse) informazioni disponibili, onde ricostruire il funzionamento del meccanismo, è costituita dal capitolato tecnico[115], allegato al contratto che la Direzione Centrale Anticrimine ha stipulato l'anno successivo con un'azienda privata italiana, a cui è stato affidato il compito di sviluppare concretamente l'applicativo[116]. Da tale documentazione, si ricava che il committente ha richiesto di sviluppare un sistema di riconoscimento automatico dei volti, a partire da immagini o *frame* video, in grado di gestire due diversi scenari operativi, chiamati, rispettivamente, *Enterprise* e *Real-Time*.

Nella prima modalità, le autorità di *law enforcement* sono messe in grado di ricercare (in meno di quindici secondi) l'identità di un volto, presente in un'immagine già acquisita agli atti, all'interno di una banca dati di grandi dimensioni, individuata nella piattaforma AFIS – SSA (*Automated Fingerprint Identification System*), ovvero il «sistema automatizzato di identificazione delle impronte digitali», integrato dal

[111] La citazione è tratta da F. Cordero, *Diatribe sul processo accusatorio*, in Id., *Ideologie del processo penale*, Milano, 1966, pp. 299 s.

[112] L'espressione è di N. Pascucci, *La natura controversa*, cit., p. 298.

[113] Il *tool* è a disposizione sia della Polizia di Stato, sia dell'Arma dei Carabinieri.

[114] Sulle origini di SARI, cfr. R. Lopez, *op. ult. cit*., pp. 240 ss.

[115] Cfr. Ministero dell'Interno, Dipartimento della pubblica sicurezza, *Capitolato tecnico. Procedura volta alla fornitura della soluzione integrata per il Sistema Automatico di Riconoscimento Immagini S.A.R.I*., in *www.poliziadistato.it*, 27 giugno 2016.

[116] L'applicazione è stata sviluppata dall'azienda PARSEC 3.26.

«sottosistema anagrafico»[117]. Si tratta di *database* preesistenti, le cui funzionalità sono state sviluppate e replicate all'interno di SARI, ove confluiscono le immagini di diverse categorie di individui oggetto di fotosegnalazione (tra cui, ad esempio, indagati, oppure persone che non siano in grado di provare la loro identità, o, ancora, migranti), nonché le informazioni concernenti i loro dati anagrafici e biometrici[118].

Più in particolare, lo scenario *Enterprise* permette di compiere un'analisi su più livelli: su base volto; su base anagrafica/descrittiva e, infine, su base combinata, in quanto elaborata tramite integrazione di entrambe le tipologie di dati. È sempre il capitolato a prevedere poi che, al termine dell'operazione di ricerca, la macchina fornisca una *candidate list*, ovvero un elenco di profili ordinato in base a un punteggio che ne indichi il grado di similarità. A questo punto, si è stabilita la necessità dell'intervento di un operatore "umano", il cui compito è quello di confermare o meno il risultato del *tool*, applicando le procedure di comparazione fisionomica, rispetto alle quali le forze di polizia scientifica ricevono una specifica formazione[119]. Non sfuggirà come l'aver contemplato la presenza di un funzionario in "carne e ossa" costituisca una garanzia importante (anche se non risolutiva)[120]: tale accorgimento permette, infatti, di rispettare il principio del cd. "*human in the loop*"[121], ossia della necessaria

[117] Cfr. ancora R. Lopez, *op. ult. cit*., p. 242.

[118] Stando a quanto riportato nella riposta a un'interrogazione parlamentare sul funzionamento di SARI (n. 5-03482 *Ceccanti*, in Atti Camera, I Commissione permanente, 5 febbraio 2020, in *www.camera.it*, p. 61), a inizio 2020 nella banca dati AFIS erano presenti 17.592.769 cartellini fotosegnaletici, corrispondenti a 9.882.490 individui diversi, di cui 2.090.064 cittadini italiani.

[119] Cfr. M. Valeri, *Mettiamoci la faccia*, in *www.poliziamoderna.poliziadistato.it*, 9 marzo 2022. Si può menzionare, a questo proposito, lo studio di fonti come il *Best Practice Manual for Facial Image Comparison*, elaborato dall'ENFSI nel 2018.

[120] Come si è giustamente osservato, tale salvaguardia non rappresenta, invero, una panacea in grado di evitare ogni rischio di false identificazioni (cfr., in questo senso, E. Sacchetto, *op. ult. cit*., p. 9). E ciò in quanto il controllo umano su una decisione automatizzata è «un "rimedio" che presenta diverse criticità, in generale e nella materia penale in particolare»; prima tra tutte quella per cui, vista la natura di *black box* degli attuali sistemi di A/IA, risulta in concreto spesso utopistico poterne «contestarne il merito in modo effettivo» (le citazioni sono tratte da G. Contissa, G. Lasagni, G. Sartor, *op. cit*., pp. 629 e s.).

[121] Sul quale, cfr., tra i molti, M. Leta Jones, *The right to a human in the loop: Polit-*

interazione tra macchina ed essere umano, prescritto, in questo settore, dall'art. 11 della direttiva 2016/680/UE[122] e recepito a livello interno dall'art. 8 del d. lgs. 18 maggio 2018, n. 51.

Viceversa, SARI *Real-Time* consente di analizzare in diretta i volti inquadrati dalle telecamere (fisse o mobili), collocate in luoghi specifici oggetto di osservazione e di confrontarli con un *database* più ristretto di persone ricercate (la c.d. "*watch-list*"), la cui grandezza è al massimo di 10.000 volti. Il sistema può, più in particolare, essere installato direttamente nel luogo ove sorga l'esigenza di disporre di una tecnologia di riconoscimento facciale per coadiuvare le forze di polizia nella gestione dell'ordine e della sicurezza pubblica, o in relazione a specifiche esigenze investigative. Allorquando la macchina riscontri una corrispondenza, viene a generarsi un *alert*, in grado di richiamare l'attenzione dei funzionari, cui spetta, anche in questo caso, il compito finale di confermare il riconoscimento e di prendere i provvedimenti conseguenti.

Sempre a livello operativo, il Viminale ha previsto che, tanto SARI *Enterprise*, quanto *Real-Time*, utilizzino quale algoritmo di riconoscimento facciale di base il medesimo *engine*, scelto tra quelli testati dall'agenzia statunitense "*National Institute of Standards and Technology*". Si tratta di un accorgimento – evidentemente teso ad assicurare il rispetto di determinati *standard* qualitativi minimi – che presenta, tuttavia, una non trascurabile eccezione: è stato il capitolato contrattuale ad aver stabilito che SARI *Enterprise* possa includere anche ulteriori algoritmi, non certificati dal *NIST*[123], aprendosi così le porte ad applicativi con livelli di affidabilità meno elevati.

Ciò posto, è ancora il caso di precisare che la versione originaria

---

ical constructions of computer automation and personhood, in *Social Studies of Science*, 2017, pp. 216 ss.

[122] Com'è noto, esso vieta le decisioni basate su trattamenti automatizzati, salvo che siano autorizzati dal diritto UE o dello Stato membro cui è soggetto il titolare del trattamento e a fronte della fissazione di garanzie adeguate, tra cui almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento. Per un'analisi critica della previsione, cfr. 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. process.*, 2021, pp. 101 ss.

[123] Ministero dell'Interno, Dipartimento della pubblica sicurezza, *Capitolato tecnico*, cit., p. 13.

dell'infrastruttura è stata già oggetto di un *restyling* tra il 2020 e il 2021. Ci si riferisce al fatto che, nell'ambito del più generale progetto ministeriale, teso a modernizzare le tecnologie a disposizione delle autorità di *law enforcement*, denominato "*Falco Extended*", l'amministrazione ha richiesto di potenziare il sistema SARI[124], tanto nella sua componente *Enterprise*, quanto in quella *Real-Time.*

È bene precisare che la circostanza per cui, già dopo pochi anni dalla creazione dell'applicativo in esame, si sia sentita la necessità di modificarlo non deve stupire: i meccanismi di *facial recognition*, basandosi su una tecnologia ancora in evoluzione, necessitano, infatti, di continui aggiornamenti[125]. Ne consegue che le iniziative volte a modernizzarli non possono che essere letti favorevolmente: solo in questo modo è possibile renderli davvero affidabili, riducendo il rischio di false individuazioni.

6. Il dibattito interno

Così come accaduto all'estero, anche in Italia la scelta ministeriale di istituire una piattaforma di riconoscimento facciale ha dato vita a un acceso dibattito interno.

A livello istituzionale, decisamente positiva è stata l'accoglienza della nuova tecnologia da parte delle forze di polizia, le quali l'hanno salutata, in modo entusiastico, come «una delle più grandi innovazioni degli ultimi anni»[126].

Per contro, i rischi legati all'impiego degli *AFRS* sono stati presi in considerazione soprattutto dal Garante della *privacy* italiano: tale autorità amministrativa ha svolto due istruttorie, tese a verificarne la compatibilità rispetto ai diritti fondamentali dell'individuo.

La prima, avente a oggetto SARI *Enterprise*, è terminata già nel 2018, con un provvedimento che ha escluso la presenza di «criticità sotto il pro-

[124] Cfr. F.S.I. – Progetto n. 87.5.1, *Avviso pubblico Sistema Automatico Riconoscimento Immagini*, *in www.poliziadistato.it*, 25 maggio 2020.

[125] Cfr. W. Crumpler, *op. cit*., il quale ricorda che «as of April 2020, the best face identification algorithm has an error rate of just 0.08% compared to 4.1% for the leading algorithm in 2014».

[126] In questo senso, v. l'articolo di M. Valeri, *op. cit.*

filo della protezione dei dati»[127]. Più in particolare, dopo aver ricordato che – in virtù del d.lgs. 51/2018, di attuazione della direttiva 2016/680/UE – il trattamento di informazioni biometriche può avvenire solo in presenza di un'adeguata base normativa, il Garante ha affermato che siffatto requisito sarebbe soddisfatto da una serie di disposizioni regolamentari[128] e legislative già vigenti, tra cui, a livello di procedimento penale di cognizione, spicca l'art. 349 del c.p.p., in materia di "identificazione"[129].

Com'è noto, le cose sono andate diversamente con riguardo alla seconda istruttoria, concernente SARI *Real-Time*, conclusasi solo nel marzo del 2021[130]. Anche sull'onda della sensibilità sempre maggiore, sviluppatasi a livello europeo circa i possibili abusi causati dalle tecnologie di IA, il Garante ha emesso un parere contrario rispetto all'impiego di tale strumento, che – è bene precisarlo – finora non dovrebbe risultare ancora operativo nella prassi[131]. L'autorità amministrativa è giunta a tale conclusione sulla base del duplice rilievo per cui, per un verso, le tec-

[127] Ci si riferisce al documento del Garante per la protezione dei dati personali, *Sistema automatico di ricerca dell'identità di un volto*, 26 luglio 2018, n. 440, doc. web n. 9040256, in *www.garanteprivacy.it.*

[128] A livello regolamentare, il Garante ha posto l'accento in particolare sulla scheda n. 19, recante la disciplina del Sistema AFIS, allegata al decreto del Ministero dell'Interno del 24 maggio 2017, recante individuazione dei trattamenti di dati personali effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza o da forze di polizia, in *G.U.*, n. 145 del 24 giugno 2017.

[129] Tale disposizione pare avere, effettivamente, una formulazione letterale sufficientemente ampia da consentire l'utilizzo di strumenti come SARI (in questo senso cfr. M. Gialuz, *op. ult. cit*., p. 63 e M. Torre, *op. cit*., p. 1052), soddisfacendo, così, la riserva di legge di cui all'art. 23 Cost. Difatti, essa, oltre a far riferimento alla possibilità di compiere rilievi fotografici e antropometrici, ammette pure lo svolgimento di "altri accertamenti"; valvola di chiusura, quest'ultima, adatta proprio ad aprire la previsione alla "scienza" (così anche T. Alesci, *op. cit*., p. 81). È ancora utile precisare che la circostanza per cui la sottoposizione a riconoscimento non implica un intervento coattivo sul "corpo fisico" della persona non sembra consentire l'applicazione estensiva nella fattispecie in esame delle garanzie di cui al co.2-*bis* dell'art. 349 c.p.p., previste in tema di prelievo di capelli o di saliva: cfr., in questo senso, anche G. Mobilio, *op. cit.*, p. 88.

[130] Cfr. Garante per la protezione dei dati personali, *Parere sul sistema Sari Real Time*, 25 marzo 2021, n. 127, doc. web n. 9575877, in *www.garanteprivacy.it.*

[131] Lo ha affermato espressamente la Ministra Lamorgese nella risposta all'interrogazione parlamentare dell'On. Sensi n. 3-02074, in Atti Camera, Resoconto stenografico dell'Assemblea, seduta n. 463, 3 marzo 2021.

nologie di riconoscimento *live* finirebbero per processare i dati di tutti coloro che sono ripresi dalle telecamere (e pertanto anche di soggetti che non siano oggetto di specifica ricerca da parte delle forze di *law enforcement*), nonché, per altro verso, della mancanza di una base giuridica idonea a disciplinare i casi e i modi di impiego del sistema.

Siffatta decisione è stata accolta con favore dagli studiosi, i quali si sono dimostrati compattamente contrari alla possibilità di utilizzare SARI *Real-Time*, in assenza di un intervento *ad hoc* del legislatore[132]. D'altra parte, trattandosi di una sorta di "videoripresa algoritmica" [133] non finalizzata a captare un comportamento comunicativo, è chiaro come – stando all'insegnamento delle sezioni unite *Prisco*[134] – la stessa non possa trovare ingresso neppure tramite un'applicazione analogica della disciplina delle intercettazioni[135].

Nondimeno, va aggiunto che una parte della dottrina, sull'onda del movimento di pensiero europeo che ritiene gli impieghi *ex post* degli *AFRS* altrettanto pericolosi per i diritti fondamentali dell'individuo di quelli *live*[136], ha censurato pure l'applicazione, a codice invariato, di SARI *Enterprise*, per finalità diverse da quelle di mera identificazione[137]. A tal riguardo, dopo essersi osservato che l'utilizzo a fini investigativi e/o probatori di tale modalità del *tool* rientrerebbe nell'alveo, rispettivamente, delle *individuazioni* o delle *ricognizioni* "atipiche", dal momento che l'attività principale di riconoscimento è compiuta da una macchina e

---

[132] V., tra gli altri, G. Borgia, *op. cit*., pp. 16 ss.; M. Gialuz, *op. ult. cit*., pp. 64 s.; R. Lopez, *op. ult. cit*., pp. 256 s.

[133] Per riprendere la terminologia di *La Quadrature du Net*, *Qu'est-ce que la vidéosurveillance algorithmique?*, in *www.laquadrature.net*, 23 marzo 2022.

[134] Cass., sez. un., 28 marzo 2006, Prisco, in *Riv. it. dir. proc. pen*., 2006, p. 1537, con nota di A. Camon, *Le sezioni unite sulla videoregistrazione come prova penale: qualche chiarimento e alcuni dubbi nuovi*.

[135] Condivide questa opinione M. Gialuz, *op. ult. cit*., p. 64.

[136] Cfr., in proposito, *Greens/EFA*, *Biometric & Behavioural Mass Surveillance,* cit., pp. 11 s., ove si afferma che «*the distinction between "real-time" and "ex-post" is irrelevant when it comes to the impact of these technologies on fundamental rights. Ex-post identification carries in fact a higher potential of harm, as more data can be pooled from different sources to proceed to the identification*». Del resto, il caso *Clearview* dimostra proprio che anche in modalità *ex post* i *tools* si prestano a impieghi assai invasivi, potendo essere utilizzati anche quali mezzi di sorveglianza di massa.

[137] In questo senso, cfr., in particolare, M. Gialuz, *op. ult. cit*., p. 64.

non da un uomo[138], si è, in particolare, negato che siffatte attività possano comunque far ingresso sulla scena procedimentale per il tramite del *passe-partout* dell'art. 189 c.p.p.[139].

Si tratta di un'opinione senz'altro condivisibile, dal momento che SARI non è – a oggi – in grado di rispettare alcuno dei presupposti, fissati dall'ordinamento affinché mezzi di prova o mezzi di ricerca della prova[140] non disciplinati dalla legge possano essere impiegati nel procedimento penale.

Da un lato, l'autorità giudiziaria non sembra essere nelle condizioni di valutare in concreto l'effettiva idoneità del programma ad assicurare l'accertamento dei fatti[141], dato che è affetto da gravi problemi di opacità[142]. A conferma di un tanto, è utile, del resto, osservare come, pur essendo oramai trascorsi diversi anni dalla creazione del sistema, mancano ancora del tutto informazioni essenziali per comprenderne il funzionamento e la sua concreta affidabilità[143]. Nulla si sa, ad esempio, circa: 1) i tassi di errore che caratterizzano gli algoritmi; 2) il percorso di "allenamento" a cui gli *engine* sono stati sottoposti; 3) i presidi volti a evitare possibili effetti discriminatori causati dalla macchina, nonché abusi dei dati personali raccolti; 4) le garanzie specifiche tese a ridurre il rischio che l'IA si comporti come una *black box*.

Da un altro lato, neppure il criterio del rispetto della "libertà morale"

---

[138] Al riguardo, v. G. Borgia, *op. cit*., p. 9; M. Gialuz, *op. ult. cit*., p. 63; R. Lopez, *op. ult. cit*., p. 255; E. Sacchetto, *op. ult. cit*., p. 13; M. Torre, *op. cit*., p. 1052.

[139] Sul punto, v., ancora, G. Borgia, *op. cit*., p. 16 ss.; M. Gialuz, *op. ult. cit*., p. 64; M. Torre, *op. cit*., p. 1053.

[140] Com'è noto, la dottrina e la giurisprudenza maggioritari ritengono che sia possibile riferire l'art. 189 c.p.p. anche ai mezzi di ricerca della prova atipici: per i dovuti riferimenti sul punto, cfr. V. Bonini, *Videoriprese investigative e tutela della riservatezza: un binomio che richiede sistemazione legislativa*, in *Processo penale e giustizia*, 2019, n. 2, p. 339. *Contra*, invece, S. Marcolini, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen*., 2015, p. 773.

[141] In questo senso, v. M. Gialuz, *op. ult. cit*., p. 64 e M. Torre, *op. cit*., pp. 1053 s.

[142] Tale difetto della piattaforma è universalmente riconosciuto in dottrina: cfr., *ex multis*, G. Borgia, *op. cit*., p. 10; M. Gialuz, *op. ult. cit*., p. 64; E. Sacchetto, *op. ult. cit*., p. 10; M. Torre, *op. cit*., p. 1053.

[143] Come afferma E. Sacchetto, *op. ult. cit*., p. 14, a fronte dei numerosi dubbi concernenti l'impiego di SARI, l'unica certezza è rappresentata da un suo grado di affidabilità estremamente debole, in quanto esito di una procedura troppo poco trasparente.

dell'individuo può dirsi rispettato[144]. Ciò si deve al fatto che, come si è avuto modo di osservare, gli *AFRS*, oltre ad assoggettare coattivamente del tutto al potere dell'autorità una porzione del corpo virtuale della persona, sono in grado pure di avere un marcato *chilling effect*, rischiando di mutare in modo radicale le normali abitudini individuali[145].

Ne consegue, pertanto, che, in assenza di una normativa che ne disciplini i casi e i modi, le individuazioni o le ricognizioni algoritmiche, compiute tramite SARI *Enterprise* o *Real-time*, debbono considerarsi inibite in assoluto: con la conseguenza che è vietata la loro acquisizione e/o utilizzazione nel procedimento[146].

Ma, a ben considerare, non è tutto. A quanto appena affermato va ancora aggiunto che, *a fortiori*, neppure le applicazioni degli apparati in

---

[144] Cfr. ancora M. Gialuz, *op. ult. cit*., p. 64. Per una posizione più articolata, cfr. M. Torre, *op. cit*., p. 1054, a detta del quale soltanto la modalità SARI *Real Time* violerebbe la libertà morale dell'individuo.

[145] La tesi secondo cui le «pratiche investigative idonee a condizionare le scelte comportamentali di chi ne sia oggetto» contrasterebbero con il dovere di rispettare la libertà morale della persona è sostenuta da F. Caprioli, *Riprese visive nel domicilio e intercettazione per immagini*, in *Giur. cost*., 2002, p. 2188.

[146] E ciò sulla base del "combinato disposto" tra artt. 189 e 191 c.p.p. Al riguardo, pare, invero, da condividere la tesi di chi ritiene che dall'art. 189 si ricavi un *divieto probatorio implicito* nei confronti delle prove non disciplinate dalla legge acquisite in spregio ai diritti fondamentali dell'individuo, la cui violazione è causa di inutilizzabilità patologica (cfr., in questo senso, C. Conti, *Accertamento del fatto e inutilizzabilità nel processo penale*, Padova, 2007, p. 173, nonché P. Tonini, C. Conti, *Il diritto delle prove penali*, Milano, 2014, p. 105. *Contra*, invece, M. Daniele, *Indagini informatiche lesive della riservatezza. Verso un'inutilizzabilità convenzionale?*, in *Cass. pen*., 2013, p. 370). Pare utile rilevare che a un risultato analogo si potrebbe pervenire anche laddove si aderisse all'interpretazione "classica" della dottrina delle "prove incostituzionali" (sulla quale cfr., anche per ulteriori riferimenti giurisprudenziali e dottrinali, l'analisi di A. Cabiale, *I limiti alla prova nella procedura penale europea*, Milano, 2019, pp. 35 ss.), secondo cui i "divieti probatori", menzionati dall'art. 191 c.p.p., potrebbero ricavarsi direttamente anche dalla Carta fondamentale. Non vi sono, invero, dubbi circa il fatto che le individuazioni e le ricognizioni algoritmiche sono, in assenza di una espressa disciplina legislativa dei casi e dei modi, acquisite in violazione di diverse previsioni costituzionali (tra cui, oltre all'art. 13 Cost., anche gli artt. 11 e 117 Cost., questi ultimi in relazione agli artt. 7, 8 e 52 della Carta di Nizza, nonché 8 CEDU). Com'è ovvio, nel caso in cui le immagini sono riprese in luoghi coperti dalla libertà di domicilio, viene in gioco pure la violazione dell'art. 14 Cost., stante la mancata attuazione della riserva di legge ivi contenuta.

esame quali forme di analisi delle emozioni possono trovare spazio per scopi ricostruttivi del fatto di reato[147]. Esse vedono irrimediabilmente bloccata la via da «quella vera e propria "linea Maginot" eretta dal codice del 1988, rispetto agli esperimenti gnoseologici che rischiano di pregiudicare la libertà morale»[148]: il riferimento va, oltre all'art. 189 c.p.p., anche agli artt. 64, co.2, 188[149] e 220, co.2, c.p.p. Il che sta a dimostrare come la "barriera etica"[150], posta dall'ordinamento all'impiego di nuovi strumenti investigativi o probatori, che non siano in grado di rispettare determinati *standard* minimi di garanzia e di affidabilità, sia, se interpretata rigorosamente, abbastanza solida da impedire l'avanzata anche di forme di IA particolarmente penetranti.

7. Riconoscimento facciale e accertamenti tecnici: un binomio (finora) impossibile

Giunti a questo punto, è il caso di precisare che, a livello ministeriale, si è tentata una strada alternativa, onde sostenere la possibilità di avvalersi di SARI, a codice invariato, per scopi investigativi e/o probatori. Si allude alla tesi secondo cui il "combinato disposto" tra esito del *tool* e conferma dell'operatore umano andrebbe ricompreso non tra le evidenze atipiche, ma in seno alla categoria degli "accertamenti tecnici"[151]. In quest'ottica, si ritiene, insomma, che gli algoritmi di riconoscimento facciale potrebbero avere ingresso sulla scena procedimentale per il tramite

[147] In questo senso, v. anche G. Mobilio, *op. cit.*, p. 91.

[148] Cfr. M. Gialuz, *op. ult. cit*., p. 64.

[149] Ciò vale in particolare nel caso in cui lo strumento venga impiegato come moderna forma di *lie detector*; ovvero uno strumento il cui utilizzo veniva considerato precluso dagli artt. 64, co.2 e 188 c.p.p. già nella *Relazione al progetto preliminare del codice del 1988*, in *G.U*., n. 250, 24 ottobre 1988, p. 60.

[150] Per riprendere la terminologia di F.R. Dinacci, *Neuroscienze e processo penale: il ragionamento probatorio tra chimica valutativa e logica razionale*, in *Processo penale e giustizia*, 2016, n. 2, p. 4.

[151] Cfr. l'avviso informativo ufficiale circa la sperimentazione di SARI da parte delle forze di polizia, *Sistema Automatico di Riconoscimento Immagini: un futuro che diventa realtà*, in *www.interno.gov.it*, 7 settembre 2018, dove si afferma che il *match* confermato dall'operatore umano «consente di integrare l'utilità investigativa del risultato anche con un accertamento tecnico a "valenza dibattimentale"».

degli ordinari istituti investigativi e/o probatori previsti dal legislatore per il caso in cui sia necessario procedere «ad accertamenti, rilievi segnaletici, descrittivi o fotografici e ad ogni altra operazione […] per cui sono necessarie specifiche competenze» (art. 359 c.p.p.).

Ancorché si tratti di una lettura suggestiva[152], la stessa non convince, per più ordini di ragione.

A parte quanto si è già detto circa l'inidoneità della piattaforma SARI, data l'"oscurità" che l'ha fino a oggi caratterizzata, a generare elementi (scientifici) sufficientemente affidabili per procedere alla verifica dell'oggetto di prova[153], il motivo principale per cui tale via non pare percorribile è connesso allo *standard* di tutela particolarmente elevato che il diritto europeo pone a presidio del diritto alla protezione dei dati biometrici[154]. Più in particolare, non sfuggirà come le previsioni codicistiche degli artt. 354 o 359 c.p.p. non siano idonee a soddisfare quella duplice valutazione di proporzionalità (in astratto e in concreto) di cui si è detto, imposta a livello eurounitario quale requisito di base con riguardo agli strumenti

[152] La stessa, infatti, ripropone, da un'ulteriore prospettiva, la diatriba tra coloro che ritengono che anche le nuove prove scientifiche possano trovare ingresso nel procedimento penale tramite gli istituti "ordinari" dell'accertamento tecnico (e della perizia) e quelli che, invece, sostengono che esse vadano ricondotte nella sfera di operatività dell'art. 189 c.p.p. Nel primo senso, cfr., per tutti, G. Ubertis, *La prova scientifica e la nottola di Minerva*, in Id., *Argomenti di procedura penale*, II, Milano, 2006, pp. 204-206. La seconda tesi si trova, invece, sviluppata da O. Dominioni, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Milano, 2005, pp. 102 ss.

[153] Al riguardo, merita precisare come SARI non pare in grado di rispettare neppure i principi stabiliti dalla giurisprudenza in tema di ammissibilità e di valutazione delle nuove prove scientifiche (si allude, in particolare, ai cosiddetti "criteri Cozzini", sviluppati a partire da Cass., sez. IV, 17 settembre 2010, n. 43786, in *Dir. pen. proc*., 2011, p. 1341, con nota di P. Tonini, *La Cassazione accoglie i criteri* Daubert *sulla prova scientifica*). Le poche informazioni disponibili sul funzionamento del sistema, sommate alla possibilità che lo stesso si comporti come una *black box*, non sembrano consentire al giudice di svolgere in modo adeguato la sua funzione chiave di "*gate keeper*" della buona scienza (l'espressione è di G. Varraso, *Neuroscienze e consulenza "investigativa"*, in A. Scalfati (a cura di), *Le indagini atipiche*, cit., p. 370), non essendo nelle condizioni di verificare la controllabilità e la falsificabilità della teoria impiegata, né di individuare il tasso di errore della stessa, nonché di sottoporla a un controllo effettivo della comunità scientifica di riferimento.

[154] V. *supra* § 3.

idonei a determinare ingerenze gravi nei diritti fondamentali alla vita privata e alla protezione dei dati personali. E ciò, sia perché tali norme affidano determinati poteri direttamente alle autorità di *law enforcement* e non a un giudice o a un'entità amministrativa indipendente, sia in quanto risultano applicabili per qualsiasi tipo di reato, senza distinzioni di sorta. Ne deriva che, utilizzandole per dare ingresso a strumenti come quelli in esame, non si farebbe altro che esporle a inevitabili profili di contrasto con le fonti sovraordinate[155].

Siffatta conclusione pare rafforzata dalla circostanza per cui l'applicazione degli *AFRS* per finalità ricostruttive del reato impatta negativamente pure sull'art. 13 Cost., quantomeno laddove esso venga inteso nel senso estensivo sopra indicato di previsione idonea a tutelare, oltre alla libertà fisica della persona, anche quella morale[156]. Fin da un primo sguardo ci si renderà, infatti, conto che gli artt. 354 o 359 c.p.p. (ma lo stesso varrebbe anche per l'art. 220 c.p.p., in tema di perizia) non delineano in modo sufficientemente preciso i "casi" e i "modi" in cui i *tools* potrebbero essere applicati da rispettare lo *standard* minimo di tassatività, imposto dall'art. 13, co.2 Cost. Né sfuggirà come, utilizzando siffatte disposizioni per far spazio a SARI, verrebbe a determinarsi un quadro simile a quello che, in passato, ha portato la Consulta a dichiarare l'incostituzionalità dell'art. 224, co.2, c.p.p., in ragione dell'indeterminatezza della disciplina su cui si faceva leva per autorizzare i prelievi coattivi[157].

A ben vedere, proprio il parallelo appena compiuto potrebbe portare a chiedersi se possano fungere da basi giuridiche, idonee a legittimare l'impiego della tecnologia *de qua* per scopi di ricostruzione del fatto di reato, non le norme generali sugli accertamenti tecnici o sulla perizia, ma quelle speciali degli artt. 359-*bis* e 224-*bis* c.p.p., tramite cui, com'è ben noto, il legislatore ha ovviato alla lacuna creata da Corte cost. 238/1996[158].

---

[155] A ben vedere, una critica analoga varrebbe anche se si tentassero di impiegare le generiche previsioni di cui agli artt. 55 e 348, co.2, lett. *b*), quale canale processuale per consentire l'impiego di SARI da parte della polizia giudiziaria.

[156] Cfr. *supra* § 3.

[157] Si allude, ovviamente, a C. cost., 27 giugno 1996, n. 238, in *www.cortecostituzionale.it*.

[158] Il riferimento va alla riforma operata dalla l. 30 giugno 2009, n. 85, sulla quale cfr., tra i molti, C. Bonzano, *Gli accertamenti medici coattivi. Legalità e proporzionalità*

Neppure tale interpretazione sembra, peraltro, utilmente sostenibile per ragioni di ordine letterale. A una disamina attenta, ci si renderà conto di come gli artt. 359-*bis* e 224-*bis* c.p.p. si riferiscano ai soli mezzi investigativi e/o probatori che incidano nella sfera tradizionale della libertà "*fisica*", mentre nulla prevedono in merito a *tools* che impattino unicamente sulle informazioni "*virtuali*" del corpo di una persona. A riprova di un tanto vanno, d'altra parte, plurimi indici testuali, quali, ad esempio, la rubrica dell'art. 359-*bis* c.p.p., ove si fa riferimento al "prelievo" coattivo di "campioni biologici"[159] e non in generale di dati "biometrici"; oppure il fatto che l'art. 224-*bis* c.p.p. menzioni solo la raccolta e l'analisi di reperti "*materiali*", come capelli, peli e mucosa del cavo orale (finalizzata, oltretutto, all'estrazione del profilo del DNA). Né – è bene precisarlo – pare potersi adattare alla fattispecie in esame neppure l'altra macro-ipotesi di perizia coattiva menzionata dall'art. 224-*bis* c.p.p., costituita dagli "accertamenti medici"; stante la mancanza, di norma, di un obiettivo "sanitario" nell'applicazione degli *AFRS*[160].

Allo stesso tempo, la lacuna appena descritta non può essere colmata interpretando gli artt. 359-*bis* e 224-*bis* c.p.p. in via analogica: trattandosi di norme che incidono direttamente sulla libertà personale, le stesse non possono essere applicate oltre ai casi e ai tempi considerati, posto

nel regime della prova, Padova, 2017; G. Conso-G. Giostra (a cura di), *La disciplina del prelievo biologico coattivo, alla luce della l. 30 giugno 2009, n. 85*, in *Giur. it.,* 2010, pp. 1217 ss.; C. Gabrielli, *Il prelievo coattivo di campioni biologici nel sistema penale*, Torino, 2012; L. Marafioti, L. Lupária (a cura di), *Banca dati del DNA e accertamento penale*, Milano, 2010; A. Presutti, *L'acquisizione forzosa dei dati genetici tra adempimenti internazionali e impegni costituzionali*, in *Riv. it. dir. proc. pen*., 2010, p. 545.

[159] Al riguardo, è utile precisare che l'art. 6, co.1, lett. c) della l. 30 giugno 2009, n. 85 definisce "campione biologico" una «quantità di sostanza biologica prelevata sulla persona sottoposta a tipizzazione del profilo del DNA». Il che dimostra come il legislatore abbia inteso riferirsi soltanto a elementi "organici".

[160] A ben vedere, si potrebbe ipotizzare un caso in cui l'impiego di un meccanismo di riconoscimento facciale rientri nella categoria degli "*accertamenti medici*": si allude all'ipotesi in cui esso serva quale strumento di *sentiment analysis* nell'ambito di una perizia psichiatrica, volta a individuare la presenza di un vizio di mente. Nondimeno, pure un'applicazione del genere della tecnologia *de qua* sarebbe da respingere, quantomeno fino a che non siano stabiliti presidi idonei ad assicurare che la stessa non vada a ledere la dignità umana. Per considerazioni analoghe, in materia di neuroscienze, cfr. C. Conti, *La prova scientifica*, in P. Ferrua, E. Marzaduri, G. Spangher (a cura di), *La prova penale*, Torino, 2013, pp. 101 s.

che altrimenti si disattenderebbe (nuovamente) la riserva di legge prevista dall'art. 13, co.2, Cost.[161].

8. Le occasioni perdute da parte della giurisprudenza penale italiana

Ancorché i *software* di riconoscimento facciale avrebbero dovuto avere uno spazio limitato nel sistema processuale penale italiano, bisogna, tuttavia, ammettere che le cose non sono andate così: essi sono applicati «su larga scala» da parte delle autorità di *law-enforcement*, che li hanno intesi come «un aiuto sempre più prezioso [specie] nelle indagini»[162].

Ebbene, per quanto qui rileva, va segnalato che tale scenario si è potuto realizzare, non solo (e non tanto) a causa di un difetto delle norme di legge, che come si è visto, se adeguatamente interpretate, avrebbero potuto fungere quantomeno da freno nei confronti di impieghi "spericolati" degli *AFRS*, ma soprattutto a causa del disinteresse dimostrato dalla Cassazione penale italiana per gli atteggiamenti antiformalistici tenuti dagli operatori in questa materia. Difatti, pur avendo avuto l'opportunità di pronunciarsi su aspetti importanti di SARI, la suprema Corte si è limitata a rigettare, in poche battute, i quesiti a lei sottoposti[163]; mentre

[161] Non a caso, la dottrina maggioritaria ritiene che l'art. 224-*bis* c.p.p. contenga un elenco tassativo di limitazioni della libertà personale: v., al riguardo, C. Gabrielli, sub *Art. 224*-bis, c.p.p., in G. Illuminati, L. Giuliani (a cura di), *Commentario breve al codice di procedura penale*, Padova, 2020, pp. 952 s., a cui si rimanda anche per ulteriori riferimenti dottrinali. Più in generale, l'opinione secondo cui, quando un'acquisizione probatoria incide direttamente su diritti fondamentali, non si può supplire alla mancanza di un'espressa regolamentazione invocando la disciplina prevista per casi più o meno simili, dal momento che, in caso contrario, si finirebbe per violare il corollario della legalità processuale, costituito da divieto di analogia *in malam partem*, è argomentata da C. Conti*, Accertamento del fatto*, cit., p. 166 e da O. Mazza, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2013, n. 3, pp. 9 s.

[162] Questa e la citazione precedente sono tratte da M. Valeri, *op. cit.*

[163] Ciò è, ad esempio, avvenuto in tema di utilizzo della piattaforma su istanza della difesa: sebbene, come accennato, la possibilità per i prevenuti di avvalersi *in favor* dei *facial recognition systems* costituisca un presidio essenziale rispetto al canone di parità delle parti, a fronte di una censura sul punto, il giudice nomofilattico si è limitato a rilevare che spetta ai singoli soggetti interessati «evidenziare analiticamente le ragioni dell'assoluta necessità del mezzo di prova da assumere in relazione al compendio istruttorio già

ha continuato a ribadire il proprio discutibile principio di diritto classico per cui il riconoscimento dell'imputato, ripreso in un filmato registrato da telecamere, compiuto dal personale di polizia giudiziaria, ha valore di indizio grave a suo carico, la cui valutazione è rimessa al giudice di merito[164].

Ora, vale la pena di rammentare che in altri Stati la giurisprudenza si è comportata diversamente[165]. Ciò è, ad esempio, avvenuto in Inghilterra e Galles, dove, una volta accertata l'inesistenza di una base giuridica idonea a regolare gli *AFRS*, la *Court of Appeal* ne ha censurato l'utilizzo[166]. Ma pure il *Conseil Constitutionnel* francese ha recentemente dimostrato una certa sensibilità avverso i rischi derivanti dagli strumenti di *reconnaissance faciale*, nel momento in cui ha ribadito la necessità di vietarne l'impiego sulle immagini captate dai droni, in ragione della compressione eccessiva del diritto alla *privacy* che altrimenti ne deriverebbe[167].

Né va tralasciato che un filone esegetico teso ad arginare i pericoli causati dalle tecnologie computazionali si è sviluppato anche in Italia, sebbene in rami dell'ordinamento diversi da quello penale: il riferimento va, in particolare, a quelle pronunce con cui il Consiglio di Stato[168]

formatosi nel caso concreto» (il rinvio va a Cass. pen., sez. IV, 18 giugno 2019, n. 39731, in *DeJure*). La piattaforma è citata anche Cass. pen., sez. I, 7 luglio 2020, n. 21823, *ivi*.

[164] Cfr., da ultimo, Cass. pen., sez. IV, 14 marzo 2022, n. 8428, in *DeJure*.

[165] In argomento, cfr. Q. Bu, *The global governance on automated facial recognition (AFR): ethical and legal opportunities and privacy challenges*, in *International Cybersecurity Law Review* 2 (2021), n. 1, pp. 120 ss.

[166] Si allude alla già menzionata sentenza *R (Bridges) – v – CC South Wales*, [2020] EWCA Civ 1058.

[167] Il riferimento va alla *Décision* n. 2021-834 DC del 20 gennaio 2022, § 54. Per contro, va segnalato che, di recente, il *Conseil d'État* si è dimostrato molto meno garantista, respingendo un ricorso, presentato dall'associazione *La Quadrature du Net*, volto a censurare l'impiego massivo del riconoscimento facciale da parte della polizia francese (*Décision* n. 442364 del 26 aprile 2022).

[168] Cfr. Cons. St., sez. VI, 4 febbraio 2020, n. 881, in *Riv. dir. process.,* 2021, p. 710; Cons. St., sez. VI, 13 dicembre 2019, n. 8474, in *DeJure*; Cons. St., sez. VI, 13 dicembre 2019, n. 8473, *ivi*; Cons. St., sez. VI, 13 dicembre 2019, n. 8472, in *Giur. it.* 2020, p. 1190, le quali hanno stabilito che «l'utilizzo di procedure informatizzate non può [in ogni caso] essere motivo di elusione dei princìpi che conformano il nostro ordinamento». Per ulteriori considerazioni in proposito si consenta il rinvio a J. Della Torre, *Le decisioni algoritmiche all'esame del Consiglio di Stato*, in *Riv. dir. process*., 2021, pp. 713 ss.

e la Cassazione civile[169] hanno stabilito una serie di salvaguardie per l'impiego "equo" degli algoritmi in ambito giuridico, valorizzando, in particolare, i canoni della trasparenza e della conoscibilità del loro funzionamento[170].

Com'era inevitabile, la mancata adozione anche da parte della giurisprudenza penale di garanzie analoghe[171] ha permesso alle autorità di *law enforcement* di perpetuare indisturbate le loro letture "securitarie", concernenti l'utilizzo di SARI anche per scopi investigativi e/o probatori. Il che dimostra, una volta di più, come, anche in Italia, i sistemi di riconoscimento facciale abbiano assunto quel preoccupante "volto oscuro", che si è avuto modo di descrivere in precedenza.

9. L'ultima frontiera: il riconoscimento facciale dopo la conversione del "decreto capienze"

Quanto finora affermato non deve far pensare che la politica italiana si sia sempre dimostrata insensibile nei confronti dei pericoli determinati dalle tecnologie di *face detection*.

La preoccupazione per un uso discriminatorio di questi sistemi e i rischi per la *privacy* a essi connessi ha portato alcuni parlamentari a presentare prima una serie di interrogazioni al Governo, finalizzate a ri-

[169] V. Cass. civ., sez. I, 25 maggio 2021, n. 14381, in *DeJure*.

[170] Uno *standard* particolarmente elevato sul punto è stato fissato dal Consiglio di Stato, il quale ha sostenuto che le esigenze di trasparenza della formula algoritmica dovrebbero considerarsi sempre prevalenti su quelle di riservatezza «delle imprese produttrici dei meccanismi informatici utilizzati» (cfr. Cons. St., sez. VI, 4 febbraio 2020, n. 881, cit., p. 711). Così facendo, i giudici italiani hanno delineato un livello di tutela maggiore rispetto a quanto fatto dalla Corte suprema del Wisconsin nel celebre caso *Loomis* (*State v. Loomis,* 881 NW 2d749 (WIS 2016), per un commento, v., per tutti, S. Quattrocolo, *op. ult. cit*., pp. 156 ss.), nella quale si è negato che l'impossibilità per un prevenuto di valutare l'attendibilità di un algoritmo, in ragione del fatto che esso si fondasse su un algoritmo brevettato e segreto, potesse costituire una lesione del diritto al *due process*.

[171] Per contro, è noto come i giudici penali nostrani siano ancora fermi nel dire che le esigenze di accertamento sottostanti al processo penale dovrebbero essere ritenute preminenti rispetto alla tutela della *privacy*: cfr., per tutte*,* Cass. pen., sez. II, 21 aprile 2017, n. 28367, in *DeJure*.

chiedere notizie circa l'effettivo funzionamento di SARI[172], e poi una proposta di legge, tesa a introdurre una secca moratoria nei confronti dell'installazione, da parte delle autorità pubbliche e di soggetti privati, di impianti di videosorveglianza "rafforzati" da sistemi di riconoscimento facciale[173]. È evidente come, così facendo, si sarebbe introdotto un divieto generale espresso, valevole anche per le autorità di *law enforcement*, di avvalersi di apparecchiature *live* di *facial recognition,* in attesa di un intervento legislativo, in grado di assicurarne la compatibilità con i diritti degli individui.

Le cose non sono, tuttavia, andate in questo modo: nel momento in cui si è trovato a convertire il cosiddetto "decreto capienze" (d.l. 8 ottobre 2021, n. 139, conv. con mod. dalla l. 3 dicembre 2021, n. 205), il Parlamento[174] ha ripreso la menzionata proposta di moratoria, introducendovi, però, una significativa eccezione, concernente proprio la materia penale. Più in particolare, l'art. 9, co.9, d.l. 139/2021 ha sì stabilito un divieto temporaneo, valido fino al 31 dicembre 2023 o fino all'adozione di un provvedimento specifico in materia, di installazione e di impiego di sistemi di riconoscimento facciale, in luoghi pubblici o aperti al pubblico. Tuttavia, il co. 12 della medesima disposizione ha, del pari, previsto che tale moratoria non si applichi ai «trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali […] in presenza, salvo che si tratti di trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali nonché di quelle giudiziarie del pubblico ministero, di parere favorevole del Garante» della *privacy*.

Sin da un primo sguardo, ci si renderà conto di come, specie in ragione del linguaggio giuridico sconnesso, la nuova disciplina risulti di difficile lettura. Ciò che è certo è che il macchinoso congegno distingue

---

[172] Cfr., ad esempio, la già citate interrogazioni presentate dall'On. Sensi, n. 3-02074 e dall'On. Ceccanti e altri n. 5-03432.

[173] Ci si riferisce alla proposta di legge A.C. n. 3009, d'iniziativa dei Deputati Sensi e a., presentata il 12 aprile 2021.

[174] La modifica è frutto dell'approvazione dell'emendamento 9.100/64 (testo 3), d'iniziativa dei Senatori Ferrari e Valente, approvato al Senato in sede referente. A ben vedere, i proponenti avevano, nel corso dei lavori preparatori, presentato anche iniziative più garantiste di quella approvata, tra cui l'emendamento 9.100/64, il quale aveva ripreso *in toto* la proposta di legge C. n. 3009.

l'ipotesi in cui gli strumenti in esame siano utilizzati dalle forze di polizia, da quella in cui essi siano attivati per iniziativa della magistratura. Mentre, infatti, nella prima fattispecie si prevede la necessità di un previo parere favorevole del Garante, affinché possa operare la deroga al divieto generale, per i giudici e gli accusatori siffatta autorizzazione amministrativa non è in alcun modo richiesta[175].

Il principale problema da risolvere sta, tuttavia, nel comprendere l'effettiva portata da attribuire all'art. 9, co.12, del "decreto capienze".

Una prima esegesi possibile – già sostenuta in via ufficiale dalle forze di polizia – è quella di interpretare tale previsione, non solo come un'eccezione alla moratoria generale di impiego dei *AFRS*, ma soprattutto quale forma di autorizzazione *implicita* "in bianco" a utilizzare SARI, anche in modalità *real-time*, per scopi di prevenzione e di repressione della criminalità in luoghi pubblici e aperti al pubblico[176]. In altri termini, si è ritenuto che il Parlamento, stabilendo che il divieto di installare e di usare impianti di videosorveglianza con riconoscimento facciale non abbia valore per determinate istituzioni, deputate al contrasto delle attività illecite, abbia voluto, *a contrario*, consentire alle medesime di avvalersene in piena libertà in tali spazi[177], salva la presenza, per le sole forze di polizia, dell'autorizzazione del Garante[178].

Il punto, tuttavia, è che, se così intesa, la nuova norma finirebbe per esporsi a inevitabili profili di illegittimità costituzionale.

Sotto un primo profilo, la stessa non rispetterebbe il già citato rigido

[175] In questo senso si esprime anche il *dossier* n. 465/1 del Senato e della Camera, del 18 novembre 2021, esplicativo del A.S. n. 2409, reperibile in *www.senato.it*, p. 73.

[176] Cfr. l'articolo di M. Valeri, *op. cit.*, ove, non a caso, si afferma che è in corso di valutazione la possibilità di presentare «una nuova interrogazione al Garante, alla luce dei recenti risvolti normativi, così che possa esprimere parere positivo all'utilizzo del Sari *real time*».

[177] Per contro, rimarrebbero, in ogni caso, ancora inutilizzabili le immagini riprese in luoghi coperti dalla libertà di domicilio, stante la mancata attuazione della riserva di legge di cui all'art. 14 Cost.

[178] Il rischio di una tale lettura è paventato anche dall'associazione a tutela dei diritti umani *Privacy Network*, la quale nel comunicato stampa *Italia – Moratoria sul riconoscimento facciale*, in *www.privacy-network.it*, 2 dicembre 2021, ha affermato che «se […] queste ipotesi sono esplicitamente fatte salve dalla moratoria […] la conclusione naturale è che l'uso di questi sistemi deve ritenersi lecito proprio sulla base di questa legge».

vaglio di proporzionalità (in astratto e in concreto) imposto dagli artt. 7, 8 e 52 della Carta di Nizza, nonché dall'art. 10 della direttiva 2016/680/UE, quale requisito essenziale per il legittimo trattamento di dati biometrici, idonei a identificare in modo univoco una persona fisica. D'altra parte, la nuova norma non stabilisce neppure che la tecnologia possa essere utilizzata solo per reati di una certa gravità e unicamente laddove ciò sia strettamente necessario.

In seconda battuta, la previsione non sarebbe neppure idonea a rispettare le condizioni stringenti a cui l'art. 13 Cost. – da intendersi nel senso estensivo sopra delineato – subordina la possibilità di restringere la libertà dell'individuo. Difatti, l'art. 9, co.12, d.l. 139/2021 nulla dice circa i *casi* e i *modi* in cui le forze di polizia o la magistratura possono avvalersi dei sistemi di riconoscimento facciale automatico; né specifica alcuna garanzia a salvaguardia dei diritti e delle libertà della persona.

L'esigenza di fugare i menzionati profili di frizione con i principi fondamentali porta, dunque, a preferire una seconda lettura, costituzionalmente orientata del *novum*. A uno sguardo attento, ci si renderà conto di come il menzionato art. 9, co.12, del "decreto capienze" possa essere inteso quale regola volta a ribadire che, anche al netto della moratoria nei confronti degli *AFRS*, le autorità di *law enforcement* possono continuare ad avvalersene, ma ciò nei *soli casi* e *con i limiti* consentiti dalle fonti sovraordinate e dal codice di rito. Tale tesi trova, d'altra parte, conferma anche in un preciso argomento logico-sistematico: non sfuggirà, invero, che intendere la previsione nel senso "liberalizzante" sopra delineato produce l'effetto di stravolgere la *ratio* dichiarata dell'intervento del Parlamento, che è stata quella di limitare l'impiego della tecnologia in esame, onde meglio salvaguardare i diritti della persona[179]. Ne deriva, pertanto, che, in assenza di un chiaro intento contrario del legislatore, la stessa non possa essere qualificata come regola implicitamente idonea ad aprire le porte dell'ordinamento a siffatti mezzi, tanto più in un settore così delicato quale quello penale.

Ebbene, è chiaro che, se interpretata in questo senso, l'eccezione al divieto nei confronti della forma di IA in questione viene ad assumere un significato molto meno "rivoluzionario": essa produce l'effetto

[179] La stessa è ben espressa nell'intervento dell'On. Romano, in Atti Camera, Resoconto stenografico dell'Assemblea, seduta n. 605, 29 novembre 2021, in *www.camera.it*.

di confermare che, anche al netto della moratoria inserita nel "decreto capienze", risulta possibile per le forze di polizia e per l'autorità giudiziaria continuare a utilizzare SARI solo quale ausilio alle operazioni di identificazione *ex* art. 349 c.p.p. Per converso, il suo impiego quale forma di individuazione/ricognizione algoritmica e a maggior ragione quello *real-time*, non essendo ancora stati regolati nei casi e nei modi dalla legge, rimane ancora impedito dalla barriera dell'art. 189 c.p.p., rafforzata dall'insieme già citato di norme, poste a tutela della libertà morale dell'individuo.

Non sfuggirà come, leggendo nel *novum* una mera conferma dell'esistente, le ombre di incostituzionalità sopra descritte vengano a diradarsi radicalmente; e ciò in quanto tale esegesi è idonea a far sì che gli impieghi più insidiosi dei *tools* – perché in grado di invadere in modo maggiormente incisivo la sfera giuridica dei singoli – continuino a non essere ammessi, fino all'adozione di una disciplina puntuale da parte del legislatore.

10. Considerazioni conclusive

Anche se risulta possibile disinnescare in via esegetica il pericolo di un'apertura indiscriminata dell'ordinamento processuale penale italiano al riconoscimento facciale di massa, il giudizio su quanto fatto dalla l. 205/2021 non può che essere negativo.

Per quanto concerne il metodo, è indubbio che il contesto della conversione di un d.l. – viste le cadenze temporali oltremodo ristrette che ne caratterizzano l'approvazione – non era certo quello adatto per regolare mezzi computazionali complessi quali quelli in esame.

A livello di merito, il quadro si fa ancora più fosco: resta, infatti, l'impressione di una novella che, nella migliore delle ipotesi, sarà idonea a lasciare inalterato il già critico *status quo ante*, mentre, nella peggiore – ovvero nel caso in cui prendesse piede la menzionata lettura "liberalizzante" dell'uso del riconoscimento facciale – potrà persino favorirne una diffusione ancor più bulimica nel sistema.

A fronte di uno scenario tanto critico, si sarebbe persino portati a concludere amaramente che il Parlamento avrebbe fatto meglio ad astenersi dal dettare qualsiasi moratoria in tema di impiego di *facial recognition*

systems. D'altra parte, è indubbio che l'ambito più delicato e invasivo in cui tali mezzi possono operare è proprio quello penale, ove, tuttavia, vale la "caotica" eccezione al divieto d'uso di cui si è detto[180].

Ciò conferma, una volta di più, che il problema del rapporto tra *AFRS* e processo penale richiede di essere affrontato sì con urgenza, ma tramite un intervento normativo meditato. Un intervento che, tenuto conto degli indiscutibili vantaggi che tali meccanismi possono avere in termini di efficienza complessiva del sistema, non persegua l'obiettivo di bandirli del tutto[181], ma che stabilisca una chiara base normativa per un loro impiego in conformità alle garanzie fondamentali dell'uomo. Il che significa precisare, in modo rigoroso, almeno i seguenti aspetti: 1) le modalità di popolazione dei *database*, contenenti le immagini di raffronto impiegate dagli algoritmi; 2) i presidi necessari ad assicurare la qualità dei dati raccolti e la loro conservazione solo per tempi definiti; 3) le tutele idonee a garantire la trasparenza dei *software* utilizzati, il loro periodico aggiornamento agli *standard* tecnologici più avanzati, nonché volte a far sì che essi siano "allenati" in modo da evitare effetti discriminatori; 4) la possibilità per l'autorità di avvalersi dei *tools* solo per reati di una certa gravità e previa autorizzazione specifica di un giudice o di un'autorità amministrativa indipendente; 5) i casi di attivazione delle operazioni di riconoscimento in favore della difesa; 6) l'indispensabilità di un controllo umano *effettivo* sui risultati forniti dalla macchina[182].

Se si volge poi lo sguardo più in generale, quanto è avvenuto in merito al riconoscimento facciale dimostra come sia indispensabile imbastire un serio cantiere di riforme, teso a introdurre una disciplina specifica delle

[180] Nondimeno, va riconosciuto che la norma di recente approvazione produce l'effetto utile di vietare espressamente l'attività di installazione in luoghi pubblici di strumenti di video-sorveglianza con riconoscimento facciale da parte degli Enti locali, già censurata dal Garante della *privacy* in alcune occasioni: cfr., ad esempio, il provvedimento del 26 febbraio 2020, doc. web n. 9309458.

[181] In termini analoghi, v. anche M. Torre, *op. cit*., p. 1054.

[182] Visto il pericolo che la macchina si comporti come una *black box*, rendendo poco effettivo il vaglio dell'agente umano, sarebbe auspicabile anche l'inserimento di un criterio di valutazione, teso a stabilire che il *match* del *software* non possa costituire prova "unica e determinate" per la condanna di un prevenuto. Per parte loro, G. Contissa, G. Lasagni, G. Sartor, *op. cit*., p. 633, onde risolvere il problema dell'imprevedibilità dell'IA, propongono di «introdurre nel processo penale il diritto a far riesaminare le valutazioni generate da un sistema A/IA da un altro sistema automatizzato».

molteplici forme di sorveglianza elettronica impiegate nel nostro Paese. Com'è ben noto, a fronte dell'importanza strategica assunta dalle moderne tecnologie del controllo, l'ordinamento processuale italiano risulta ancora affetto da previsioni datate e da gravissime lacune normative[183], non essendo stati regolati – in spregio al canone, di portata costituzionale, di legalità processuale (art. 111, co.1, Cost.) – neppure istituti classici come le semplici videoriprese investigative[184]. Onde rimediare a siffatte problematiche, rese ancora più gravi dall'atteggiamento securitario mantenuto tradizionalmente dalla giurisprudenza penale interna, è necessario smetterla di farsi ipnotizzare dal "canto delle sirene"[185] dei *big data*: la sfida ineludibile per i prossimi anni deve essere quella di costruire un "*algorithimic due process*"[186], fondato sulle salvaguardie, specificamente tarate sul funzionamento degli algoritmi e dall'IA[187], racchiuse nelle

[183] Cfr., al riguardo, *ex multis*, G. Di Paolo, *op. cit*., p. 264 e, più di recente, F. Nicolicchia, *op. cit*. Merita precisare che tali rilievi sono validi anche a "valle" della l. 27 settembre 2021, n. 134, la quale, pur avendo favorito una marcata digitalizzazione del procedimento (cfr., anche per ulteriori riferimenti dottrinali, F. Del Vecchio, *Prospettive e tempi della digitalizzazione del processo*, in *Processo penale e giustizia,* 2022, n. 1, pp. 8 ss.; B. Galgani, *Il processo penale in "ambiente" digitale: ragioni e (ragionevoli) speranze*, in *Questione giustizia*, 2021, n. 4, pp. 181 ss., nonché, volendo, M. Gialuz, J. Della Torre, *Giustizia per nessuno. L'inefficienza del sistema penale italiano tra crisi cronica e riforma Cartabia*, Torino, 2022, pp. 293 ss.), non ha colto l'occasione per colmare le lacune ataviche esistenti in quest'ambito. Ciò nondimeno, ci pare che un ruolo propulsivo chiave potrà averlo il Comitato tecnico-scientifico per la digitalizzazione della giustizia penale, di cui proprio l'art. 2, co.20, della l. 134/2021 ha previsto la possibile istituzione.

[184] Sul tema, com'è noto, la letteratura è sconfinata: per reperire i dovuti riferimenti dottrinali, cfr. V. Bonini, *op. cit*., p. 338; N. Triggiani, *Le videoriprese investigative e l'uso dei droni*, in A. Scalfati (a cura di), *Le indagini atipiche*, cit., p. 161, oltre alla voce di A. Camon, *Captazione di immagini (diritto processuale penale)*, in *Enc. Dir. – Annali*, VI, Milano, 2013, pp. 133 ss.

[185] Cfr. G. Di Chiara, *Il canto delle sirene. Processo penale e modernità scientifico-tecnologica: prova dichiarativa e diagnostica della verità*, in *Criminalia*, 2007, p. 19.

[186] Per l'impiego di tale espressione, v. E. Israni, E. Chang, *Algorithmic Due Process: Mistaken Accountability and Attribution in* State v. Loomis, in *www.jolt.law.harvard.edu*, 31 agosto 2017.

[187] Non a caso, la dottrina più accorta richiede, da tempo, la creazione di una "nuova procedura penale", costruita tenendo conto delle sfide poste dalle moderne società dell'infosfera: cfr., in questo senso, il saggio di O.S. Kerr, *Digital Evidence and the New Criminal Procedure*, in *Columbia Law Review*, 2005, pp. 279 ss.

sempre più numerose Carte dei diritti europee proclamate in materia. Solo in questo modo sarà, invero, possibile cogliere le opportunità offerte dagli applicativi digitali, senza con ciò rischiare che essi – come nelle più cupe opere di fantascienza – finiscano per produrre frutti avvelenati.

Bibliografia

A. Adensamer, L.D. Klausner, "*Part Man, Part Machine, All Cop": Automation in Policing*, in *Frontiers in Artificial Intelligence*, 4 (23 giugno 2021).

T. Alesci, *Corpo dell'imputato (fonte di prova nel processo penale)*, in *Digesto Pen. – Agg*., X, Torino, 2018, p. 76.

G. Alpa (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020.

M. Balkin, *The Three Laws of Robotics in the Age of Big Data*, in *Ohio State Law Journal* 78 (2017), n. 5, p. 1217.

N. Balossino, S. Siracusa, *L'identificazione basata sul volto: metodi fisionomici e metrici*, in *Security Forum*, Bergamo, 2004, reperibile in *www.docplayer.it.*

P. Barile, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984.

G. Barone, *Intelligenza artificiale e processo penale: la linea dura del Parlamento europeo. Considerazioni a margine della risoluzione del Parlamento europeo del 6 ottobre 2021*, in *Cass. pen*., 2022, p. 1180.

F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Diritto penale contemporaneo – Archivio web*, 29 settembre 2019.

A. Bernasconi, *La ricognizione di persone nel processo penale. Struttura e procedimento probatorio*, Torino, 2003.

A. Bernasconi, *Il riconoscimento fotografico curato dalla polizia giudiziaria*, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2014, p. 167.

A. Bertillon, *Identification anthropométrique. Instructions signalétiques*, Melun, 1892.

A. Bertillon, *La photographie judiciaire. Avec un appendice sur la classification et l'identification anthropométriques*, Parigi, 1890.

C. Blacklaws, *Algorithms: transparency and accountability*, in *Philosophical Transactions of the Royal Society* 376 (2018), pp. 1 ss.

V. Bonini, *Videoriprese investigative e tutela della riservatezza: un binomio che richiede sistemazione legislativa*, in *Processo penale e giustizia*, 2019, n. 2, p. 338.

A. Bonomi, *Libertà morale e accertamenti neuroscientifici: profili costituzionali*, in *BioLaw Journal – Rivista di biodiritto*, 2017, n. 3, p. 142.

M. Bontempelli, *La ricognizione nel processo penale*, Torino, 2012.

C. Bonzano, *Gli accertamenti medici coattivi. Legalità e proporzionalità nel regime della prova*, Padova, 2017.

G. Borgia, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, in *www.lalegislazionepenale.eu*, 11 dicembre 2021.

Q. Bu, *The global governance on automated facial recognition (AFR): ethical*

and legal opportunities and privacy challenges, in *International Cybersecurity Law Review* 2 (2021), n. 1, pp. 120 ss.

C. Burchard, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *Riv. it. dir. proc. pen.,* 2019, p. 1908.

A. Cabiale, *I limiti alla prova nella procedura penale europea*, Milano, 2019.

M. Caianiello, *Dangerous Liaisons. Potentialities and Risks Deriving from the Interaction between Artificial Intelligence and Preventive Justice*, in *European Journal of Crime, Criminal Law and Criminal Justice* 29 (2021), n. 1, pp. 1 ss.

A. Camon, *Captazione di immagini (diritto processuale penale)*, in *Enc. Dir. – Annali*, VI, Milano, 2013, p. 133.

A. Camon, *Le sezioni unite sulla videoregistrazione come prova penale: qualche chiarimento e alcuni dubbi nuovi*, in *Riv. it. dir. proc. pen*., 2006, p. 1550.

A.M. Capitta, *Ricognizioni e individuazioni di persone nel diritto delle prove penali*, Milano, 2001.

F. Caprioli, *Riprese visive nel domicilio e intercettazione per immagini*, in *Giur. cost*., 2002, p. 2176.

S. Cavini, *Le ricognizioni e i confronti*, Milano, 2015.

G. Cecanese, *Aspetti problematici e snodi interpretativi dell'individuazione di persone e di cose*, in *Archivio penale – Rivista web*, 2018, n. 1.

G. Cecanese, *Confronto, ricognizione ed esperimento giudiziale nella logica dei mezzi di prova*, Napoli, 2013.

G. Conso-G. Giostra (a cura di), *La disciplina del prelievo biologico coattivo, alla luce della l. 30 giugno 2009, n. 85*, in *Giur. it.,* 2010, p. 1217.

C. Conti, *Accertamento del fatto e inutilizzabilità nel processo penale*, Padova, 2007.

C. Conti, *La prova scientifica*, in P. Ferrua, E. Marzaduri, G. Spangher (a cura di), *La prova penale*, Torino, 2013, p. 87.

G. Contissa, F. Galli, F. Godano, G. Sartor, *La nuova Proposta di Regolamento europeo sull'intelligenza artificiale: questioni giuridiche e approcci regolatori*, in R. Brighi (a cura di), *Nuove questioni di informatica forense*, Roma, 2022, p. 387.

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, n. 4, p. 619.

F. Cordero, *Ideologie del processo penale*, Milano, 1966.

F. Cordero, *Procedura penale*, Milano, 1987.

E. Currao, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *Dir. pen. e uomo*, 19 maggio 2021.

D. Curtotti, *Rilievi ed accertamenti tecnici*, Padova, 2013.
M. Daniele, *Indagini informatiche lesive della riservatezza. Verso un'inutilizzabilità convenzionale?*, in *Cass. pen*., 2013, p. 367.
J. Della Torre, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della* High Court of Justice, in *Diritto penale contemporaneo – Rivista trimestrale*, 2020, n. 1, p. 231.
J. Della Torre, *Le decisioni algoritmiche all'esame del Consiglio di Stato*, in *Riv. dir. process.*, 2021, p. 713.
F. Del Vecchio, *Prospettive e tempi della digitalizzazione del processo*, in *Proc. penale e giustizia,* 2022, n. 1, p. 8.
G. Di Chiara, *Il canto delle sirene. Processo penale e modernità scientifico-tecnologica: prova dichiarativa e diagnostica della verità*, in *Criminalia*, 2007, p. 19.
F.R. Dinacci, *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia: luci europee e ombre legislative*, in *Processo penale e giustizia*, 2022, n. 2, p. 310.
F.R. Dinacci, *Neuroscienze e processo penale: il ragionamento probatorio tra chimica valutativa e logica razionale*, in *Processo penale e giustizia*, 2016, n. 2, p. 1.
G. Di Paolo, *Tecnologie del controllo e prova penale. L'esperienza statunitense e spunti per la comparazione*, Padova, 2008.
O. Dominioni, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Milano, 2005.
S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020.
C. Fanuele, *La libertà personale*, in F.R. Dinacci (a cura di), *Processo penale e Costituzione*, Milano, 2010, p. 209.
P. Felicioni, *Il riconoscimento del parlante tra prassi e modelli normativi*, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2019, p. 259.
L. Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Milano, 2022.
L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017.
L. Floridi, *La rivoluzione dell'informazione*, Torino, 2012.
L. Floridi, J.W. Sanders, *On the Morality of Artificial Agents*, in *Minds and Machines*, 2004, p. 349.
C. Gabrielli, *Il prelievo coattivo di campioni biologici nel sistema penale*, Torino, 2012.
B. Galgani, *Giudizio penale,* habeas data *e garanzie fondamentali*, in *Archivio penale – Rivista web*, 2019, n. 1.

B. Galgani, *Il processo penale in "ambiente" digitale: ragioni e (ragionevoli) speranze*, in *Questione giustizia*, 2021, n. 4, p. 181.

L. Garlati, *Alle origini della prova scientifica: la scuola di polizia di Salvatore Ottolenghi*, in *Revista brasileira de Direito processual penal*, 2021, p. 885.

C. Garvie, *Garbage in, garbage out. Face recognition on flawed data*, in *www.flawedfacedata.com*, 16 maggio 2019.

M. Gialuz, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in Aa.Vv, *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, p. 51.

M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Diritto penale contemporaneo – Archivio web*, 29 maggio 2019.

M. Gialuz, J. Della Torre, *Giustizia per nessuno. L'inefficienza del sistema penale italiano tra crisi cronica e riforma Cartabia*, Torino, 2022.

G. Giostra, *I mali della libertà di stampa si curano solo con più libertà*, in *DDl Alfano: se lo conosci lo eviti*, Roma, 2009, p. 101.

P.F. Grossi, *Libertà personale, libertà di circolazione ed obbligo di residenza dell'imprenditore fallito*, in *Giur. cost*., 1962, p. 200.

E. Israni, E. Chang, *Algorithmic Due Process: Mistaken Accountability and Attribution in* State v. Loomis, in *www.jolt.law.harvard.edu*, 31 agosto 2017.

B. Keenan, *Automatic Facial Recognition and the Intensification of Police Surveillance*, in *Modern Law Review* 84 (2021), n. 4, p. 886.

O.S. Kerr, *Digital Evidence and the New Criminal Procedure*, in *Columbia Law Review* 105 (2005), n. 1, p. 279.

G. Lasagni, G. Contissa, *Making Criminal Procedure Rights Computable*, in Contissa, G. Lasagni, M. Caianiello, G. Sartor (a cura di), *Effective Protection of the Rights of the Accused in the EU Directives. A Computable Approach to Criminal Procedure Law*, Leiden-Boston, 2022, p. 42.

M. Leta Jones, *The right to a human in the loop: Political constructions of computer automation and personhood*, in *Social Studies of Science* 47 (2017), n. 2, p. 216.

E. Li, *Europe's Next Steps in Regulating Facial Recognition Technology*, in *Columbia Journal of Transnational Law – Bullettin Blogposts*, 7 novembre 2021.

R. Lopez, *La rappresentazione facciale tramite* software, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2019, p. 239.

R. Lopez, *Riconoscimento facciale tramite* software *e individuazione del sospettato*, in A. Scalfati (a cura di), *Pre-investigazioni (Espedienti e mezzi)*, Torino, 2020, p. 295.

L. Lupária, *Artificial Intelligence in Criminal Courts. Opportunity or Threat?*,

in A.M. Lopez Rodriguez, M.D. Green, M.K. Kubica (a cura di), *Legal Challenges in the New Digital Age*, Leiden, 2021, p. 160.

L. Lupária, Data retention e *processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Diritto di internet*, 2019, p. 758.

L. Lupária, Privacy, *diritti della persona e processo penale*, in *Riv. dir. process.*, 2019, p. 1448.

V. Manes, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, p. 547.

L. Marafioti, L. Lupária (a cura di), *Banca dati del DNA e accertamento penale*, Milano, 2010.

A. Marandola, *L'identificazione fotografica*, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2019, p. 209.

S. Marcolini, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.*, 2015, p. 760.

E. Masini, *Sacro arsenale ovvero Prattica dell'officio della Santa Inquisizione, Seconda Parte, Del modo di formare i processi, e essaminare Testimoni, e Rei*, Bologna, 1665.

O. Mazza, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2013, n. 3, p. 4.

A. McStay, *Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy*, in *Big Data & Society*, 2020, p. 1.

H.-W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, G. De Gregorio (a cura di), *Constitutional Challenges in the Algorithmic Society*, Cambridge, 2021.

G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021.

A. Najibi, *Racial Discrimination in Face Recognition Technology*, in *www.sitn.hms.harvard.edu*, 24 ottobre 2020.

R. Nania, *Appunti per un bilancio sulla libertà individuale nella esperienza costituzionale italiana*, in R. Nania (a cura di), *L'evoluzione costituzionale delle libertà e dei diritti fondamentali. Saggi e casi di studio*, Torino, 2012, p. 3.

D. Negri, *Compressione dei diritti di libertà e principio di proporzionalità*, in *Diritti della persona e nuove sfide del processo penale*, Milano, 2019, p. 55.

I. Neroni Rezende, *Facial recognition in police hands: Assessing the "Clearview case" from a European perspective*, in *New Journal of European Criminal Law*, 2020, n. 3, p. 375.

J. Nieva-Fenoll, *Intelligenza artificiale e processo*, Torino, 2019.

S. Ottolenghi, *Il segnalamento del delinquente in servizio della polizia giudiziaria*, Palermo, 1889.

U. Pagallo, *Algoritmi e conoscibilità*, in *Rivista di filosofia del* diritto, 2020, n. 1, p. 93.

F. Paolucci, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *Media Laws – Rivista di diritto dei Media*, 2021, n. 1, p. 204.

L. Parlato, *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale*, in *Proc. pen. giust*., 2020, p. 291.

N. Pascucci, *La natura controversa della ricognizione fotografica*, in *Riv. it. dir. proc. pen*., 2017, p. 287.

N. Pascucci, *Un nodo ancora da sciogliere nel processo penale: il riconoscimento informale di persona in udienza*, in *Dir. pen. proc*., 2018, p. 721.

P.P. Paulesu, *Intelligenza artificiale e giustizia penale. Una lettura attraverso i principi,* in *Archivio penale – Rivista web*, 2022, n. 1.

A. Pin, "*A novel and controversial technology". Artificial face recognition, privacy protection and algorithm bias in Europe,* in *William & Mary Bill of Rights Journal* 30 (2021-2022), n. 2, p. 291.

A. Presutti, *L'acquisizione forzosa dei dati genetici tra adempimenti internazionali e impegni costituzionali*, in *Riv. it. dir. proc. pen*., 2010, p. 545.

J. Purshouse, L. Campbell, *Automated facial recognition and policing: A Bridge too far?*, in *Legal Studies* 42 (2022), n. 2, p. 209.

S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Cham, 2020.

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, n. 2, p. 107.

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.eu*, 18 dicembre 2018.

S. Quattrocolo, *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *Media laws – Rivista di diritto dei Media*, 2020, n. 3, p. 127.

T. Rafaraci, *Verso una* law of evidence *dei dati*, in *Dir. pen. proc*., 2021, p. 853.

S. Rodotà, *Il mondo nella rete. Quali i dritti, quali i vincoli*, Roma, 2014.

S. Rodotà, *Trasformazioni del corpo*, in *Politica dir*., 2006, p. 3.

U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020.

E. Sacchetto, Face to face: *il complesso rapporto tra* automated facial rec-

ognition technology *e processo penale*, in *www.lalegislazionepenale.eu*, 16 ottobre 2020.

E. Sacchetto, *Spunti per una riflessione sul rapporto tra biometria e processo penale*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2019, n. 2, p. 465.

L. Saponaro, *Le nuove frontiere tecnologiche dell'individuazione personale*, in *Archivio penale – Rivista web*, 2022, n. 1.

L. Scomparin, *La tutela del testimone nel processo penale*, Padova, 2000.

S. Signorato, *Giustizia penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo*, in *Riv. dir. process.*, 2020, p. 605.

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. process.*, 2021, p. 101.

S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018.

C. Slogobin, *Public privacy: camera surveillance of public places and the right to anonymity*, in *Mississippi Law Journal* 72 (2002), n. 1, pp. 213 ss.

P. Tonini, *La Cassazione accoglie i criteri* Daubert *sulla prova scientifica,* in *Dir. pen. proc.*, 2011, p. 1341.

P. Tonini, C. Conti, *Il diritto delle prove penali*, Milano, 2014.

M. Torre, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Dir. pen. proc*., 2021, p. 1042.

N. Triggiani, *Le videoriprese investigative e l'uso dei droni*, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2019, p. 161.

G. Ubertis, *Argomenti di procedura penale*, II, Milano, 2006.

G. Ubertis, *Intelligenza artificiale e diritto penale*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2020, n. 4, pp. 75 ss. (ora anche in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, pp. 9 ss.)

M. Valeri, *Mettiamoci la faccia*, in *www.poliziamoderna.poliziadistato.it*, 9 marzo 2022.

R.V.O. Valli, *Sull'utilizzabilità processuale di Sari: il confronto automatizzato di volti rappresentati in immagini*, in *ilPenalista*, 16 gennaio 2019.

G. Varraso, *Neuroscienze e consulenza "investigativa"*, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2019, p. 343.

G. Vassalli, *Il diritto alla libertà morale. Contributo alla teoria dei diritti della personalità*, in Id., *Scritti giuridici*, III, *Il processo e le libertà*, Milano, 1997, p. 253.

R.A. Waelen, *The struggle for recognition in the age of facial recognition technology*, in *AI and Ethics*, 2022.

C. WENDEHORST, Y. DULLER, *Biometric Recognition and Behavioural Detection. Study Requested by the JURI and PETI committees*, Bruxelles, 2021.

M. ZALNIERIUTE, *Burning* Bridges: *The Automated Facial Recognition Technology and Public Space Surveillance in The Modern State*, in *The Columbia Science & Technology Law Review* 22 (2021), n. 2, p. 243.

DIFENDERSI DALL'INTELLIGENZA ARTIFICIALE O DIFENDERSI CON L'INTELLIGENZA ARTIFICIALE?

VERSO UN CAMBIO DI PARADIGMA

Giulia Lasagni

1. Introduzione

Nell'ultimo decennio, algoritmi e intelligenza artificiale (d'ora in avanti, IA) hanno conquistato un ruolo imprescindibile nelle attività di accertamento e prevenzione dei reati. Dalla predeterminazione delle aree più a rischio per la commissione di specifici reati al riconoscimento facciale, dall'esame delle prove digitali alla (presunta) possibilità di verificare la genuinità delle prove dichiarative o di misurare il tasso di recidiva: le applicazioni di queste tecnologie sono ormai decisamente diffuse, così come il dibattito dottrinale e giurisprudenziale che ne analizza limiti e potenzialità[1].

[1] Su cui si vedano, *ex multis*, S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings*. *A Framework for A European Legal Discussion*, Cham, 2020; U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020; M. Gialuz, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, pp. 51 ss.; M. Caianiello, *Dangerous Liaisons. Potentialities and risks deriving from the interaction between Artificial Intelligence and preventive justice*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2021, n. 1, pp. 1 ss.; A.

Spesso, però, la prospettiva a partire dalla quale questi temi sono affrontati, sia da parte di chi sviluppa sistemi di IA, sia da parte di chi li esamina in modo critico, si rivela monodirezionale, e cioè focalizzata essenzialmente sull'impiego delle tecnologie automatizzate a supporto delle funzioni inquirenti.

Da un lato, lo spaccato è comprensibile, considerando la varietà di *tools* investigativi e la gravità degli interrogativi da essi sollevati. Al tempo stesso, tuttavia, l'impostazione mostra anche i limiti di un approccio tendenzialmente "di rimessa" nei confronti delle sfide tecnologiche che stanno investendo il sistema della giustizia penale.

Detto altrimenti: mentre cittadini e giuristi sono (fortunatamente) sempre più consapevoli dei vantaggi e dei rischi causati da indagini scientificamente avanzate, il potenziale di sviluppo delle tecnologie automatizzate per rafforzare i diritti di difesa resta ad oggi in gran parte inesplorato. Ciò, da una parte, tende a fornire una immagine incompleta e talvolta distorta dei sistemi di IA in ambito penale; dall'altra, a non stimolare l'espansione di questi strumenti su fronti applicativi diversi ed innovativi.

Le considerazioni del presente contributo prendono le mosse proprio da questa asimmetria, per tentare di delineare una visione più ampia dell'apporto di algoritmi e IA in una materia tanto delicata come quella penale.

In tale ottica, quindi, qui non si affronteranno le problematiche tipiche dei sistemi IA, già da tempo evidenziate da dottrina e organizzazioni sovranazionali, quali, ad esempio, la limitata trasparenza[2], la mancanza di *explainability*[3] o il rischio di discriminazione insito nell'utilizzo di

---

M. Maugeri, *L'uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra* evidence based practices *e tutela dei diritti fondamentali,* in *Archivio penale – Rivista web*, 2021, n. 1, pp. 1 ss.

[2] Cfr., *ex multis*, M. Brkan, *Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond*, in *International Journal of Law and Information Technology*, 2019, n. 2, p. 113.

[3] Su cui, per tutti, V. Manes, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia,* in U Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, cit., pp. 551 ss.; S. Quattrocolo, *Artificial Intelligence,* cit., pp. 93 ss.; F. Palmiotto, *The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, in M. Ebers, M. Cantero Gamito (a cura di), *Algorith-*

data set e procedure di *training* caratterizzati da *bias*[4]. Dando per scontate suddette criticità, si assumerà invece la prospettiva del difensore, per cercare di determinare quali sfide e quali opportunità si aprono oggi a fronte dell'impiego crescente di tecnologie automatizzate.

L'analisi esaminerà dapprima alcune possibilità di interpretare i diritti difensivi, ed in particolare il diritto al rimedio effettivo, in modo adeguato a garantire una protezione efficace a fronte di indagini (parzialmente) automatizzate (§ 2).

In secondo luogo, si vedrà come algoritmi e IA possano già essere impiegati per potenziare le risorse e le capacità conoscitive del difensore, rafforzandone le strategie processuali e cercando di ridurre l'asimmetria che tradizionalmente caratterizza il rapporto fra accusa e difesa, specialmente in procedimenti transnazionali (§ 3). A tal fine, peraltro, è opportuno ricordare come riscontrare un carattere di "transnazionalità" oggi sia molto più frequente che in passato: si pensi alla ampia gamma di casi nei quali è necessario ricorrere alla collaborazione di un *service provider* per ottenere prove digitali o, almeno nel contesto dell'Unione, a provvedimenti di cooperazione giudiziaria come il mandato di arresto europeo o l'ordine europeo di indagine penale.

Infine, si forniranno alcuni spunti ancora più promettenti per lo sviluppo di strategie difensive innovative. In altre parole, si discuterà di come, volendolo, le tecnologie automatizzate possano portare ad un innalzamento del livello di tutela dei diritti fondamentali, migliorando taluni aspetti del procedimento penale attualmente caratterizzati da una protezione tendenzialmente limitata delle prerogative difensive (§ 4). Sebbene ancora in gran parte sperimentale, questo ultimo passaggio getta le basi per un cambio di paradigma che appare sempre più necessario nel modo di concepire il ruolo del difensore nell'attuale contesto tecnologico.

---

mic Governance and Governance of Algorithms. Legal and Ethical Challenges, Cham, 2021, pp. 49-70.

[4] Nella sterminata letteratura in materia, si vedano, ad esempio, K. Crawford, *The Hidden Biases in Big Data*, in *Harvard Business Review Blog Network*, 1° aprile 2013; K. Miller, *Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm*, in *Journal of Technology Law & Policy*, 2014, n. 1, p. 105; C. O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, New York, 2016, p. 10.

2. Difendersi dall'intelligenza artificiale: il diritto al rimedio effettivo

Che il potenziamento degli strumenti di indagine causato dalle tecnologie automatizzate metta in crisi molteplici profili fondamentali dei nostri sistemi di giustizia penale è un fatto ormai noto. Si pensi, a titolo esemplificativo, al diritto ad una valutazione individuale, apparentemente negato dalle analisi statistiche rilasciate dai sistemi di IA[5]; alla presunzione di innocenza, difficilmente compatibile con le "predizioni" di fatto quasi assolute prodotte dai *risk assessment tools*[6]; o al diritto a non autoincriminarsi, contraddetto da quegli strumenti nei quali si richiede al soggetto interessato di contribuire al calcolo dell'indicatore finale[7].

La vulnerabilità dei diritti tradizionalmente riconosciuti all'indagato o imputato a fronte dello sviluppo tecnologico, però, è solo uno degli elementi che possono inficiare l'efficacia di una strategia difensiva. In tale computo, in particolare, un ruolo di primo piano è rivestito dall'interpretazione e dal conseguente riconoscimento del diritto al rimedio effettivo. La possibilità di rimediare al pregiudizio subito, infatti, riduce il rischio che la compressione dei diritti fondamentali sfoci inevitabilmente in vere e proprie violazioni. L'interpretazione di questo diritto fondamentale, tuttavia, è tutt'altro che pacifica.

Da un lato, a livello europeo la nozione di "rimedio effettivo" rimane ancora decisamente indeterminata, specialmente se comparata con

---

[5] G. Contissa, G. Lasagni, *When it is (also) algorithms and AI that decide on criminal matters: In search for an effective remedy*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2020, n. 3, pp. 285-286; I. Neroni Rezende, *Predictive policingsafeguards for the choice of data and automated processing in the preventive context*, in S. Barona Vilar (a cura di), *Justicia algorítmica y neuroderecho: una mirada multidisciplinar*, Valencia, 2021, pp. 361 ss.; sulla necessità di utilizzare con cautela il termine "predizione" in questo contesto, S. Quattrocolo, *Intervento alla Conversazione del 20 ottobre 2020,* pubblicato in *Processo penale e Intelligenza Artificiale*. *Position Paper n. 1*, Fondazione Leonardo Civiltà delle Macchine, 2020, pp. 17 ss.

[6] Profilo evidenziato anche nel considerando n. 38 della *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale*, COM (2021) 206, Bruxelles, 21 aprile 2021, come rilevato da A.M. Maugeri, *L'uso di algoritmi predittivi per accertare la pericolosità sociale,* cit., p. 21.

[7] Cfr. C. Deskus, *Fifth Amendment Limitations on Criminal Algorithmic Decision-Making*, in *New York University Journal of Legislation & Public Policy*, 2018, n. 3, p. 250.

la definizione di altri diritti fondamentali[8]. Tale ambiguità è certamente aiutata dalla vaghezza delle disposizioni sovranazionali che riconoscono espressamente questo diritto, segnatamente gli articoli 13 Conv. eur. dir. uomo e 47 Carta dei dir. fond. UE[9]; ciò, a sua volta, si ripercuote sulla legislazione secondaria. Si pensi, per tutti, alla scarsa incisività delle disposizioni in materia contenute nelle sei direttive sui diritti di difesa incluse nel cosiddetto "Programma di Stoccolma", non per nulla trasposte con esiti decisamente poco armonizzati nei singoli Stati Membri[10].

---

[8] Tanto da essere definita una delle norme più oscure di tutta la Convenzione, cfr. l'opinione dei giudici Matscher e Pinheiro Farinha nel caso *Malone c. Regno Unito*, ric. n. 8691/79, 2 agosto 1984. La vaghezza di questo diritto persiste anche nella giurisprudenza CGUE più recente, si veda, ad esempio, *R.N.N.S. e K.A. c. Minister van Buitenlandse Zaken*, cause riunite C-225/19 e C-226/19, 24 novembre 2020.

[9] A fronte di disposizioni testuali piuttosto generiche, la giurisprudenza europea ha tracciato alcuni tratti distintivi della nozione, che tuttavia forniscono solo alcune indicazioni minime su cosa possa qualificarsi come "rimedio effettivo". Ad esempio, tale è considerato lo strumento che sia accessibile al ricorrente non sono in principio, ma anche in concreto e che possa impedire la persistenza di una presunta violazione o fornire una risposta adeguata alle violazioni già occorse (cfr., *e.g.* Corte EDU, *Kudła c. Polonia*, ric. n. 30210/96, 26 dicembre 2000, §§ 157–58). Al tempo stesso, entrambe le Corti europee, pur esprimendo una preferenza per la possibilità di fare valere eventuali violazioni davanti ad un'autorità giudiziaria, tendono a considerare effettivo un rimedio anche se esperito davanti ad una autorità amministrativa, purché indipendente e imparziale (*e.g.* Corte EDU, *Zakharov c. Russia*, ric. n. 47143/06, 4 dicembre 2015, § 258 ss. e l'art. 8 Carta dir. fond. UE); diverso invece il caso dell'art. 47 Carta dei dir. fond. UE che si riferisce invece espressamente al "Diritto a un ricorso effettivo e a un giudice imparziale" (su cui si veda la giurisprudenza ormai risalente *Marguerite Johnston c Chief Constable*, causa 222/84, 15 maggio1986; U*nion nationale c. Georges Heylens e a.*, causa 222/86, 15 ottobre 1987; *Oleificio Borelli SpA c Commissione*, causa C-97/91, 3 dicembre 1992). In certa misura, inoltre, il diritto al rimedio effettivo, almeno nella materia penale o punitiva, è sovrapponibile con la nozione di *full judicial review*, cioè della capacità della autorità interpellata di esaminare sia questioni di fatto, che di diritto (cfr. Corte EDU, *Umlauft c Austria*, 23 ottobre 1995, ric. n. 15527/89, § 37; *Oztürk c Germania*, 21 febbraio 1984, ric. n. 8544/79 § 56; *Menarini Diagnostics S. R. L. c Italia*, 27 settembre 2011, ric. n. 43509/08, §§ 59-63-67; *Schmautzer c Austria*, 23 ottobre 1995, ric. n. 15523/89, § 36; *Gradinger c Austria*, 23 ottobre 1995, ric. n. 15963/90, § 44; per la CGUE, ad esempio v. *Chalkor c. Commissione*, causa, C-386/10 P, 8 dicembre 2011, § 47; *Schindler Holding Ltd e a*., causa T-138/07, 13 luglio 2011, § 36; *Telefónica SA e Telefónica de España SAU c Commissione*, causa C-295/12 P, 10 luglio 2014, §§ 51-52).

[10] Cf. S. Allegrezza, V. Covolo (a cura di), *Effective Defence Rights in Criminal Proceedings. A European and Comparative Study on Judicial Remedies*, Milano, 2018;

D'altro canto, anche a livello nazionale, spesso non esiste una disciplina chiara sul punto, che si traduca in una sufficiente prevedibilità per la difesa delle conseguenze di una eventuale violazione delle garanzie processuali. Negli ordinamenti europei, infatti, la questione non di rado è rimessa alla discrezionalità del giudice[11]: una soluzione che conferisce certamente flessibilità al sistema, ma spesso a discapito della certezza del diritto per i soggetti interessati dal processo penale.

Una simile incertezza è poi amplificata dalla pressoché totale assenza di una tassonomia condivisa a livello transnazionale (o anche solo unionale) su quali tipi di rimedi debbano applicarsi a fronte di determinate violazioni[12].

Queste considerazioni, naturalmente, non vengono in rilievo solo quando algoritmi ed IA entrano in campo. Tuttavia, in tali circostanze le conseguenze della mancanza di meccanismi consolidati per rimediare alle criticità causate dalle tecnologie automatizzate nell'accertamento penale e, ancor prima, dell'assenza di una nozione condivisa di "rimedio", sono specialmente esacerbate. Non a caso, come si vedrà brevemente in seguito, l'impiego dell'IA ha richiesto, sin dalle origini, la creazione di regole specifiche proprio riferite alla definizione di diritto al rimedio effettivo nell'ambito in questione. Qui, infatti, alla vaghezza intrinseca del diritto si uniscono profili critici ulteriori: in primo luogo, il dubbio, non trascurabile, sulle effettive capacità di un giudice umano di riesaminare decisioni automatizzate in tutto o in parte.

M. Caianiello, G. Lasagni, *Comparative Remarks*, in G. Contissa, G. Lasagni, M. Caianiello, G. Sartor (a cura di), *Effective Protection of the Rights of the Accused in the EU Directives. A Computable Approach to Criminal Procedure Law*, Leiden, 2022, pp. 233 ss.

[11] J.A.E. Vervaele, *Lawful and Fair Use of Evidence from a European Human Rights Perspective*, in F. Giuffrida, K. Ligeti (a cura di), *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings*, Lussemburgo, 2019, pp. 56 ss.; M. Delmas-Marty, J.R. Spencer (a cura di), *European Criminal Procedures*, Cambridge, 2002, pp. 594 ss.

[12] Si veda, ad esempio, l'annoso dibattito sulla valenza delle regole di esclusione probatoria, su cui cfr. per tutti, in ottica comparata, S. Gless, T. Richter (a cura di), *Do Exclusionary Rules Ensure a Fair Trial? A Comparative Perspective on Evidentiary Rules*, Cham, 2019.

2.1. Alla ricerca di effettività: i dubbi sull'efficacia di un "intervento umano" ex post

All'interno dell'Unione, il principale riferimento normativo, quando si parla di rimedi avverso decisioni assunte nella materia penale con l'ausilio di tecnologie di IA, è certamente l'art. 11 della Direttiva 2016/680, secondo cui:

> Una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici negativi o incida significativamente sull'interessato [è] 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[13].

Linee argomentative dello stesso tenore si riscontrano peraltro anche nel nostro ordinamento, dove la giurisprudenza interna, sinora sviluppata soprattutto con riferimento a procedimenti amministrativi relativi al mondo dell'istruzione scolastica, ha sottolineato come:

> In proposito, deve comunque esistere nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatica[14].

---

[13] Art. 11 Dir. 2016/680/UE, rubricato «Processo decisionale automatizzato relativo alle persone fisiche». Lo stesso approccio è peraltro applicato anche al di fuori del diritto penale, cfr. l'art. 22 GDPR. Nello stesso senso si veda anche quanto sostenuto dal Gruppo di lavoro Articolo 29 per la protezione dei dati, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679* (wp251rev.01), 3 ottobre 2017, secondo cui: «If a human being reviews and takes account of other factors in making the final decision, that decision would not be 'based solely' on automated processing. The controller cannot avoid the Article 22 provisions by fabricating human involvement […oversight of the decision] should be carried out by someone who has the authority and competence to change the decision».

[14] Cons. St., sez. VI, sent. 4 febbraio 2020 n. 881, § 11.2; su cui si veda M. Gialuz, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, cit., p. 66; J. Della Torre, *Le decisioni algoritmiche all'esame del Consiglio di Stato*, in *Riv. dir. process*., 2021, n. 2, p. 713. Sullo stesso tenore, in precedenza, ad esempio anche TAR Lazio, sez. III-*bis*, sent. n. 03769/2017 (udienza del 14 febbraio 2017) e n. 09230/2018 (udienza del 26 giugno 2018).

Da entrambi i piani, quindi, sembra emergere un modello di rimedio incentrato sul rigetto di una delega totale all'automazione e sull'esercizio di un controllo *ex post* da parte di un essere umano sulle valutazioni emesse dai sistemi di IA[15]. Questa soluzione può sembrare in principio ragionevole e, tutto sommato, ribadendo la centralità della nostra specie sul processo decisionale, anche rassicurante.

Ad un esame più ravvicinato e sulla base di alcuni esempi derivanti dalla prassi, però, i presupposti di un simile approccio possono essere messi in dubbio. Più precisamente, si deve evidenziare come, almeno in determinate circostanze, le capacità umane di rivedere una decisione automatizzata siano tutto sommato limitate e, probabilmente, insufficienti a garantire un rimedio davvero effettivo a chi subisce le conseguenze di una decisione automatizzata.

L'esempio più eclatante si rinviene certamente in ambito medico, dove si è già osservato come le diagnosi prodotte da sistemi di IA sono tendenzialmente accettate o rigettate *in toto* dall'operatore umano. In altre parole, o ci si fida della macchina e quindi si adotta la diagnosi proposta, oppure non ci si fida e quindi la valutazione automatizzata non sarà presa in considerazione[16]. La decisione in un senso o nell'altro, naturalmente, dipende in gran parte anche dal contesto in cui questa deve essere presa. Un fattore significativo, certamente, è quello temporale: se la componente umana deve agire in fretta (tipica, l'urgenza di eseguire un determinato intervento chirurgico per salvare la vita al paziente), le possibilità di mettere in discussione il merito della decisione automatizzata diventano in concreto decisamente ridotte. Questo profilo, particolarmente evidente in ambito medico, non è tuttavia estraneo al mondo del diritto.

Si pensi, segnatamente, al caso di *Frontex*, l'agenzia europea che si occupa del controllo dei confini esterni dell'Unione e la cui azione ha quindi effetti diretti, e spesso drammatici, per le persone che cercano l'ingresso sul nostro territorio. Stime ufficiali indicano in circa dodici se-

[15] Definito efficacemente come «controllo umano significativo» da G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo,* in *Diritto penale contemporaneo – Rivista trimestrale*, 2020, n. 4, pp. 83-84.

[16] F. Lagioia, G. Contissa, *The Strange Case of Dr. Watson: Liability Implications of AI Evidence-Based Decision Support Systems in Health Care*, in *European Journal of Legal Studies*, 2020, n. 2, pp. 263 ss.

condi a persona il tempo medio a disposizione di una guardia di frontiera nel prendere la decisione di concedere o negare l'ingresso nell'Unione, ad esempio valutando sommariamente l'autenticità della documentazione presentata[17].

Nel 2019, *Frontex* ha ufficialmente dichiarato di non fare uso di sistemi di IA nello svolgimento dei propri compiti[18]. Ciò nonostante, la situazione è tutt'altro che immutabile. Da un lato, l'agenzia è incaricata della gestione del sistema EUROSUR (*European Border Surveillance System*), che utilizza un approccio basato sull'intelligence e sull'analisi dei rischi per supportare le proprie capacità decisionali[19]. Dall'altro lato, nel 2020, uno studio redatto da un gruppo di esperti di IA, istituto dalla Commissione europea, si è occupato di identificare gli ambiti di intervento di queste tecnologie anche in relazione al controllo delle frontiere, ad esempio nella valutazione del rischio e nella selezione delle domande nell'ambito del procedimento di rilascio dei visti[20]. Nel 2021, peraltro, la stessa *Frontex* ha pubblicato uno studio per mappare le possibilità di impiego di strumenti di IA per il monitoraggio dei confini europei[21] e,

---

[17] Cfr. J. Fergusson, *Twelve Seconds to Decide. In search of excellence: Frontex and the principle of best practice*, *Frontex Information and Transparency Team*, 2014.

[18] Secondo quanto dichiarato in una interrogazione davanti al Parlamento europeo, cfr. *Parliamentary question*, *Answer given by Ms Gabriel on behalf of the European Commission,* 28 marzo 2019.

[19] Il sistema è operativo dal 2013. Per ulteriori riferimenti, v. https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/border-crossing/eurosur_en.

[20] Cfr. *Commission Expert Group on Artificial Intelligence in the domain of Home Affairs.* Per ulteriori riferimenti al riguardo: https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3727&news=1. Altri studi condotti per conto della Commissione europea hanno esplorato la possibilità di sviluppare uno strumento di previsione e di allerta precoce per la migrazione basato sulla tecnologia dell'intelligenza artificiale: cfr. Ecorys, *Feasibility study on a forecasting and early warning tool for migration based on artificial intelligence technology*, novembre 2020, disponibile *online* al seguenti indirizzo: https://op.europa.eu/lv/publication-detail/-/publication/946b0bc7-7006-11eb-9ac9-01aa75ed71a1/language-lv/format-PDF/source-search; A. Renda *et alii*, *Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe*, 21 aprile 2021, disponibile *online* al seguente indirizzo: https://digital-strategy.ec.europa.eu/en/library/study-supporting-impact-assessment-ai-regulation.

[21] Cfr. Frontex, *Artificial Intelligence – based capabilities for European Border and Coast Guard*, Varsavia, marzo 2021, disponibile *online* al seguente indirizzo: https://

nello stesso anno, la Commissione ha inserito l'utilizzo di strumenti IA nella nuova strategia Schengen[22]. In tale contesto, si inserisce il progetto di *European Travel Information Authorisation System* (ETIAS), che diverrà pienamente operativo alla fine del 2022 e che consentirà di valutare automaticamente i cittadini di Paesi terzi in base ai rischi di migrazione irregolare, per la sicurezza o per la salute pubblica. Secondo le informazioni attualmente disponibili, le regole di *screening* saranno integrate da un algoritmo che permetterà di identificare i viaggiatori che corrispondono a profili di rischio predefiniti[23]. Secondo il modello di riferimento già illustrato, in caso di "risposta positiva", la domanda dovrebbe essere riesaminata da un funzionario. Anche in questo caso, però, a fronte delle risorse limitate e delle tempistiche ridotte, l'efficacia di un simile rimedio sembra alquanto limitata[24].

Considerazioni in parte comparabili possono essere riscontrate anche in relazione all'accertamento penale in senso stretto. Al di là della struttura teorica di riferimento, infatti, è ben noto come situazioni di sovraccarico lavorativo, assai comuni nel nostro sistema, mettano in difficoltà

---

frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf.

[22] Commissione europea, *Comunicazione della Commissione al Parlamento europeo e al Consiglio. Strategia per uno spazio Schengen senza controlli alle frontiere interne pienamente funzionante e resiliente,* COM/2021/277 final, Bruxelles, 2 giugno 2021.

[23] Gli indicatori saranno formati a seguito del confronto fra i dati prodotti dal soggetto e quelli inclusi nei sistemi informativi UE, inclusi i dati di *Europol*, e le banche dati di *Interpol* e terranno in considerazione fattori quali età, sesso, nazionalità, Paese e città di residenza, livello di istruzione e occupazione attuale: cfr. C. Dumbrava (*European Parliamentary Research Service*), *Artificial intelligence at EU borders. Overview of applications and key issues*, luglio 2021, disponibile *online* al seguente indirizzo: https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf, p. 6.

[24] Peraltro, uno studio del 2020 condotto per conto della Commissione ha indicato anche le potenzialità di includere uno strumento di IA nell'ETIAS per «la valutazione del rischio individuale in caso di "esito positivo" nella prima valutazione automatica del rischio, facilitando un'ulteriore revisione da parte di uno Stato membro»: cfr. Deloitte, *European Commission, Directorate-General for Migration and Home Affairs*, *Opportunities and challenges for the use of artificial intelligence in border control, migration and security*, vol. I, *Main report*, Bruxelles, 2020, disponibile *online* al seguente indirizzo: https://op.europa.eu/en/publication-detail/-/publication/c8823cd1-a152-11ea-9d2d-01aa75ed71a1/language-en, pp. 19 e 91-92.

sia l'efficienza del sistema di giustizia penale, sia il diritto ad una ragionevole durata del processo.

In questo contesto, l'introduzione di strumenti che, tramite tecnologie di IA, supportino il lavoro del giudice, facilitando l'esecuzione di taluni compiti (ad esempio, la valutazione sulla pericolosità dell'imputato per l'applicazione di misure alternative alla detenzione) potrebbe trovare accoglimento nella prassi, in modo non troppo dissimile da quanto avviene per gli strumenti di diagnosi in ambito medico. Detto altrimenti: schiacciato dalla pressione di smaltire nel minor tempo possibile il carico giudiziario, anche il giudice umano potrebbe essere tentato dall'opzione fidarsi/non fidarsi dei risultati prodotti dalla macchina, piuttosto che imbarcarsi nel difficile compito di entrare nel merito del risultato fornito.

A meno di errori macroscopici, infatti, quest'ultima operazione potrebbe rivelarsi più dispendiosa che assumere direttamente una decisione. Da un lato, specialmente a fronte della scarsa *explainability* dei sistemi di IA nelle condizioni attuali, gli elementi a disposizione del giudice nel rivedere le decisioni automatizzate risultano piuttosto limitati. Questo problema è già stato evidenziato da alcune decisioni giurisprudenziali, che hanno mostrato come, anche quando sia dato accesso al codice sorgente dell'algoritmo, ciò spesso non sia sufficiente a dare un accesso effettivo al "ragionamento" sviluppato dalla macchina[25]. Si è sottolineato, infatti, come a tal fine sia necessario avere accesso anche ai dati utilizzati per produrre il risultato[26]. Poiché il valore prodotto è essenzialmente una elaborazione statistica parametrata ad un gruppo di riferimento prescelto, essere in grado di individuare quest'ultimo diventa essenziale per contestare nel merito della decisione presa. L'accesso a tali dati, però, è difficilmente ottenibile nella prassi. In primo luogo, perché le banche dati in questione spesso non sono nel possesso degli inquirenti, ma piuttosto di privati magari operanti in altre giurisdizioni. Inoltre, quand'anche acces-

[25] Il caso forse più emblematico in tal senso è quello relativo agli algoritmi utilizzati in Francia per determinare in quale università gli studenti potevano iscriversi a seguito dell'equivalente dell'esame di maturità (*Admission Post Bac*): cfr. la decisione della *Commission d'Accès aux Documents Administratifs* (*CADA*), 23 giugno 2016, n. 20161990, disponibile *online* al seguente indirizzo: https://www.cada.fr/20161989.

[26] Cfr. L. Edwards, M. Veale, *Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For*, in *Duke Law & Technology Law Reiew*, 2017, n. 1, pp. 18 ss.

sibili agli inquirenti, la condivisione di tali dati solleva diverse difficoltà rispetto alle necessità di dare tutela ai soggetti terzi, estranei al procedimento penale, e che pure sarebbero coinvolti come *benchmark* nella valutazione automatizzata.

Anche a non voler considerare queste difficoltà, peraltro, la capacità del giudice umano di mettere in discussione una elaborazione di IA sembra realisticamente risibile tenuto conto delle conoscenze tecniche ad oggi in possesso da parte dell'operatore giuridico medio. Si considerino le difficoltà, mostrate anche dalla nostra giurisprudenza, nell'analizzare le "mere" prove digitali, che presentano un contenuto tecnologico già più consolidato di quelle generate da sistemi di IA[27].

Per queste ragioni, il riconoscimento di un intervento umano successivo, più che garanzia di rimedio effettivo, sembra ridursi essenzialmente all'elaborazione di un criterio di imputazione di responsabilità. In altre parole, con tale clausola ci si assicura la possibilità di identificare una persona fisica a cui imputare le eventuali conseguenze negative della decisione automatizzata. Pur trattandosi di un apporto significativo, questo risultato si pone però ben al di sotto del contenuto garantistico richiesto dal diritto fondamentale in oggetto.

Il rischio di un vuoto di tutela è quindi reale e, in verità, non limitato esclusivamente al modello europeo.

Fragilità su questo fronte, difatti, si riscontrano anche nell'approccio sinora sviluppato dalle corti oltreoceano e reso celebre dal noto caso *Loomis*[28]. In tale decisione, la Corte suprema del Wisconsin aveva affermato che il risultato di un sistema di *risk assessment* potesse essere uti-

[27] Ai classici problemi tipici della prova scientifica (informatica nel caso di specie), riassumibili in gran parte nel concetto di *data fundamentalism*, cioè nella tendenza a fare affidamento sulle prove scientifiche informatiche ritenendole tendenzialmente a priori come elementi oggettivi, senza interrogarsi su come tali prove siano state raccolte o formate (simile, su altri fronti, quindi, al più noto *CSI effect*, relativo alla prova del DNA), cfr. A. Kroll, S. Barocas, E. Felten, J.R. Reidenberg, D. G. Robinson, H. Yu, *Accountable Algorithms*, in *University of Pennsylvania Law Review*, 2016, p. 633; K. Crawford, *The Hidden Biases*, cit. Sulla possibilità di considerare le prove prodotte da sistemi di IA come una sub-specie delle prove digitali, cf. M. Gialuz, *Intelligenza artificiale*, cit., p. 61; G. Ubertis, *Intelligenza artificiale,* cit., p. 84.

[28] *Supreme Court of Wisconsin, State v. Loomis*, 881 N.W.2d 749 (Wis. 2016). Sulla stessa linea anche altre decisioni, come ad esempio quella dell'Indiana Court of Appeals, *Malenchik v. State*, 928 N.E.2d 564, 574 (Ind. 2010),

lizzato anche per fini diversi da quelli originariamente previsti (commisurazione della pena, invece che misurazione del rischio di recidiva nella *probation*), purché la decisione automatizzata non costituisse l'unico elemento fondante della decisione del giudice. Oltre alle numerose problematiche, già sollevate dalla dottrina e in gran parte legate all'utilizzo dello specifico *tool* in questione (COMPAS)[29], l'approccio illustrato ha almeno il merito di non fondarsi sulla presunta capacità dell'essere umano di discostarsi, nella prassi, da un risultato prodotto da sistemi di IA.

Secondo questo modello, infatti, la valutazione automatizzata non viene riesaminata da parte del giudice umano, che però è tenuto a solo a verificare l'esistenza di elementi di riscontro ai risultati raggiunti. L'efficacia garantista di un simile approccio, tuttavia, finisce per ricadere in larga misura sulla qualità della *corroboration* richiesta. In mancanza di criteri adeguati o di una vigilanza adeguata sul punto, il rischio di un appiattimento del giudizio umano sulla valutazione proposta dall'IA si ri-espande, come nel caso europeo. Di questo esito infausto, *Loomis*, in cui si erano stati utilizzati in funzione di riscontro elementi alquanto controversi – come la mera esistenza di altre imputazioni a carico del medesimo soggetto[30] – rappresenta un chiaro esempio.

2.2. Alla ricerca di effettività: altre soluzioni possibili

A questo punto, pare d'obbligo chiedersi se, per garantire l'effettività dei diritti di difesa quando siano in gioco sistemi di IA, sia davvero la revisione umana la migliore opzione possibile.

Alla luce delle numerose difficoltà evidenziate poco sopra, infatti, sono state proposte anche interpretazioni alternative, fondate sulla ne-

[29] Sulla sterminata letteratura in materia, si vedano, per tutti, J. Angwin, J. Larson, S. Mattu, L. Kirchner, *Machine Bias: There's Software Used across the Country to Predict Future Criminals. And It's Biased against Blacks*, 23 maggio 2016, disponibile *online* al seguente indirizzo: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing; S. Quattrocolo, *Quesiti nuovi e soluzioni antiche?* Consolidated regulatory paradigms *vs.* risks and fears of 'predictive' digital justice, in *Cass. pen*., 2019, n. 4, pp. 1748 ss.; M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei rischi assessment tools tra Stati uniti ed Europa,* in *Diritto penale contemporaneo – Archivio web*, 29 maggio 2019; A. M. Maugeri, *L'uso di algoritmi,* cit., p. 30.

[30] Le cosiddette "*read-in charges*".

cessità rispondere secondo il principio di parità delle armi alle sfide poste dall'automazione anche nel contesto della giustizia penale. L'idea, in pratica, è quella di difendersi dall'IA *con* l'IA, potenziando la tecnologia per rimettere sullo stesso piano, o almeno su un piano paragonabile, gli elementi prodotti dall'accusa con gli argomenti proponibili dalla difesa.

Su tale piano si collocano, innanzitutto, alcune proposte tecniche: dallo sviluppo di una *explicable AI*, ovvero di sistemi di intelligenza artificiale comprensibili nel loro funzionamento, per superare il problema delle cosiddette *black box*[31]; alla creazione di appositi sistemi di certificazione, che assicurino una certa qualità strutturale degli strumenti in uso[32].

A queste misure tecniche possono poi accompagnarsi approcci integrati, già sviluppati in settori che, in un certo senso come quello penale, richiedono una gestione molto stringente del rischio. Il riferimento va, in particolare, al cosiddetto *redundancy approach*, tipicamente utilizzato nell'aviazione. L'idea è, in pratica, quella di testare la affidabilità dei risultati ottenuti da sistemi di IA confrontandole con altre valutazioni automatizzate prodotte in via indipendente. Se nel caso dell'aviazione questo approccio è adottato per ovvie cause di sicurezza, si è già sostenuto come un modello simile potrebbe trovare applicazione anche nell'ambito della giustizia penale[33]. Il vantaggio di un simile approccio rispetto ai precedenti potrebbe essere quello di portare all'attenzione dell'essere umano giudicante almeno due risultati della valutazione automatizzata. A questo punto, utilizzando strumenti logico-cognitivi più prossimi a quelli già in suo possesso, il giudice potrebbe realisticamente avere maggiori *chances* di effettuare in modo effettivo un riesame della attendibilità delle decisioni di IA. Naturalmente, anche tale opzione presenta alcune

[31] R. Guidotti, A. Monreale, S. Ruggieri, F. Turini, F. Giannotti, D. Pedreschi, *A Survey of Methods for Explaining Black Box Models*, in *ACM Computing Surveys*, 2018, n. 5, pp. 1 ss.

[32] Cfr. *The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems*, First Edition. IEEE, 2019, disponibile *online* al seguente indirizzo: https://standards.ieee.org/content/ieee-standards/en/industry-connections/ec/autonomous-systems.html, p. 16.

[33] Secondo il quale, in termini ampi, per ritenere affidabile un determinato risultato, è essenziale che questo sia prodotto da più macchine, sviluppate con lo stesso scopo, ma da programmatori differenti e con pezzi diversi: cfr., al riguardo, G. Contissa, G. Lasagni, *When it is (also) algorithms*, cit., pp. 288 ss.

complessità. Ad esempio, si dovrebbe chiarire quale valore conferire alla seconda valutazione: se questa debba sostituire la prima, oppure se debba essere assunto un approccio più simile a quello della perizia, in cui la valutazione delle diverse tesi di periti e consulenti è rimessa al libero convincimento del giudice.

Una ipotesi di soluzione, tuttavia, è forse prospettabile: di nuovo al netto di errori macroscopici che indichino chiaramente la preferibilità di un *tool* di IA rispetto all'altro (quali errori di produzione o nel *training*), la seconda opzione pare preferibile. Essa sembra infatti riproporre interrogativi già presenti nel dibattito giurisprudenziale e dottrinale, ad esempio rispetto alle controversie questioni riguardanti l'ammissione e valutazione della prova scientifica[34]. Questo approccio, quindi, seppure applicato ad un ambito tecnologicamente innovativo, potrebbe ricondurre l'attività giudicante a paradigmi non semplici, ma comunque più "maneggiabili" dall'essere umano.

Partendo da una prospettiva simile, peraltro, si potrebbe proporre anche un correttivo al criterio della *corroboration* richiesto dalla giurisprudenza americana. Nello specifico, si potrebbe affinare la regola di valutazione probatoria, consentendo l'uso di dati prodotti da sistemi di IA, purché riscontrati non più in modo generico, ma da una valutazione conforme prodotta da un diverso *tool* automatizzato.

Naturalmente non ha senso interrogarsi su questi profili senza tenere in considerazione anche il lato pratico di simili proposte. Da un lato, per ovviare alle risorse limitate di molti studi legali, sarebbe opportuno che l'investimento per tali strumenti "di controllo" venga fatto a livello istituzionale (ad esempio, mettendo a disposizione *tools* di verifica presso le corti d'appello)[35].

D'altro canto, niente di tutto ciò potrebbe in ogni caso portare i frutti sperati per la tutela dei diritti fondamentali se si dimenticasse l'urgenza di agire anche sul *gap* culturale oggi presente nella formazione dei giuristi. Questi ultimi, infatti, spesso non godono di una preparazione

[34] Su cui si veda, per tutti G. Canzio, L. Lupária (a cura di), *Prova scientifica e processo penale*, Milano, 2017; volendo, con un *focus* specifico sulla prova digitale, v. G. Lasagni, *Admissibility of Digital Evidence*, in V. Franssen, S. Tosza (a cura di), *The Cambridge Handbook of Digital Evidence in Criminal Matters*, Cambridge, in corso di pubblicazione.

[35] G. Contissa, G. Lasagni, *When it is (also) algorithms,* cit., p. 288.

adeguata, che consente loro di comprendere le logiche dei meccanismi statistico-probabilistici o i principi tecnici di base sottesi al funzionamento di IA e algoritmi[36]. In altre parole, al di là di interpretazioni innovative del diritto al rimedio effettivo, lo sviluppo di paradigmi educativi aggiornati e, nei limiti del possibile, multidisciplinari, si prefigura come un passo essenziale per garantire al difensore le capacità di difendere il proprio assistito in modo efficace dall'impatto di indagini caratterizzate da automazione.

3. Difendersi con l'intelligenza artificiale: uno strumento per potenziare il ruolo del difensore

Non è solo con un'ottica meramente speculativa, però, che il difensore si può approcciare alle tecnologie di IA per aumentare le proprie *chance* di successo. Grazie a *tools* già oggi accessibili, infatti, l'automazione può essere utilizzata innanzitutto per potenziare le capacità cognitive del difensore.

L'idea, in altre parole, è quella di sfruttare algoritmi ed IA per colmare talune lacune conoscitive comuni, che possono essere causate dalle più varie ragioni. Si pensi, ad esempio, alla necessità di pianificare una strategia difensiva potenzialmente vincente davanti ad una autorità complessa o di cui è difficile anticipare le modalità di ragionamento; o a quella di operare in contesti che richiedono competenze specialistiche di tipo linguistico o legale anche solo per individuare la normativa applicabile (scenario tipico nei procedimenti transnazionali, ma, come si diceva, ormai piuttosto comune grazie alla diffusione del digitale). O ancora, alle problematiche causate dall'impellenza di venire a conoscenza del significato non solo letterale conferito ad un determinato concetto nel contesto legale e culturale di riferimento: esemplificativa, in tal senso, la nozione di "indagato", al centro delle direttive europee del cosiddetto "Programma di Stoccolma" (caso tutt'altro che infrequente, se si pensa ai numerosi procedimenti riguardanti un mandato di arresto europeo o,

[36] Aspetto sottolineato in particolar modo da L. Luparia Donati, *Notazioni controintuitive su intelligenza artificiale e libero convincimento*, in AA.VV., *Intelligenza artificiale, giurisdizione penale ed etica del giudizio*, cit., pp. 118-119.

in via incrementale, un ordine europeo di indagine penale)[37]. La consapevolezza del mero termine, senza una conoscenza sufficiente del substrato giuridico-culturale di riferimento, rischia infatti di essere fuorviante nella predisposizione di una strategia difensiva efficace. Tradizionalmente, affrontare tali complessità richiede il possesso di conoscenze qualificate non a portata di uno studio legale medio.

A fronte di simili problematiche, la tecnologia IA può venire in soccorso tramite strumenti di assistenza "intelligenti" di varia natura e funzione. Ci si riferisce qui, soprattutto, all'apporto fornito da quella branca dell'informativa giuridica che si occupa dell'analisi semantica del testo giuridico, la quale, tramite metodologie di ragionamento logico fondate su tecniche di IA, riesce a rendere computabile, cioè leggibile dalle macchine, un testo giuridico[38].

Nello specifico, la varietà di questi sistemi è ovviamente assai ampia. Vi si possono includere innanzitutto quei sistemi in grado di fornire un supporto customizzato al difensore, equivalente ad una prognosi di successo della tesi da sostenere, sulla base dell'analisi delle decisioni nel settore di riferimento. In altre parole, descrivendo le argomentazioni che si vorrebbero utilizzare per la propria strategia difensiva, il *tool* calcolerà in termini percentuali la probabilità di accoglimento degli argomenti selezionati[39].

Altre tipologie di strumenti di supporto operano invece su di un pia-

---

[37] A parità di uso terminologico e nonostante l'avvenuta trasposizione, infatti, la parola *suspect* mantiene ad oggi contenuti variabili all'interno dei sistemi nazionali, per esempio richiedendo in alcuni casi una formale notifica delle accuse al soggetto, in altri riferendosi alla mera notazione in un apposito registro. Paradigmatico, in tal senso, il caso della Polonia, come analizzato da K. Kremens, W. Jasiński, D. Czerwińska, D. Czerniak, *Poland. There and Back Again. A Struggle with Transposition of EU Directives*, in G. Contissa, G. Lasagni, M. Caianiello, G. Sartor (a cura di), *Effective Protection,* cit., pp. 154 ss.

[38] Su cui si vedano, ad esempio, M. Billi, G. Contissa, Galileo Sartor, *Logic Representation of Legal Norms*, e L. Di Caro, L. Humphreys, E. Sulis, R. Nanda, *EU Directives Implementation. Automated Analysis of Complexity and Harmonization,* entrambi in G. Contissa, G. Lasagni, M. Caianiello, G. Sartor (a cura di), *Effective Protection,* cit., rispettivamente pp. 277 e 309 ss.

[39] Cf. S. Brüninghaus, K.D. Ashley, *Predicting Outcomes of Case-based Legal Arguments,* in *ICAIL '03: Proceedings of the 9th international conference on Artificial intelligence and law,* 2003*,* pp. 233-242.

no più prettamente conoscitivo, aiutando il difensore, o il consulente, a colmare lacune specifiche. Ad esempio, il sistema "intelligente" potrebbe aiutare l'utente a superare ostacoli legati alla difformità linguistica, nel caso di procedimenti con tratti transnazionali. In questi scenari, infatti, nonostante la possibilità di nominare un difensore nello Stato di esecuzione, il dispiegamento di una strategia difensiva efficace richiede comunque, almeno in certa misura, la comprensione dei meccanismi processuali negli ordinamenti coinvolti.

In questo frangente, l'apporto dell'IA spazia ben al di là del mero supporto offerto da banche dati di tipo tradizionale, offrendo una soluzione non solo alla necessità di accesso alle risorse legali in una lingua comprensibile alle parti (tendenzialmente, in inglese), ma anche affrontando alla radice la problematicità della divergenza culturale fra i diversi ordinamenti. Il valore aggiunto di questi sistemi, quindi, si traduce nella capacità di porre in relazione i concetti giuridici, andando al di là di appellativi formali e similitudini terminologiche, per risalire ai tratti sostanziali che definiscono una determinata situazione processuale, mettendo il difensore nella condizione di assumere decisioni strategiche più consapevoli[40].

I vantaggi offerti dall'IA in questo senso non si limitano, peraltro, solo alla sfera conoscitiva, ma possono espandersi anche a quella strutturale-organizzativa. Nel caso in cui tali strumenti siano messi a disposizione del difensore gratuitamente o a costi contenuti (ad esempio, quando sviluppati da istituzioni o con fondi pubblici), essi consentono infatti una riduzione significativa dei costi. Ciò aprirebbe quindi anche a studi legali di piccole o medie dimensioni la possibilità di affrontare in modo efficace i casi illustrati.

Infine, merita un cenno l'eventualità, già presente in altri ambiti

[40] Tale risultato può essere ottenuto con un approccio computazionale al testo giuridico, cioè con una attenta traduzione del linguaggio legale in contenuto comprensibile alla macchina. Questa operazione, da realizzarsi con l'impiego di competenze multidisciplinari, viene poi raffinata tramite addestramento con tecniche di *machine learning* e *test* con i professionisti del settore. Un esempio, in questo senso, può essere la piattaforma sviluppata all'interno del Progetto *Crossjustice* (*Knowledge, Advisory and Capacity Building Information Tool for Criminal Procedural Rights in Judicial Cooperation*), finanziato dalla Commissione europea (GA n. 847346 – https://crossjustice.eu/en/index.html) ed in particolare il Modulo 3: "*Reasoning Tool*".

dell'ordinamento, che i sistemi di supporto intelligente si possano proporre come veri e propri sostituti di parte di quell'attività di consulenza difensiva caratterizzata da un basso quoziente di complessità e un alto dispendio di risorse in termini temporali o di personale.

Ci si riferisce, a titolo esemplificativo, a quei sistemi che consentono di riconoscere in via automatizzata profili potenzialmente dannosi, come le clausole vessatorie nei contratti per adesione[41]. Naturalmente, la variabilità e la delicatezza dei procedimenti penali richiedono capacità di valutazione che, ad oggi, non trovano corrispondenti tecnologici davvero soddisfacenti. Questa considerazione, però, riduce solo parzialmente il potenziale di tali strumenti sulla definizione del ruolo del difensore anche nella materia penale. È innegabile infatti che, in prospettiva, il valore aggiunto dell'avvocato (umano) rispetto all'aiuto proveniente dal supporto automatizzato dovrà essere adeguatamente ridefinito, concentrandosi sugli aspetti più qualitativi della professione.

4. L'intelligenza artificiale per il potenziamento dei diritti di difesa: alla ricerca di strategie innovative per migliorare la tutela dei diritti fondamentali

Si è parlato sinora di come i sistemi di IA possano essere utilizzati per ristabilire la parità fra le parti (o per tentare di farlo) e per aiutare il difensore nello svolgimento delle proprie attività.

Da ultimo, vale la pena interrogarsi sulla possibilità di utilizzare gli strumenti di IA in modo proattivo per la realizzazione di strategie difensive veramente innovative.

Un primo approccio è quello di sfruttare gli strumenti di IA sviluppati a fini preventivi o di indagine penale anche a scopo di difesa. Su questa linea, nel nostro ordinamento si registrano già i primi tentativi.

In un caso portato all'attenzione del giudice di legittimità, ad esem-

[41] Si veda, ad esempio, il sistema *Claudette* (http://claudette.eui.eu/), anch'esso sviluppato all'interno di un progetto europeo, su cui G. Contissa, F. Lagioia, G. Sartor, P. Torroni, *CLAUDETTE: an Automated Detector of Potentially Unfair Clauses in Online Terms of Service*, 2018, disponibile *online* al seguente indirizzo: https://cris.unibo.it/handle/11585/663874.

pio, si era cercato di utilizzare un *software* di riconoscimento facciale (nello specifico, il sistema di identificazione SARI) come prova a discarico[42]. Il ricorso, però, veniva rigettato dalla Corte di cassazione, poiché il difensore non aveva documentato la valenza scientifica dello strumento in questione[43]. Tale argomento, che in astratto potrebbe anche essere considerato ragionevole, suscita però qualche perplessità: SARI, infatti, viene comunemente utilizzato dalle forze dell'ordine, tanto da sollevare il dubbio che in questo frangente si applichi un doppio *standard*, più stringente nel caso delle richieste provenienti dalla difesa[44].

La pronuncia è quindi interessante sotto un duplice profilo: da un lato, essa costituisce una testimonianza della persistente difficoltà nel dare effettività al principio di parità delle parti, specialmente con riferimento alla materia probatoria. Dall'altro, però, la decisione è anche sintomatica della possibilità, da parte del difensore, di rivendicare la polifunzionalità degli strumenti di IA esistenti, pure a favore dell'imputato. Sebbene ancora minoritaria, è auspicabile che la consapevolezza di poter sfruttare tutta la gamma dei possibili elementi probatori, anche tecnologici, nel predisporre la strategia difensiva cresca e sia adeguatamente coltivata. Da questo punto di vista, pertanto, un ruolo essenziale deve essere svolto nei processi di formazione e aggiornamento della professione forense, che per prima deve farsi parte attiva nello sfruttare appieno tutte le potenzialità offerte dalla moderna tecnologia, inclusa quella automatizzata.

Le possibilità di applicazione degli strumenti IA a fini difensivi, però, possono espandersi anche oltre una applicazione innovativa degli strumenti IA già in uso. Detto altrimenti, è tempo che anche le necessità di-

[42] Cass. pen., sez. IV, sent. 18 giugno 2019, n. 39731, su cui v. anche *supra*, cap. I, § 8, nt. 163.

[43] Di fatto alla luce dei criteri interpretativi ispirati alla sentenza *Daubert*, già fatti propri nel nostro ordinamento nella nota pronuncia *Cozzini* (Cass. pen., sez. IV, 17 settembre 2010, n. 43786) su cui, proprio in relazione ai sistemi di IA, si vedano i già citati contributi di M. Gialuz, *Intelligenza artificiale*, cit., p. 61 e G. Ubertis, *Intelligenza artificiale,* cit., p. 84.

[44] Cfr. Garante dei dati personali, *Sistema automatico di ricerca dell'identità di un volto*, 26 luglio 2018 [9040256], disponibile online al seguente indirizzo: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9040256; più critico da ultimo invece rispetto al sistema *Sari Real Time*, 25 marzo 2021 [9575877], disponibile online al seguente indirizzo: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9575877.

fensive, e non solo quelle degli organi inquirenti, vengano poste alla base del processo creativo e di *design* concernente la tecnologia automatizzata. In questo senso, algoritmi ed IA potrebbero essere utilizzati non solo per evitare una riduzione delle garanzie processuali riconosciute nel processo penale tradizionale, ma anche per espandere e potenziare le stesse.

Ad esempio, si potrebbe pensare di applicare taluni strumenti di IA per estendere o rafforzare la portata dei principi del giusto processo sin dalla fase delle indagini, dove di solito il loro riconoscimento è solo parziale. Una possibilità in tal senso potrebbe essere offerta da alcuni strumenti di IA del tipo *Multi-Agent*[45]. L'idea, come ipotizzato altrove, potrebbe essere quella di fare leva sulla capacità di questi sistemi, originariamente sviluppati per lo svolgimento di operazioni di *digital forensics*, di gestire in contemporanea una pluralità di valutazioni anche contrastanti sullo stesso oggetto[46]. Questo potenziale potrebbe essere impiegato per cercare di ridurre l'impatto di errori tipici delle prime fasi investigative (come il *tunnel vision effect*[47]) che hanno un impatto ad oggi difficilmente misurabile, ma spesso drammaticamente irreparabile. In tal senso, l'IA potrebbe essere sfruttata dal difensore per estendere almeno in parte il metodo socratico alle prime scelte degli inquirenti (ad esempio, riguardanti la selezione delle ipotesi investigative da privilegiare); o, quantomeno, per

[45] Con l'espressione "*Multi-agent systems*" ci si riferisce a sistemi informatici complessi, risultanti dall'interazione di diversi agenti artificiali "intelligenti"; essi costituiscono oggetto di studio e ricerca da parte della più attenta letteratura sin dalla fine degli anni '90 (cfr., ad esempio, R. Conte, R. Falcone, G. Sartor, *Introduction: Agents and Norms How to Fill the Gap*, in *Artificial Intelligence and Law,* 1999, pp. 1-15; C. Cevenini, A. Oskamp*, Proceedings of the 4th International Workshop on the Law of Electronic Agents*, Nijmegen, 2005).

[46] Volendo, G. Lasagni, Policing via Multi-Agent Systems*: un nuovo volto per la digital forensics (e non solo)?* in R. Brighi (a cura di), *Nuove Questioni di Informatica Forense*, Roma, 2022, p. 303-321, in corso di pubblicazione anche in versione inglese ed aggiornata in un volume a cura di L. Bachmaier Winter, S. Ruggeri.

[47] Su cui si vedano, *ex multis,* P.C. Wason, *On the failure to eliminate hypotheses in a conceptual task*, in *Quarterly Journal of Experimental Psychology*, 1960, n. 12, pp. 129 ss.; E.J. Lange, *The Illusion of Control*, *Journal of Personality and Social Psychology*, 1975, n. 2, pp. 311 ss.; K. Findley, M. Scott, *The Multiple Dimensions of Tunnel Vision in Criminal Cases*, in *Wisconsin Law Review*, 2006, n. 2, pp. 291 ss.; A. Forza, *La psicologia nel processo penale*, Milano, 2008, pp. 395 ss.

raccogliere elementi utili a far valere, nel corso del giudizio, la rilevanza di eventuali errori commessi in questa fase[48].

Rispetto ai margini di azione sinora indicati, quest'ultimo passaggio è evidentemente ancora sperimentale e non ancora operativo. Nondimeno, esso è indicativo della possibilità e, sempre più, della necessità per il difensore di diventare un soggetto proattivo rispetto all'uso della tecnologia automatizzata.

In altre parole, il difensore, così come le altre parti processuali[49], può e deve diventare un attore che non solo è in grado di gestire in modo consapevole l'applicazione degli strumenti IA già esistenti, ma anche di fungere da stimolo per l'innovazione della tecnologia in oggetto. In altre parole, diventando uno dei motori per il *design* di visioni inedite che migliorino la posizione del proprio assistito rispetto al processo tradizionale.

5. Conclusioni

Sebbene con ritardo rispetto ad altri ambiti, anche nel diritto penale il dilagare dei sistemi algoritmici e di IA ha reso ormai inevitabile considerare queste tecnologie come mezzi sempre più presenti nelle attività di accertamento dei reati. Ciò non implica, ovviamente, un'accettazione passiva di tutti i *tools* automatizzati; in questo senso, la vigilanza critica ed attiva di cittadini, associazioni, comitati e dottrina svolge un ruolo essenziale per difesa dei diritti fondamentali così come li abbiamo sinora conosciuti.

Anche un'altra prospettiva è però possibile e, si ritiene, ormai imperativa nell'approcciarsi alle tecnologie automatizzate in ambito penale: interrogarsi senza pregiudizi su quale potenziale possa essere estratto da queste dall'IA per migliorare la tutela dei diritti fondamentali rispetto a come li abbiamo sinora conosciuti.

---

[48] G. Lasagni, *Policing*, cit., pp. 315 ss.

[49] Tale esigenza si pone in modo particolarmente sentito in relazione all'imputato, su cui il presente contributo si concentra; naturalmente, però, considerazioni simili potrebbero essere sviluppate anche in relazione agli interessi propri di ulteriori soggetti processuali, come, per esempio, quelli della vittima.

Si è cercato brevemente di illustrare che un simile cambio di paradigma può applicarsi su livelli diversi: da una rilettura tecnologicamente aggiornata dei principi (e soprattutto dei rimedi, in caso di una loro violazione), allo sfruttamento dei sistemi di potenziamento delle capacità cognitive o organizzative del difensore; dall'uso di strumenti di indagine tecnologica in chiave difensiva, allo sviluppo di nuove applicazioni su fronti ancora inesplorati, che si spingano oltre il livello attuale di tutela dei diritti fondamentali.

Assumere un approccio simile è certamente complesso nella prassi, dove è inevitabile – e verosimilmente lo sarà ancora a lungo – scontrarsi con l'inerzia del legislatore o con l'incomprensione o la diffidenza di parte della giurisprudenza.

Questo, però, non può e non deve essere un elemento di scoramento per il difensore. Dopo tutto, l'intelligenza artificiale è stata creata apposta proprio per potenziare le funzionalità e le capacità dell'essere umano, anche al di là dei modelli di azione e ragionamento[50]. Ciò si applica alle attività di repressione e prevenzione dei reati, così come alle capacità di porre in essere forme di difesa sempre più efficaci ed avanzate. Detto altrimenti, se l'impiego di tecnologie automatizzate comporta nuovi rischi all'interno dell'accertamento penale, le stesse possono anche aprire la strada a nuove opportunità di azione e di tutela, sino ad oggi difficilmente percorribili o anche solo immaginabili.

Ciò richiede al giurista e, soprattutto, al difensore di abbandonare una visione incentrata essenzialmente sulla minimizzazione del rischio, promuovendo un approccio proattivo che, esercitando l'inventiva, sia capace di indirizzare la ricerca e lo sviluppo tecnologico verso nuove frontiere di tutela dei diritti fondamentali.

[50] J. Millar, I. Kerr, *Delegation, Relinquishment and Responsibility: The Prospect of Expert Robots,* 17 marzo 2013, disponibile *online* su SSRN: https://ssrn.com/abstract=2234645; L. Floridi *et alii*, *AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, in *Minds & Machines*, 2018, n. 4, pp. 689-707.

Bibliografia

S. Allegrezza, V. Covolo (a cura di), *Effective Defence Rights in Criminal Proceedings. A European and Comparative Study on Judicial Remedies*, Milano, 2018.

J. Angwin, J. Larson, S. Mattu, L. Kirchner, *Machine Bias: There's Software Used across the Country to Predict Future Criminals. And It's Biased against Blacks*, 23 maggio 2016, disponibile *online* al seguente indirizzo: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (ultimo accesso il 30 giugno 2022).

M. Billi, G. Contissa, G. Sartor, *Logic Representation of Legal Norms*, in G. Contissa, G. Lasagni, M. Caianiello, G. Sartor (a cura di), *Effective Protection of the Rights of the Accused in the EU Directives. A Computable Approach to Criminal Procedure Law*, Leiden, 2022, pp. 277 ss.

M. Brkan, *Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond*, in *International Journal of Law and Information Technology* 27 (2019), n. 2, p. 113.

S. Brüninghaus, K.D. Ashley, *Predicting Outcomes of Case-based Legal Arguments,* in *ICAIL '03: Proceedings of the 9th international conference on Artificial intelligence and law,* 2003*,* pp. 233-242.

M. Caianiello, *Dangerous Liaisons. Potentialities and risks deriving from the interaction between Artificial Intelligence and preventive justice*, in *European Journal of Crime, Criminal Law and Criminal Justice* 29 (2021), n. 1, pp. 1 ss.

G. Canzio, L. Lupária (a cura di), *Prova scientifica e processo penale*, Milano, 2017.

C. Cevenini, A. Oskamp (a cura di)*, Proceedings of the 4th International Workshop on the Law of Electronic Agents*, Nijmegen, 2005.

R. Conte, R. Falcone, G. Sartor, *Introduction: Agents and Norms How to Fill the Gap*, in *Artificial Intelligence and Law* 7 (1999), pp. 1-15.

K. Crawford, *The Hidden Biases in Big Data*, in *Harvard Business Review Blog Network*, 1° aprile 2013 (reperibile al seguente indirizzo: https://hbr.org/2013/04/the-hidden-biases-in-big-data, ultimo accesso il 30 giugno 2022).

G. Contissa, F. Lagioia, G. Sartor, P. Torroni, *CLAUDETTE: an Automated Detector of Potentially Unfair Clauses in Online Terms of Service*, 2018, disponibile *online* al seguente indirizzo: https://cris.unibo.it/handle/11585/663874 (ultimo accesso il 30 giugno 2022).

G. Contissa, G. Lasagni, *When it is (also) algorithms and AI that decide on criminal matters: In search for an effective remedy*, in *European Journal of Crime, Criminal Law and Criminal Justice* 28 (2020), n. 3, pp. 280 ss.

G. Contissa, G. Lasagni, M. Caianiello, G. Sartor (a cura di), *Effective Protection of the Rights of the Accused in the EU Directives. A Computable Approach to Criminal Procedure Law*, Leiden, 2022

M. Delmas-Marty, J.R. Spencer (a cura di), *European Criminal Procedures*, Cambridge, 2002.

Deloitte, *European Commission, Directorate-General for Migration and Home Affairs*, *Opportunities and challenges for the use of artificial intelligence in border control, migration and security*, vol. I, *Main report*, Bruxelles, 2020, disponibile *online* al seguente indirizzo: https://op.europa.eu/en/publication-detail/-/publication/c8823cd1-a152-11ea-9d2d-01aa75ed71a1/language-en (ultimo accesso il 30 giugno 2022).

J. Della Torre, *Le decisioni algoritmiche all'esame del Consiglio di Stato*, in *Riv. dir. process*., 2021, n. 2, pp. 713 ss.

C. Deskus, *Fifth Amendment Limitations on Criminal Algorithmic Decision-Making*, in *New York Journal of Legislation & Public Policy*, 21 (2018), n. 3, pp. 237 ss.

L. Di Caro, L. Humphreys, E. Sulis, R. Nanda, *EU Directives Implementation. Automated Analysis of Complexity and Harmonization*, in in G. Contissa, G. Lasagni, M. Caianiello, G. Sartor (a cura di), *Effective Protection of the Rights of the Accused in the EU Directives. A Computable Approach to Criminal Procedure Law*, Leiden, 2022, pp. 309 ss.

Ecorys, *Feasibility study on a forecasting and early warning tool for migration based on artificial intelligence technology*, novembre 2020, disponibile *online* al seguenti indirizzo: https://op.europa.eu/lv/publication-detail/-/publication/946b0bc7-7006-11eb-9ac9-01aa75ed71a1/language-lv/format-PDF/source-search (ultimo accesso il 30 giugno 2022).

L. Edwards, M. Veale, *Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For*, in *Duke Law & Technology Law Review* 16 (2017), n. 1, pp. 16 ss.

J. Fergusson, *Twelve Seconds to Decide. In search of excellence: Frontex and the principle of best practice*, *Frontex Information and Transparency Team*, 2014 (reperibile al seguente indirizzo: https://op.europa.eu/it/publication-detail/-/publication/75d39cda-0447-4ba6-829e-23214486e261/language-en, ultimo accesso il 30 giugno 2022).

K. Findley, M. Scott, *The Multiple Dimensions of Tunnel Vi-sion in Criminal Cases*, in *Wisconsin Law Review* 108 (2006), n. 2, pp. 291 ss.

L. Floridi, *et alii*, *AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, in *Minds & Machines* 28 (2018), n. 4, pp. 689 ss.

A. Forza, *La psicologia nel processo penale*, Milano, 2008, pp. 395 ss.

FRONTEX, *Artificial Intelligence – based capabilities for European Border and Coast Guard*, Varsavia, marzo 2021, disponibile *online* al seguente indirizzo: https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf. (ultimo accesso il 30 giugno 2022).

M. GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, pp. 51 ss.

M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati uniti ed Europa,* in in *Diritto penale contemporaneo – Archivio web*, 29 maggio 2019 (reperibile all'indirizzo https://archiviodpc.dirittopenaleuomo.org/, ultimo accesso il 30 giugno 2022).

S. GLESS, T. RICHTER (a cura di), *Do Exclusionary Rules Ensure a Fair Trial? A Comparative Perspective on Evidentiary Rules*, Cham, 2019.

R. GUIDOTTI, A. MONREALE, S. RUGGIERI, F. TURINI, F. GIANNOTTI, D. PEDRESCHI, *A Survey of Methods for Explaining Black Box Models*, in *ACM Computing Surv*eys 51 (2018), n. 5, pp. 1 ss.

The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, First Edition. IEEE, 2019 (disponibile *online* al seguente indirizzo: https://standards.ieee.org/content/ieee-standards/en/industry-connections/ec/autonomous-systems.html, ultimo accesso il 30 giugno 2022).

F. LAGIOIA, G. CONTISSA, *The Strange Case of Dr. Watson: Liability Implications of AI Evidence-Based Decision Support Systems in Health Care*, in *European Journal of Legal Studies* 12 (2020), n. 2, pp. 245-289.

E.J. LANGE, *The Illusion of Control*, *Journal of Personality and Social Psychology* 32 (1975), n. 2, pp. 311 ss.

G. LASAGNI, Policing via Multi-Agent Systems*: un nuovo volto per la digital forensics (e non solo)?* in R. BRIGHI (a cura di), *Nuove Questioni di Informatica Forense*, Roma, 2022, pp. 303-321.

G. LASAGNI, *Admissibility of Digital Evidence*, in V. FRANSSEN, S. TOSZA (a cura di), *The Cambridge Handbook of Digital Evidence in Criminal Matters*, Cambridge, in corso di pubblicazione.

L. LUPARIA DONATI, *Notazioni controintuitive su intelligenza artificiale e libero convincimento*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, pp. 113 ss.

K. KREMENS, W. JASIŃSKI, D. CZERWIŃSKA, D. CZERNIAK, in *Poland. There and Back Again. A Struggle with Transposition of EU Directives*, in G. CONTISSA, G. LASAGNI, M. CAIANIELLO, G. SARTOR (a cura di), *Effective Protection of*

the Rights of the Accused in the EU Directives. A Computable Approach to Criminal Procedure Law, Leiden, 2022, pp. 154 ss.

A. KROLL, S. BAROCAS, E. FELTEN, J. R. REIDENBERG, D. G. ROBINSON, H. YU, *Accountable Algorithms*, in *University of Pennsylvania Law Review* 165, (2016), pp. 633 ss.

V. MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia,* in U RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, pp. 547 ss.

A. M. MAUGERI, *L'uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra* evidence based practices *e tutela dei diritti fondamentali*, in *Archivio penale – Rivista web*, 2021, n. 1, pp. 1 ss.

K. MILLER, *Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm*, in *Journal of Technology Law & Policy* 119 (2014), n. 1, p. 105.

J. MILLAR, I. KERR, *Delegation, Relinquishment and Responsibility: The Prospect of Expert Robots,* 17 marzo 2013, disponibile *online* su SSRN: https://ssrn.com/abstract=2234645.

C. O'NEIL, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, New York, 2016.

I. NERONI REZENDE, *Predictive policingsafeguards for the choice of data and automated processing in the preventive context*, in S. BARONA VILAR (a cura di), *Justicia algorítmica y neuroderecho: una mirada multidisciplinar*, Valencia, 2021, p. 361.

F. PALMIOTTO, *The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, in M. EBERS, M. CANTERO GAMITO (a cura di), *Algorithmic Governance and Governance of Algorithms. Legal and Ethical Challenges*, Cham, 2021, p. 49.

C. DUMBRAVA (*European Parliamentary Research Service*), *Artificial intelligence at EU borders. Overview of applications and key issues*, luglio 2021, disponibile *online* al seguente indirizzo: https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf (ultimo accesso il 30 giugno 2022).

S. QUATTROCOLO, *Quesiti nuovi e soluzioni antiche?* Consolidated regulatory paradigms *vs.* risks and fears of 'predictive' digital justice, in *Cass. pen.*, 2019, n. 4, pp. 1748 ss.

S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Cham, 2020.

S. QUATTROCOLO, *Intervento alla Conversazione del 20 ottobre 2020,* pubblicato in *Processo penale e Intelligenza Artificiale. Position Paper n. 1*, Fondazione Leonardo Civiltà delle Macchine, 2020, pp. 17 ss.

A. Renda *et alii*, *Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe*, 21 aprile 2021, disponibile *online* al seguente indirizzo: https://digital-strategy.ec.europa.eu/en/library/study-supporting-impact-assessment-ai-regulation (ultimo accesso il 30 giugno 2022).

U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020.

G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2020, n. 4, pp. 75 ss. (ora anche in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, pp. 9 ss.)

J.A.E. Vervaele, *Lawful and Fair Use of Evidence from a European Human Rights Perspective*, in F. Giuffrida, K. Ligeti (a cura di), *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings*, Lussemburgo, 2019, pp. 56 ss.

P.C. Wason, *On the failure to eliminate hypotheses in a conceptual task*, in *Quarterly Journal of Experimental Psychology* 3 (1960), n. 12, pp. 129 ss.

INTELLIGENZA ARTIFICIALE E RAGIONAMENTO PROBATORIO NEL PROCESSO PENALE

Luca Pressacco

1. Intelligenza artificiale e ricostruzione dei fatti: un binomio ineludibile

Il titolo della presente relazione propone un accostamento suggestivo e interessante, sebbene per certi versi ambiguo e, in ogni caso, assai problematico.

Suggestivo poiché evoca scenari "orwelliani"[1] – come quelli del "giudice-robot" ovvero della "decisione robotica"[2] – che hanno alimentato

[1] Per una breve riflessione, che prende spunto da un'opera letteraria di fantascienza (*rectius*: distopia) giudiziaria, v., da ultimo, M. CECCHI, *Sfogliando* Justice Machines*: evocazioni antesignane su diritto e intelligenza artificiale*, in *Cass. pen.*, 2021, n. 12, pp. 4172 ss.

[2] Apprezzabile lo sforzo definitorio compiuto da E. VINCENTI, *Il «problema» del giudice-robot*, in A. CARLEO (a cura di), *Decisione robotica*, Bologna, 2019, p. 111, il quale precisa che per «decisione robotica giudiziale» dovrebbe intendersi quella «basata sulla mera relazione tra i dati digitalizzati raccolti, la funzione logico-matematica che li orienta e lo strumento elettronico che li processa». In senso più ampio, invece, E. GABELLINI, *La «comodità del giudicare»: la decisione robotica*, in *Riv. trim. dir. e proc. civ.*, 2019, n. 4, p. 1306, ritiene invece, che sia lecito discorrere di "decisioni automatizzate e/o robotiche" in tutte le ipotesi in cui «una statuizione del giudice è interessata o in essa viene ricompresa in parte l'azione di algoritmi».

il dibattito scientifico più recente, suscitando legittime preoccupazioni, in virtù delle implicazioni che si intravedono nel settore della giustizia penale (e non solo)[3].

Interessante perché, anche in assenza di una definizione universalmente accolta del concetto in esame, l'intelligenza artificiale (d'ora in avanti, IA) viene generalmente intesa come «l'insieme dei metodi scientifici, [delle] teorie e [delle] tecniche finalizzate a riprodurre mediante le macchine le capacità cognitive degli esseri umani»[4]. Sorge, dunque,

[3] Sulla cosiddetta "decisione robotica", nell'ambito della letteratura più recente, cfr. A. Caratta, *Decisione robotica e valori del processo*, in *Riv. dir. process.*, 2020, n. 2, pp. 491 ss.; E. Gabellini, *Algoritmi decisionali e processo civile*, in *Riv. trim. dir. proc. civ.*, 2022, n. 1, pp. 59 ss.; A.A. Martino, *Chi teme i giudici robot*, in *Rivista italiana di informatica e diritto*, 2020, n. 2, pp. 15 ss. Nella prospettiva specificamente penalistica, v. anche M. Caterini, *Verso un diritto penale inumano*, in A. Bondi, G. Fiandaca, G.P. Fletcher, G. Marra, A.M. Stile, C. Roxin, K. Volk (a cura di), *Studi in onore di Lucio Monaco*, Urbino, 2020, pp. 199 ss.; nonché O. Di Giovine, *Il* judge-bot *e le sequenze giuridiche in materia penale (intelligenza artificiale e stabilizzazione giurisprudenziale)*, in *Cass. pen.*, 2020, n. 3, pp. 951 ss. Per un approccio culturale al tema della "decisione robotica" cui lo scrivente aderisce pienamente, v. A. Punzi, Judge in the Machine. *E se fossero le macchine a restituirci l'umanità del giudicare?*, in A. Carleo (a cura di), *Decisione robotica*, cit., pp. 319 ss. Infine, per un'efficace sintesi delle principali sfide che l'avvento delle tecnologie di intelligenza artificiale pone nei confronti del cosiddetto "paradigma della decisione", v. C. Casonato, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Diritto pubblico comparato ed europeo – Rivista web*, Speciale 2019, pp. 118 ss.

[4] Questa è la definizione contenuta nell'Appendice III della «Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi», adottata dalla Commissione europea per l'efficienza della giustizia (CEPEJ) nel corso della sua XXXI Riunione plenaria, Strasburgo, 3 dicembre 2018 [CEPEJ (2018) 14]. Come si può notare, si tratta di una definizione tendenzialmente "ricorsiva", poiché individua le tecnologie di intelligenza artificiale tramite il riferimento alle capacità cognitive degli esseri umani. Per una definizione "operativa", fondata invece sul tentativo di individuare le caratteristiche principali dell'intelligenza artificiale, v. il documento *A definition of AI: Main capabilities and scientific disciplines* redatto dall'*High-Level Expert Group on Artificial Intelligence* nominato dalla Commissione europea, Bruxelles, 18 dicembre 2018, p. 7: «Artificial intelligence (AI) refers to systems designed by humans that, given a complex goal, act in the physical or digital world by perceiving their environment, interpreting the collected structured or unstructured data, reasoning on the knowledge derived from this data and deciding the best action(s) to take (according to pre-defined parameters) to achieve the given goal». Per un approccio similare in dottrina, v. anche G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significati-*

spontaneo domandarsi se sia (tecnicamente) possibile e (giuridicamente) auspicabile l'impiego delle tecnologie fondate sull'IA per riprodurre le attività conoscitive che conducono alla ricostruzione fattuale definitiva in sede giudiziaria[5].

Ambiguo perché il riferimento al "ragionamento probatorio" se, da un lato, consente di circoscrivere l'indagine alle attività funzionali alla ricostruzione dei fatti[6]; dall'altro, reca con sé la vasta e complessa tematica della cosiddetta "logica del giudice"[7].

---

vo, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, p. 12. Sulla «natura composita ed eterogenea del fenomeno», la cui definizione appare «in continua evoluzione» e, per questa ragione, storicamente relativa, si sofferma, infine, G. Padua, *Intelligenza artificiale e giudizio penale: scenari, limiti, prospettive*, in *Processo penale e giustizia*, 2021, n. 6, p. 1481, distinguendo «tre diverse stagioni», lungo le quali si osservano mutamenti significativi nel modo di intendere il concetto di "intelligenza artificiale" ed il suo ambito di applicazione.

[5] Sulla necessità di privilegiare il termine «ricostruzione» in luogo del più tradizionale «accertamento» del fatto, v. – per tutti – G. Ubertis, *Fatto e valore nel sistema probatorio penale*, Milano, 1979, p. 93, spec. nt. 35. Nel medesimo senso, più di recente, P. Ferrua, *La prova nel processo penale*, I, *Struttura e procedimento*, 2017, pp. 16 ss.

[6] Si può, dunque, prescindere in questa sede dal contributo dell'intelligenza artificiale rispetto alle attività di ricognizione e di interpretazione delle norme e dei precedenti giurisprudenziali. Sulla possibilità e sull'opportunità di distinguere, nel contesto processuale, la *quaestio facti* dalla *quaestio iuris* – senza, peraltro, negare il loro collegamento dialettico e le loro reciproche interferenze – v. P. Comanducci, *La motivazione in fatto*, in G. Ubertis (a cura di), *La conoscenza del fatto nel processo penale*, Milano, 1992, pp. 222 ss., secondo cui tale distinzione rispecchia la «divisione tra discorsi assertivi e discorsi valutativo-prescrittivi» (*ivi*, p. 223). Analogamente, secondo P. Ferrua, *Il giudizio penale: fatto e valore giuridico*, in AA.VV., *La prova nel dibattimento penale*, Torino, 2007, p. 318, la distinzione nell'ambito del giudizio fra il tema storico e quello di valore giuridico corrisponde alla differenza tra «il discorso referenziale e il discorso legislativo». Sul punto, in prospettiva teorica generale, v. anche F. Cordero, *Giudizio*, in *Nov. Digesto It.*, VIII, Torino, 1961, p. 883; M. Taruffo, *Giudizio (teoria generale)*, in *Enc. Giur. Treccani*, XVI, Roma, 1989, pp. 2-3. Infine, per una posizione più articolata, cfr. G. Ubertis, *Fatto e valore nel sistema probatorio penale*, cit., pp. 70 ss., il quale sostiene che fra *quaestio facti* e *quaestio iuris* vi sia un rapporto dialettico, nell'ambito del quale «si può parlare soltanto di una distinzione metodologica tra i due termini della coppia, funzionale alle varie esigenze che, in differenti momenti, vengono in rilievo nell'ambito processuale» (*ivi*, p. 76).

[7] Non a caso, già diversi anni addietro in dottrina si era osservato come «interrogarsi sul tessuto inferenziale sotteso a un sistema intelligente finalizzato all'apprezzamento delle prove in un contesto giudiziale [equivalga] a esaminare, da un nuovo angolo pro-

Ciò nonostante, non ci si può esimere dal riflettere sulle implicazioni derivanti dall'impiego delle tecnologie di IA nella dimensione specifica del ragionamento probatorio, sia esso inteso come un'attività mentale oppure come l'insieme degli enunciati linguistici che della prima costituiscono il risultato e la sintesi razionale[8]. Ciò per almeno due ordini di ragioni.

In primo luogo, è noto che il settore probatorio risulta particolarmente esposto alle innovazioni tecnologiche, se non altro poiché queste ultime trovano sovente un primo terreno di applicazione nella fase delle indagini preliminari – come strumenti di investigazione, utilizzati dalle agenzie di *law enforcement* – e, in seguito, cingono d'assedio la "cittadella" del processo[9]. Secondariamente, non si può affermare che il tema sia privo di

---

spettico, la logica del giudice e gli elementi che ne vanno a comporre il ragionamento»: L. Luparia, *Introduzione. Prova giudiziaria e ragionamento artificiale: alcune chiavi di lettura*, in J. Sallantin, J.J. Szczeciniarz (a cura di), *Il concetto di prova alla luce dell'intelligenza artificiale*, Milano, 2005, p. XIV. Con ciò, evidentemente, riemerge tutta una serie di aporie concettuali, derivanti essenzialmente dal fatto che il termine "logica" può indicare «sia la 'scienza del pensiero' (rientrante nell'ambito della psicologia) sia la 'scienza del discorso' (descrivendo e costruendo le regole del linguaggio)»: G. Ubertis, *Fatto e valore nel sistema probatorio penale*, cit., p. 50. Analogamente, P. Comanducci, *op. cit*., p. 217, osserva che «'motivazione' e 'decisione' possono essere intese sia come attività che si svolgono nella mente del giudice sia come prodotti documentali di tali attività». D'altra parte, anche a prescindere da questa dicotomia, si è da tempo riconosciuto come non sia possibile né opportuno ricondurre il ragionamento del giudice entro comode visioni unilaterali (come, ad esempio, lo schema del sillogismo giudiziario) poiché tale ragionamento risulta intessuto di elementi «di volta in volta definibili secondo una o più forme logiche, oppure secondo schemi di qualificazione quasi logici o puramente topici, valutativi o retorici»: M. Taruffo, *La motivazione della sentenza civile*, Padova, 1975, p. 212. Per una recente indagine sul tema, v. da ultimo R. Poli, *Logica e razionalità nella ricostruzione giudiziale dai fatti*, in *Riv. dir. process.*, 2020, n. 2, pp. 515 ss.

[8] Da ultimo, sostiene che il «ragionamento» – inteso come «un processo mentale in forza del quale da dati noti si perviene a dati ignoti» – sia il «grande tema che lega il processo agli sviluppi dell'intelligenza artificiale», A. Venanzoni, *La valle del perturbante: il costituzionalismo alla prova delle intelligenze artificiali e della robotica*, in *Politica dir.*, 2019, n. 2, p. 252.

[9] Secondo G. Fiorelli, *Diritto probatorio e giudizi criminali ai tempi dell'Intelligenza Artificiale*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, Milano, 2022, p. 784, «la spinta evolutiva dell'Intelligenza Artificiale non si arresta al momento genetico del procedimento: travalica i confini segnati dalle indagini preliminari ed irrompe in sede

risvolti applicativi, considerato che già è possibile osservare la presenza, in talune vicende giudiziarie, di elementi di prova generati, raccolti o elaborati mediante l'ausilio delle tecnologie di IA[10]. La sola presenza di questi elementi impone di svolgere una riflessione sulle loro specifiche caratteristiche e sulle conseguenze derivanti dal loro ingresso sulla scena processuale[11].

Nel presente contributo l'attenzione sarà rivolta, in particolare, alla dimensione del ragionamento probatorio e, dunque, alle attività conoscitive poste in essere dalle parti e dal giudice per giungere a una ricostruzione fattuale definitiva in sede giudiziaria[12]. A tal fine si procederà

---

dibattimentale». Registrando il primo stadio dell'evoluzione descritta, M. Pisati, *Indagini preliminari e intelligenza artificiale: efficienza e rischi per i diritti fondamentali*, in *Processo penale e giustizia*, 2020, n. 4, p. 958, osserva invece che «le applicazioni dell'intelligenza artificiale nell'attività giurisdizionale penale, le quali destano fondate perplessità non sono, allo stato, riscontrabili nella prassi giudiziaria domestica, mentre proliferano gli strumenti tecnologici di assistenza all'attività investigativa e di *predictive policing*».

[10] Per non parlare delle ipotesi, rare ma non impossibili, in cui l'algoritmo costituisce di per sé stesso una fonte di prova, com'è accaduto – ad esempio – nel cosiddetto "*Dieselgate*". In tale vicenda, come ricorda F. Palmiotto, *The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, in M. Ebers, M. Cantero Gamito (a cura di), *Algorithmic Governance and Governance of Algorithms. Legal and Ethical Challenges*, Cham, 2021, p. 52, l'accusa mossa nei confronti di alcuni dirigenti del gruppo *Volkswagen* era proprio quella di aver installato illegalmente negli autoveicoli un *software* progettato per aggirare le normative ambientali sulle emissioni inquinanti da gasolio.

[11] La dottrina, d'altronde, sembra ben consapevole della necessità di approfondire lo studio del rapporto tra il fenomeno probatorio e le tecnologie di IA, come dimostrano alcuni recenti contributi. Con precipuo riferimento al processo penale, v. M. Gialuz, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, cit., pp. 51 ss.; K. Quezada-Tavárez, P. Vogiatzoglou, S. Royer, *Legal challanges in bringing AI evidence to the criminal courtroom*, in *New Journal of European Criminal Law*, 2021, n. 4, pp. 531 ss.

[12] L'approccio che qui si propone è simile a quello coltivato, in relazione al processo civile, da E. Fabiani, *Intelligenza artificiale e accertamento dei fatti nel processo civile*, in *Il giusto processo civile*, 2021, n. 1, pp. 45 ss., a dimostrazione della comunanza dei problemi che le discipline processuali si trovano volta per volta ad affrontare. Nella medesima prospettiva si è posto, da ultimo, anche A. Bonafine, *L'intelligenza artificiale applicata al ragionamento probatorio nel processo civile. È davvero possibile e/o auspicabile?*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, cit., pp. 923 ss.

come segue. In primo luogo, si osserverà l'incidenza delle tecnologie di IA sulle categorie dogmatiche impiegate tradizionalmente per descrivere il fenomeno probatorio (par. 2). In seguito, si analizzerà la disciplina che regola l'emissione delle decisioni automatizzate nel processo penale (par. 3), senza dimenticare le specificità che connotano tale settore dell'ordinamento (par. 4). Infine, dopo aver esaminato le funzioni che gli strumenti di IA possono svolgere nei diversi contesti epistemologici in cui si articola il procedimento giudiziario (par. 5), si passeranno in rassegna alcuni modelli di collaborazione tra uomo e macchina per la formulazione del giudizio di fatto (par. 6). Ciò che si vuole dimostrare, in linea con lo spirito del presente convegno, è che le applicazioni dell'IA nel processo penale non sono necessariamente foriere di conseguenze negative per la tutela dei diritti fondamentali. Al contrario, ove l'utilizzo di queste tecnologie fosse correttamente regolato e sottoposto al governo della legge, esse potrebbero persino contribuire proficuamente all'esplicazione del confronto dialettico tra le parti processuali e, dunque, alla ricostruzione dei fatti nel contesto di un processo penale di stampo tendenzialmente accusatorio.

2. Necessità di un rinnovato apparato concettuale

Prima di entrare in *medias res*, sembra opportuno svolgere alcune considerazioni preliminari, utili per comprendere il rapporto che intercorre tra IA e ricostruzione dei fatti nel processo penale.

Anzitutto, bisogna ammettere che l'irruzione dell'IA sulla scena processuale rende necessario predisporre un apparato concettuale rinnovato – mediante l'introduzione di nuove categorie o una differente interpretazione di quelle già esistenti – per descrivere il fenomeno probatorio alla luce dalla sopravvenuta evoluzione tecnologica[13]. Questa attività di ela-

[13] «Quel che è certo è che lo sviluppo tecnologico sta travolgendo l'intera nostra dogmatica della prova, ancora costruita sul modello della prova dichiarativa, come ai tempi della Rivoluzione francese»: F. Caprioli, *Tecnologia e prova penale: nuovi diritti e nuove garanzie*, L. Luparia, L. Marafioti, G. Paolozzi, *Dimensione tecnologica e prova penale*, Torino, 2019, p. 45. Nel medesimo senso, v. anche G. Riccio, *Ragionando su intelligenza artificiale e processo penale*, in *Archivio penale – Rivista web*, 2019, n. 3, p. 9 e, da ultimo, G. Spangher, *Le prove che utilizzano dati raccolti mediante strumenti*

borazione categoriale coinvolge, in linea di principio, tutti i livelli entro cui si svolge l'esperienza giuridica, come appare evidente non appena si sofferma l'attenzione su qualche esempio specifico.

Sul versante legislativo, merita segnalare l'art. 2 lett. e) d.lgs. 18 maggio 2018 n. 51[14], che fornisce la definizione di "profilazione" rilevante quando il trattamento dei dati personali viene realizzato dalle autorità competenti per finalità di prevenzione, indagine, accertamento dei reati o esecuzione di sanzioni penali[15]. Secondo questa disposizione, per "profilazione" si intende «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica». Il pensiero corre immediatamente ai *software* utilizzati nell'esperienza nordamericana per quantificare il rischio di commissione di nuovi reati da parte dei soggetti sottoposti a procedimento penale[16], ma

---

digitali (inoltre: captatore informatico; perquisizioni on line*)*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, cit., p. 760. In termini generali, cfr. anche G. Tuzet, *L'algoritmo come pastore del giudice? Diritto, tecnologie, prova scientifica*, in *Media Laws – Rivista di diritto dei Media*, 2020, n. 1, p. 48, il quale – dopo aver ricordato che «uno strumento tradizionale per far fronte alle novità è l'analogia» – precisa che, quando il ricorso a tale risorsa ermeneutica si rivela insufficiente, «occorre configurare dei nuovi assetti normativi per far fronte alle nuove esigenze»

[14] D.lgs. 18 maggio 2018 n. 51, recante «Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio», in GU 24 maggio 2018 n. 119, pp. 1 ss.

[15] La profilazione, in realtà, è una tecnica di trattamento dei dati personali che può essere effettuata con finalità differenti, ad esempio per motivi commerciali (profilazione del consumatore) o politici (profilazione degli elettori). Sul rapporto fra tecniche di profilazione e libertà di manifestazione del pensiero v., anche per ulteriori riferimenti bibliografici, M. Fasan, *Intelligenza artificiale e pluralismo: uso delle tecniche di profilazione nello spazio pubblico democratico*, in *BioLaw Journal – Rivista di biodiritto*, 2019, n. 1, pp. 101 ss.

[16] Per gli opportuni approfondimenti sul punto, v. *infra*, cap. IV.

non è difficile immaginare le potenzialità applicative delle operazioni di profilazione, anche in chiave diagnostica. Tali operazioni, infatti, potrebbero essere svolte, sin dalla fase delle indagini preliminari, per estrarre informazioni a partire da un insieme di "dati grezzi", disponibili negli archivi pubblici e privati cui le forze dell'ordine o l'autorità giudiziaria abbiano accesso[17], oppure ricavati mediante strumenti di captazione occulta. È facile prevedere, ad esempio, che informazioni concernenti la situazione economica, le abitudini o gli spostamenti di un determinato individuo potrebbero assumere notevole rilievo probatorio nel contesto di un procedimento penale.

Volgendo ora lo sguardo al piano della elaborazione dottrinale, viene in rilievo la categoria della "*Automated-Generated Evidence*", la quale costituisce una specie particolare della "*Machine-Generated Evidence*"[18]. Con questa locuzione, gli studiosi si riferiscono usualmente a quei dati che vengono generati o raccolti automaticamente, per finalità differenti da quelle tipiche del procedimento penale, prevalentemente di natura commerciale.

Si pensi, a titolo esemplificativo, ai cosiddetti "dati esterni" delle comunicazioni (durata, soggetti coinvolti, localizzazione dei dispositivi), i quali – raccolti dai fornitori dei servizi di telecomunicazioni per esigenze

[17] V., ad esempio, l'art. 1 commi 682 e 686 l. 27 dicembre 2019 n 160, che consente all'Agenzia delle entrate e alla Guardia di finanza di utilizzare i dati contenuti nell'Archivio dei rapporti finanziari, avvalendosi delle tecnologie, delle elaborazioni e delle interconnessioni con le altre banche dati, di cui esse dispongono, allo scopo di individuare criteri di rischio utili per individuare posizioni fiscali da sottoporre a controllo. Per una ricognizione delle modalità di utilizzo "integrato" delle banche dati a disposizione dell'amministrazione fiscale, v. P. Sorbello, *Banche dati, attività informativa e predittività. La garanzia di un diritto penale del fatto*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2019, n. 2, pp. 380 ss., ove si trova anche l'esempio del Sistema Informativo Antifrode (SIAF), una piattaforma informatica utilizzata dalla Guardia di finanza per migliorare l'analisi di rischio e così potenziare il contrasto alle frodi in danno del bilancio dell'Unione europea (*ivi*, p. 384, nt. 56).

[18] Sul punto, anche per ulteriori riferimenti bibliografici, v. M. Pisati, *op. cit*., p. 959, il quale – rifacendosi alla tradizionale suddivisione tra *computer-derived evidence* e *computer-generated evidence* – distingue le ipotesi in cui i sistemi basati sull'IA siano oggetto di un accertamento investigativo o probatorio dai casi in cui tali sistemi, invece, siano utilizzati in funzione di analisi o di classificazione di informazioni raccolte in precedenza dagli organi inquirenti.

aziendali – sono suscettibili di trasformarsi in elementi probatori, utili per la ricostruzione dei fatti nel processo. In questa prospettiva, d'altronde, il legislatore ha introdotto specifiche disposizioni di legge che impongono ai soggetti obbligati la conservazione dei dati in questione, disciplinandone le modalità di acquisizione da parte dell'autorità giudiziaria[19].

Ebbene, proprio con riferimento alla categoria della *automated generated evidence*, la dottrina più sensibile ha evidenziato il rischio che l'avvento delle "prove digitali" o "algoritmiche" generi un grave squilibrio conoscitivo (*knowledge impairment*) tra le parti processuali, ponendo in tal modo a repentaglio il fondamentale principio di parità delle armi. Ciò, soprattutto a causa della difficoltà che incontrerebbero le medesime parti processuali – in particolare, la difesa – nel contestare l'accuratezza e l'attendibilità degli elementi di prova ottenuti tramite l'ausilio delle nuove tecnologie di IA[20].

Infine, per completare questa breve rassegna senza trascurare il formante giurisprudenziale, può essere utile soffermarsi sulla nozione della cosiddetta "probabilità logica". Essa si identifica tradizionalmente con il grado di conferma dell'ipotesi formulata in ordine al fatto da provare e si distingue dalla cosiddetta "probabilità statistica" poiché contiene la verifica aggiuntiva – realizzata sulla base dell'intera evidenza disponibile – dell'attendibilità dell'impiego della legge scientifica di copertura

[19] Sugli obblighi di conservazione e sulle modalità di acquisizione dei dati relativi al traffico telefonico e telematico per finalità di accertamento e repressione dei reati cfr. l'art. 132 d.lgs. 30 giugno 2003 n. 196. Tale disposizione, peraltro, è stata oggetto di significative modifiche ad opera del d.l. 30 settembre 2021 n. 132, per adeguare la normativa italiana agli *standard* di tutela della riservatezza imposti dalla giurisprudenza delle corti europee di Strasburgo e di Lussemburgo. Sul punto, *ex multis*, v. F.R. Dinacci, *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia: luci europee e ombre legislative*, in *Processo penale e giustizia*, 2022, n. 2, pp. 301 ss.

[20] Sul punto, v. U. Pagallo, S. Quattrocolo, *The impact of AI on criminal law, and its twofold procedures*, in W. Barfield, U. Pagallo (a cura di), *Research Handbook on the Law of Artificial Intelligence*, Cheltenham-Northampton, 2018, pp. 395 ss. Per ulteriori approfondimenti al riguardo, cfr. anche S. Quattrcolo, *Equità del processo penale e* automated evidence *alla luce della Convenzione europea dei diritti dell'uomo*, in *Revista italo-Española de Derecho Procesal*, 2019, n. 2, pp. 1 ss.; ead., *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *Media Laws – Rivista di diritto dei Media*, 2020, n. 3, pp. 126 ss.; nonché F. Palmiotto, *op. cit.*, pp. 58-61; K. Quezada-Tavárez, P. Vogiatzoglou, S. Royer, *op. cit*., pp. 542-545.

in relazione al singolo evento. Com'è noto, muovendo dalla nozione di "probabilità logica", la Cassazione ha delineato un criterio metodologico, che consente di addivenire a una pronuncia di condanna soltanto in presenza di una ricostruzione fattuale dotata di una «elevata probabilità razionale», secondo l'insegnamento offerto a partire dalla celeberrima sentenza Franzese[21].

La Cassazione affermò, in particolare, che il nesso causale tra condotta ed evento può ritenersi sussistente anche in presenza di una legge di copertura fondata su frequenze statistiche medio-basse, purché gli ulteriori elementi probatori a disposizione del giudice siano tali da escludere la verificazione di decorsi causali alternativi. Così, è stato delineato un itinerario metodologico che richiede di porre in relazione elementi di prova differenti, alcuni dei quali suscettibili di valutazione soltanto mediante il ricorso a leggi scientifiche di copertura; mentre altri necessitano di una valutazione fondata sulle cosiddette "massime di esperienza"[22].

Non è detto che questo approccio metodologico debba necessariamente mutare nel prossimo futuro. Ciò che preme sottolineare, invece, è che tale modalità di verifica del nesso causale potrebbe oggi giovarsi

[21] Cass. pen., sez. un., sent. 10 luglio 2002 n. 30328, in *Riv. it. dir. proc. pen.*, 2002, pp. 1133 ss. Per una retrospettiva dei risvolti giuridici ed epistemologici di tale pronuncia, cfr. – con varietà di accenti e opinioni – E. Ancona, *All'origine della svolta epistemologica della sentenza Franzese. ricerche sulla probabilità logica o baconiana*, in *Rivista internazionale di filosofia del diritto*, 2017, n. 4, pp. 679 ss.; F. D'Alessandro, *Spiegazione causale mediante leggi scientifiche, a dieci anni dalla sentenza Franzese*, in *Criminalia*, 2012, pp. 331 ss.; F.M. Iacoviello, *La "Franzese": ovvero quando buone teorie producono cattiva giustizia*, in *Critica del diritto*, 2014, n. 3, pp. 241 ss.; P. Tonini, *L'influenza della sentenza Franzese sul volto attuale del processo penale*, in *Dir. pen. proc.*, 2012, n. 10, pp. 1225 ss.

[22] «La spiegazione causale raggiunta attraverso la sussunzione dell'accadimento storico nella base scientifica probabilistica deve essere infatti corroborata (*rectius*: verificata) alla stregua delle concrete e singolari circostanze della fattispecie concreta, al fine di escludere ipotesi esplicative alternative… Si tratta del c.d. procedimento di 'abduzione selettiva'»: T. Padovani, *Diritto penale*, Milano, 2019, p. 161. Nel medesimo senso, v. anche O. Mazza, *Il ragionevole dubbio nella teoria della decisione*, in *Criminalia*, 2012, p. 360: «la probabilità statistica, desunta dalla legge scientifica di copertura, non è il criterio tautologico di valutazione della prova o di giudizio, bensì un elemento di prova che va valutato unitamente a tutte le altre evidenze del caso concreto le quali, a loro volta, devono consentire di escludere l'incidenza di altri fattori interagenti».

delle capacità computazionali tipiche dei *software* di IA[23]. Questi ultimi, in altre parole, potrebbero costituire utili strumenti di ausilio per l'emissione delle decisioni giurisdizionali nei contesti probatori complessi, modificando lo stesso modo di intendere (*rectius*: verificare) il grado di conferma delle ipotesi esplicative antagoniste, vale a dire la loro "probabilità logica"[24]. Si badi bene: ciò non significa pretendere di misurare esattamente tale grado di conferma, quanto piuttosto riconoscere l'esigenza che la ricostruzione giudiziale dei fatti si svolga in un contesto probabilisticamente coerente, cioè rispettoso degli assiomi fondamentali del calcolo delle probabilità[25].

In ogni caso, al di là delle esemplificazioni sommariamente illustrate, occorre essere ben consapevoli dello sfondo sul quale si collocano le singole questioni che attengono al rapporto tra IA e processo penale, specialmente per quanto riguarda il settore probatorio. Non sembra, infatti, eccessivo affermare che la disponibilità e l'uso delle tecnologie fondate sull'IA per coadiuvare il giudice e le parti nella ricostruzione dei fatti sono fattori idonei a incidere in modo significativo sui metodi di pro-

[23] Nella medesima direzione, v. già C. Costanzi, *La matematica del processo: oltre le colonne d'Ercole della giustizia penale*, in *Questione giustizia*, 2018, n. 4, pp. 166 ss., il quale – proprio muovendo da un'analisi del significato della sentenza Franzese nel panorama dell'epistemologia giudiziaria contemporanea – giunge ad affermare che «l'inesorabile sviluppo della matematica del processo sembra offrire realmente al sistema giudiziario un compendio di algoritmi cognitivi sempre più sofisticati, in grado di supportare – non surrogare – il giudicante nel perseguimento di una maggiore prevedibilità delle decisioni ed eliminazione delle anamorfosi» (*ivi*, p. 188).

[24] Si è, infatti, ancora osservato – sempre con riferimento alla questione del nesso causale nei reati omissivi impropri – «come il recupero di uno strumento c.d. induttivo nell'accertamento del nesso di dipendenza causale tra condotta omissiva ed evento [possa] condurre ad un indebolimento del carattere 'nomologico' (o scientifico) del giudizio condizionalistico, iniettando in esso incontrollabili (e non falsificabili) componenti valutative, rimesse alla discrezionalità (e all'intuizionismo soggettivo) dell'organo giudicante»: T. Padovani, *op. cit*., p. 168.

[25] D'altra parte, gli assiomi fondamentali del calcolo delle probabilità rappresentano leggi logiche o scientifiche che ben potrebbero fungere da criteri di valutazione probatoria *ex* art. 192 comma 1 c.p.p. e che – lungi dal deprimere il libero convincimento del giudice – ne garantiscono una declinazione razionale. Non si vede, dunque, il motivo per cui il loro utilizzo dovrebbe essere inibito proprio in sede giudiziaria.

duzione della cosiddetta "verità giudiziale"[26] e, dunque, sul rapporto tra individuo e autorità in un determinato frangente storico[27].

Occorre guardarsi, in particolare, dal pericolo che l'IA possa trasformarsi in una sorta di nuova «vorace potenza superlogica», prendendo a prestito l'immaginifica locuzione coniata da Franco Cordero molti anni or sono[28]. Com'è noto, l'illustre autore si riferiva alle torsioni subite dal principio del libero convincimento del giudice che, nel vigore del c.p.p. 1930, era stato evocato strumentalmente al di fuori della sua dimensione tipica – quella della valutazione probatoria – per giustificare l'utilizzo di prove illegittimamente acquisite nel processo[29]. Nella contingenza storica attuale, invece, il pericolo che si intravede è che la disponibilità di tecnologie fondate sull'IA induca gli organi preposti alla prevenzione e alla repressione dei reati a servirsi di dati raccolti o trattati in violazione delle libertà fondamentali degli individui (in particolare, del diritto alla riservatezza sancito dall'art. 8 Conv. eur. dir. uomo e del diritto alla protezione dei dati stabilito dall'art. 8 Carta dir.

[26] Sul concetto di "verità giudiziale" v., per tutti, G. Ubertis, *Fatto e valore nel sistema probatorio penale*, cit., p. 129: «La ricostruzione fattuale cui si perviene al termine del processo è conforme a quella che – ritualmente ricercata e ottenuta – può essere definita come *verità giudiziale*. Essa è tale sia perché conseguita nel giudizio, inteso come fase processuale o 'luogo' in cui dialetticamente si realizza, sia perché derivante dal giudizio, inteso tanto come attività di ricerca degli elementi su cui si fonda una deliberazione quanto come formazione di quest'ultima, sia perché manifestata tramite il giudizio, inteso come decisione e sua definitiva pronuncia giurisdizionale». Per un accenno fugace e provocatorio alla "verità digitale", quale orizzonte gnoseologico tipico del processo penale del futuro più o meno prossimo, v. F. Caprioli, *op. cit*., p. 45.

[27] Nella medesima direzione, se non ci inganniamo, sembra orientato anche N. Irti, *Il tessitore di Goethe (per la decisione robotica)*, in A. Carleo (a cura di), *Decisione robotica*, cit., p. 20, in particolare laddove riconosce che «l'insopprimibile momento della soggettività, la quale … non rispecchia i dati ma li costruisce e li conforma … è anche il luogo dei conflitti di potere, che non sono 'neutralizzati' o composti dalla tecnica robotica ma, per così dire, spostati alla fase di scelta delle informazioni. Qui il potere giudiziario trova la sua nuova sede».

[28] F. Cordero, *Diatribe sul processo accusatorio* (1966), in *Ideologie del processo penale (con un'appendice)*, Roma, 1997, p. 213.

[29] Per un'efficace sintesi retrospettiva di questa involuzione, v. M. Nobili, *Esiti, errori, arbitrii dietro un'illustre formula: gli ultimi trent'anni*, in *Il libero convincimento del giudice penale. Vecchie e nuove esperienze*, Milano, 2004, pp. 33 ss.

fond. UE) al fine sfruttare le potenzialità computazionali tipiche delle tecnologie in esame[30].

In questa prospettiva, lo scandalo che ha coinvolto la società statunitense *Clearview* – una controversa *start-up* che elabora algoritmi di riconoscimento facciale – assume un significato (sinistramente) emblematico. Com'è noto, al fine di costruire un archivio di dati biometrici, tale società ha sistematicamente sottratto e trattato illecitamente le immagini dei volti di milioni di persone, estraendole dai *social network* più comuni, come *Facebook*, *YouTube*, *Twitter*, *Instagram* e *Linkedin*. Al di là della vicenda concreta e delle sanzioni irrogate[31], ciò testimonia, da una parte, la facilità con cui si realizzano violazione estese e sistematiche della disciplina sul trattamento dei dati personali; dall'altra parte, l'incentivo perverso che cattura sia gli operatori di mercato (indotti ad avallare prassi illegittime pur di assicurarsi maggiori profitti), sia le agenzie di *law enforcement* (sospinte ad avvalersi degli ultimi ritrovati della tecnologia, con l'illusione di svolgere con maggiore incisività la propria funzione di prevenzione e di repressione dei reati).

3. Intelligenza artificiale e decisioni automatizzate nel processo penale

Esaurite le premesse concettuali, occorre immediatamente avvertire che nel nostro ordinamento vi sono già alcune disposizioni che si occupano dell'utilizzo di strumenti fondati sulle tecnologie di IA ai fini dell'emissione di decisioni giurisdizionali. Tali previsioni coinvolgono, naturalmente, anche la dimensione del ragionamento probatorio, nella misura in cui le attività di deliberazione e di giustificazione della sentenza richiedono al giudice di valutare gli elementi di prova legittimamente acquisiti nel corso del processo.

Viene in rilievo, anzitutto, l'art. 11 dir. 2016/680/UE, cui è stata data attuazione tramite l'art. 8 del già citato d.lgs. 18 maggio 2018 n. 51, con-

[30] Sul punto, *mutatis mutandis*, v. *supra* cap. I, § 3 spec. nt. 73-74.

[31] Per un'analisi dei profili giuridici della vicenda *Clearview*, condotta muovendo dalla specifica prospettiva europea, v. I. Neroni Rezende, *Facial recognition in police hands: Assessing the Clearview case from a European perspective*, in *New Journal of European Criminal Law*, 2020, n. 3, pp. 375 ss.

cernente la protezione delle persone fisiche con riguardo al trattamento dei dati personali con finalità di prevenzione, indagine e perseguimento di reati. Tale ultima disposizione sancisce espressamente (co.1) che «sono vietate le decisioni basate unicamente su un trattamento automatizzato, compresa la profilazione, che producono effetti negativi nei confronti dell'interessato, salvo che siano autorizzate dal diritto dell'Unione europea o da specifiche disposizioni di legge».

In linea di principio, si può affermare che la *ratio* della norma sia quella di evitare che decisioni pregiudizievoli nei confronti di un determinato soggetto siano assunte direttamente da elaboratori artificiali, sulla base di un trattamento automatizzato di dati.

Tuttavia, è agevole osservare che la disposizione in commento non stabilisce un vero e proprio divieto, come si evince anche dal suo tenore letterale[32]. Essa prevede, invece, una riserva di legge così che l'emissione di decisioni basate unicamente su trattamenti automatizzati non risulta affatto preclusa, nei casi in cui ciò sia espressamente previsto dalle normative nazionali o dell'Unione europea.

Nei casi in cui la riserva in questione sia stata attuata, l'art. 8, co.2, d.lgs. 18 maggio 2018 n. 51 stabilisce che «le disposizioni di legge devono prevedere garanzie adeguate per i diritti e le libertà dell'interessato»; precisando, altresì, che «in ogni caso [deve essere] garantito il diritto di ottenere l'intervento umano da parte del titolare del trattamento». Si conferma, dunque, la natura relativa del divieto, visto che il controllo umano sulla decisione automatizzata non è oggetto di un obbligo per il soggetto titolare del trattamento, ma di un diritto (*rectius*: potere) il cui esercizio è rimesso alla determinazione discrezionale di coloro che subiscano gli effetti di una decisione siffatta[33]. Ciò significa che, in mancanza di una

[32] Nel medesimo senso, v. L. Luparia, *Diritto probatorio e giudizi criminali ai tempi dell'intelligenza artificiale*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, cit., p. 782.

[33] Sul punto, v. S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, p. 101, che ricava dalla disposizione in esame l'esistenza di un «nuovo diritto, che potremmo definire diritto a decisioni non basate esclusivamente su trattamenti automatizzati, inteso quale diritto da parte dei soggetti a non essere destinatari di decisioni che poggino in via esclusiva su trattamenti automatizzati». Da questa angolazione visuale, sembra corretto affermare che la dir. 2016/680/UE abbia inteso for-

richiesta diretta ad ottenere l'intervento umano in funzione di controllo sulla decisione automatizzata, quest'ultima sarebbe perfettamente legittima (purché, s'intende, assunta nei casi previsti dalla legge e corredata dalle opportune garanzie)[34].

L'ambito di applicazione della norma, peraltro, non è di agevole individuazione. Difatti, è legittimo chiedersi se oggetto del divieto – nei termini in cui è stato delineato in precedenza – sia solamente l'adozione di decisioni giurisdizionali attraverso *software* di IA; oppure se esso si estenda fino a ricomprendere anche l'emissione di decisioni giurisdizionali fondate in modo esclusivo o determinante su elementi probatori generati o raccolti tramite l'impiego di tecnologie di IA.

Il dato letterale farebbe propendere per l'interpretazione più lata, visto che oggetto del divieto sono tutte le «decisioni *basate unicamente* su un trattamento automatizzato». In favore di questa soluzione ermeneutica depone anche un'ulteriore circostanza: l'art. 8 co.1 d.lgs. 18 maggio 2018 n. 51 – così come l'art. 11 § 1 dir. 2016/680/UE di cui il primo costituisce attuazione – menziona esplicitamente la «profilazione» quale trattamento non idoneo a fondare in via esclusiva una decisione emessa con finalità di prevenzione e repressione dei reati. Questo inciso assume un significato compiuto solamente ipotizzando una decisione assunta

---

nire ai soggetti interessati una tutela più ampia rispetto a quella stabilita dalla disciplina generale sul trattamento dei dati personali. Per rendersi conto di ciò è sufficiente osservare che, in base all'art. 11 § 1 dir. 2016/680/UE, i soggetti destinatari di una decisione automatizzata assunta per finalità di prevenzione e repressione dei reati potrebbero indubbiamente prestare acquiescenza rispetto agli effetti di tali decisioni. Tuttavia, essi non potrebbero rinunciare preventivamente al diritto di sollecitare un intervento umano in funzione di controllo da parte del titolare del trattamento. Ciò, invece, risulta consentito dall'art. 22 § 2 lett. c) reg. 2016/679/UE (cosiddetto "GDPR"), nei casi in cui la decisione in questione «si basi sul consenso esplicito dell'interessato».

[34] In termini critici, al riguardo, v. 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. process.*, 2021, pp. 107 ss., la quale sostiene che la decisione algoritmica si ponga in contrasto insanabile con il diritto al rispetto della dignità umana e che «tale violazione non potrebbe ritenersi sanata dal successivo (oltretutto eventuale) intervento umano» (*ivi*, p. 108). Di conseguenza, l'autrice dubita «della legittimità dell'art. 11 dir. 2016/680/UE e dell'art. 8, d.lgs. 18 maggio 2018, n. 51 nella parte in cui essi prevedono che la decisione robotica possa essere autorizzata dal diritto dell'Unione o degli Stati membri» (*ivi*, p. 109).

sulla base di questa specifica tipologia di trattamento. Ciò accadrebbe, per esempio, nel caso in cui un provvedimento concernente la detenzione cautelare fosse emesso esclusivamente sulla base delle risultanze di una profilazione funzionale a stabilire il rischio di recidiva del destinatario della misura. Nel disegno normativo, dunque, l'emissione del provvedimento costituisce un'entità concettualmente distinta – e logicamente successiva – rispetto al trattamento di dati personali, su cui la prima risulta fondata.

Muovendo da queste considerazioni, si giunge ad affermare che la disposizione in commento non si limita a vietare l'emissione (*rectius*: la deliberazione) di provvedimenti giurisdizionali tramite strumenti di IA, ma prescrive anche una regola negativa di valutazione della prova, analoga a quella prevista dall'art. 192, co.2 c.p.p. Di conseguenza, gli elementi generati o raccolti attraverso tecnologie di IA dovrebbero essere considerati alla stregua di veri e propri indizi, almeno per quanto concerne le modalità di valutazione delle prove algoritmiche[35].

Infine, può essere interessante notare che l'art. 8, co.1 d.lgs. 18 maggio 2018 n. 51 vieta le decisioni basate esclusivamente su un trattamento automatizzato, nella misura in cui queste ultime producono *effetti negativi* nei confronti dei soggetti interessati[36]. *Quid iuris*, dunque, se gli ele-

[35] In questa direzione, almeno per quanto a nostra conoscenza, si è mosso per primo M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Diritto penale contemporaneo – Archivio web*, 29 maggio 2019, p. 17: «Insomma, accanto all'obbligo di un intervento umano andrebbe ritenuta sussistente quella che, nel lessico processualpenalistico, chiameremmo regola di valutazione, in forza della quale l'*output* prodotto dall'IA va considerato come un mero indizio, che va sempre corroborato con altri elementi di prova … Di regola, pertanto, non ci si può accontentare di questo [intervento umano, ma] occorre che l'elemento cognitivo generato dall'intelligenza artificiale sia confermato da altre fonti». Sul punto v. anche *infra*, § 5.3.

[36] Non si può fare a meno di notare la discrepanza testuale che intercorre fra la disposizione in commento e l'art. 11 § 1 dir. 2016/680/UE, di cui la norma interna costituisce attuazione. La disposizione europea, infatti, prevede 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». Benché si tratti solamente di una lieve discrepanza, sembra legittimo domandarsi se la normativa interna abbia introdotto una restrizione effettiva del contenuto precettivo della norma europea e se, dunque, debba considerarsi legittima oppure in contrasto con la direttiva da cui trae origine.

menti generati o raccolti mediante tecnologie di IA dovessero ridondare a favore dell'imputato?

Sembra riproporsi, sotto nuove sembianze, l'antica diatriba dottrinale sull'efficacia delle prove illegittimamente acquisite, le quali sarebbero inutilizzabili *contra reum*, mentre – secondo parte della dottrina – potrebbero essere oggetto di valutazione in favore dell'imputato[37]. Riecheggia, in modo analogo, il dibattito sviluppatosi più di recente intorno al significato e alla portata dell'art. 526, comma 1-*bis* c.p.p., che – secondo alcuni autori – consentirebbe di utilizzare le dichiarazioni rese da soggetti che si siano volontariamente sottratti al confronto con l'imputato, purché si rivelino favorevoli a quest'ultimo[38]. Sembra, dunque, significativo, anche alla luce dei "precedenti" cui si è rapidamente accennato, che il legislatore italiano si sia riferito unicamente alle decisioni che producono *effetti pregiudizievoli* nei confronti dei soggetti interessati, con ciò discostandosi dal tenore letterale delle corrispondenti disposizioni europee.

4. Segue*: applicazioni dell'intelligenza artificiale e specificità della giustizia penale*

Esaminati i vincoli legislativi stabiliti in via generale nei confronti

[37] In questo senso, v. F. Cordero, *Prove illecite* (1961), in *Tre studi sulle prove penali*, 1963, p. 171, il cui pensiero è stato ripreso, recentemente, anche da F. Caprioli, *Verità e giustificazione nel processo penale*, in G. Forti, G. Varraso, M. Caputo (a cura di), *«Verità» del precetto e della sanzione alla prova del processo*, Napoli, 2014, pp. 204-205, ricordando che «l'accertamento dell'innocenza è una posta troppo importante, per essere sacrificata agli idoli della procedura». Sul punto, anche per ulteriori riferimenti bibliografici, v. anche D. Vicoli, *La "ragionevole durata" delle indagini*, Torino, 2012, pp. 170 ss., spec. p. 178.

[38] Sul punto, v. P. Ferrua, *La prova nel processo penale*, I, *Struttura e procedimento*, cit., p. 55, secondo cui l'art. 526 comma 1-*bis* c.p.p. «a prima vista appare come una regola di esclusione perché le dichiarazioni in parola non possono in alcun modo provare la colpevolezza, neppure se unite ad altre prove o utilizzate come semplici elementi di riscontro. Ma la dizione della norma lascia intendere che è, invece, possibile il loro uso in chiave difensiva, a favore dell'imputato; si tratta, quindi, di un criterio di valutazione grazie al quale le dichiarazioni potranno essere acquisite al processo e valutate *in utilibus*, ferma restando la loro assoluta inidoneità a provare la colpevolezza». Per ulteriori approfondimenti, v. anche M. Daniele, *Regole di esclusione e regole di valutazione della prova*, Torino, 2009, pp. 161 ss.

delle decisioni automatizzate, è necessario adesso tenere in debita considerazione le "specificità" proprie della giustizia penale, anche nei confronti dei settori contigui dell'ordinamento. Tali specificità, infatti, sono state riconosciute non solo dalla dottrina, ma anche dai principali documenti internazionali che, nel contesto europeo, si sono occupati delle applicazioni dell'IA nell'ambito del processo penale.

La già menzionata Carta etica europea sull'utilizzo dell'IA nei sistemi di giustizia, ad esempio, afferma esplicitamente che il ricorso alle tecnologie in questione nel settore della giustizia penale «deve essere esaminato con le massime riserve»[39], mentre se ne auspica l'impiego nei settori civile, commerciale e amministrativo per migliorare la prevedibilità dell'applicazione delle norme giuridiche e la coerenza delle decisioni giudiziarie. In modo ancor più radicale, la risoluzione del Parlamento europeo del 6 ottobre 2021 sull'IA nel diritto penale[40] invita addirittura le istituzioni dell'Unione a bandire «l'uso dell'intelligenza artificiale e delle relative tecnologie per l'emanazione delle decisioni giurisdizionali» (§ 16)[41].

Anche se si tratta di strumenti di *soft law*, la convergenza dei documenti in questione appare, comunque, assai significativa. Essi, infatti, esprimono le medesime riserve in ordine alle applicazioni dell'IA nel processo penale, specialmente per quanto riguarda l'impiego delle tecnologie in esame in funzione di supporto all'emissione di decisioni giurisdizionali.

D'altra parte, per quanto concerne l'ordinamento italiano, non si può trascurare che nelle ultime decadi si è assistito a un progressivo approfondimento delle regole di decisione su cui è fondata la sentenza dibatti-

[39] Sul punto, v. l'Appendice I (Studio approfondito sull'utilizzo dell'intelligenza artificiale [IA] nei sistemi giudiziari, segnatamente delle applicazioni dell'intelligenza artificiale al trattamento di decisioni e dati giudiziari) della «Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi», spec. § 117 ss.

[40] Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale, in G.U.U.E. 24 marzo 2022, n. C 132, pp. 17 ss.

[41] Per un primo commento al documento di indirizzo politico approvato dal Parlamento europeo, v. G. Barone, *Intelligenza artificiale e processo penale: la linea dura del Parlamento europeo. Considerazioni a margine della Risoluzione del Parlamento europeo del 6 ottobre 2021*, in *Cass. pen.*, 2022, n. 3, pp. 1180 ss.

mentale; nonché ad un parallelo rafforzamento degli obblighi motivazionali che gravano sull'organo giurisdizionale e dei corrispondenti poteri di controllo.

Dal primo punto di vista, basti ricordare la modifica dell'art. 533 c.p.p. ad opera della l. 20 febbraio 2006 n. 46, che ha inteso irrobustire la tutela della presunzione d'innocenza quale regola di giudizio nell'ambito del processo penale[42]. Nella seconda direzione, invece, si può citare la novella dell'art. 546 c.p.p., riformulato dalla l. 23 giugno 2017 n. 103 al fine di precisare analiticamente il contenuto della motivazione del provvedimento, in particolare per quanto attiene alla risoluzione della *queastio facti*[43]. Infine, per quanto concerne il controllo sui vizi della motivazione, giova rammentare che la l. 20 febbraio 2006 n. 46 era intervenuta pure sul testo dell'art. 606 comma 1 lett. e) c.p.p., ampliando le fonti della cognizione *ex actis* devoluta alla Corte di cassazione. Com'è noto, in seguito a questo intervento legislativo, la patologia che affligge la motivazione non deve necessariamente emergere dal «testo del provvedimento impugnato», potendosi tenere conto anche di tutti gli atti del processo «specificamente indicati nei motivi di gravame».

In questa sede non è importante soffermarsi sui dettagli dei singoli interventi normativi. Giova, piuttosto, segnalare come queste modifiche

---

[42] Al riguardo, senza pretesa di completezza, v. C. Conti, *Al di là del ragionevole dubbio*, in A. Scalfati (a cura di), *Novità su impugnazioni penali e regole di giudizio. Legge 20 febbraio 2006, n. 46 "legge Pecorella"*, Torino, 2006, pp. 87 ss.; P. Ferrua, *La colpevolezza oltre ogni ragionevole dubbio*, in L. Filippi (a cura di*), Il nuovo regime delle impugnazioni tra Corte costituzionale e sezioni unite*, Padova, 2007, pp. 137 ss.; C. Piergallini, *La regola dell'"oltre ragionevole dubbio" al banco di prova di un ordinamento di* Civil Law, in M. Bargis, F. Caprioli (a cura di), *Impugnazioni e regole di giudizio nella legge di riforma del 2006: dai problemi di fondo ai primi responsi costituzionali*, Torino, 2007, pp. 361 ss.

[43] Per gli opportuni approfondimenti, cfr. A. Capone, *La motivazione della sentenza*, in L. Giuliani, R. Orlandi (a cura di), *Indagini preliminari e giudizio di primo grado. Commento alla legge 23 giugno 2017, n.* 103, pp. 297 ss.; G. Di Paolo, *L'art. 546, comma 1, lett. e): verso un nuovo modello normativo di motivazione "in fatto" della sentenza penale?*, in G.M. Baccari, C. Bonzano, K. La Regina, E.M. Mancuso (a cura di), *Le recenti riforme in materia penale. Dai decreti di depenalizzazione (d.lgs n. 7 e n. 8/2016 alla legge Orlando (l. n. 103/2017)*, Milano, 2017, pp. 241 ss.; V. Maffeo, *La motivazione della sentenza. Art. 1, co. 52, l. n. 103 del 2017*, in *Arch. pen. – Rivista web*, *Speciale* 2018, pp. 599 ss.

si pongano in controtendenza rispetto a quanto si registra nei settori contigui dell'ordinamento e, in particolare, nell'ambito del processo civile. In quel contesto, infatti, non si discute più tanto della "crisi della motivazione" – tema, a onore del vero, piuttosto risalente nel dibattito giuridico italiano – bensì del suo definitivo "tramonto", riferendosi agli interventi legislativi e giurisprudenziali che hanno progressivamente ridotto le opportunità di ottenere un controllo effettivo sulla completezza e la logicità della motivazione in fatto, incidendo sulla garanzia sancita dall'art. 111, co.6 Cost.[44] Nella medesima direzione, d'altronde, si pongono anche le riforme che hanno introdotto l'ordinanza post-istruttoria di cui all'art. 186-*quater* e la sentenza *ex* art. 281-*sexies* c.p.c., con una significativa contrazione degli oneri motivazionali in capo al giudice[45].

Il processo penale, dunque – almeno nella sua articolazione ordinaria – sembra rivendicare uno "statuto epistemologico" più rigido rispetto ai settori contigui dell'ordinamento, con una maggiore sensibilità per le esigenze di valutazione razionale della prova e il rispetto delle regole di decisione che governano la sentenza dibattimentale[46].

Ad ogni modo, gli sviluppi cui si è rapidamente accennato generano, ad avviso di chi scrive, una sorta di "paradosso" rispetto ai possibili impieghi dell'IA in funzione di supporto all'emissione delle decisioni giurisdizionali nel processo penale.

Per un verso, la fisionomia progressivamente assunta dalla sentenza emessa all'esito del giudizio dibattimentale sembra aver creato un terreno fertile per l'impiego di strumenti computazionali – idonei a conferire alla ricostruzione dei fatti maggiore attendibilità e precisione – in funzione di ausilio alla razionalità umana, i cui limiti nella gestione del

[44] Per una sintesi efficace al riguardo, v. M. Taruffo, *Brevi note sulla motivazione della sentenza* (2018), in Id., *Verso la decisione giusta*, Torino, 2020, pp. 409 ss. Sul punto, anche per ulteriori riferimenti bibliografici, cfr. L. Passanante, *Le sezioni unite riducono al "minimo costituzionale" il sindacato di legittimità sulla motivazione della sentenza civile*, in *Riv. trim. dir. e proc. civ.*, 2015, n. 1, pp. 179 ss., spec. pp. 187 ss. Per una ricognizione generale della materia, v. C. Rasia, *La crisi della motivazione nel processo civile*, Bologna, 2016, *passim*.

[45] Per gli opportuni approfondimenti, v. ancora C. Rasia, *op. cit*., pp. 104 ss.

[46] Sul punto, da ultimo, v. G. Canzio, *La motivazione della sentenza e la prova scientifica:* "reasoning by probabilities", in G. Canzio, L. Luparia Donati (a cura di), *Prova scientifica e processo penale*, Milano, 2022, pp. 3 ss., spec. pp. 7 ss.

ragionamento in condizioni di incertezza sono ormai ben noti, soprattutto grazie agli studi di psicologia cognitiva[47]. Per altro verso, tuttavia, le attività necessarie allo svolgimento di un giudizio così complesso ed eterogeneo – assistito, peraltro, da significativi oneri motivazionali – non sembra possano essere imitate o riprodotte dalle tecnologie di IA (almeno quelle attualmente disponibili)[48].

Difatti, al netto delle indubbie potenzialità computazionali, i *software* di IA difettano ancora della sensibilità "semantica" indispensabile per la redazione dei provvedimenti giurisdizionali[49]. Proprio per questo motivo, diversi autori sostengono che le applicazioni più promettenti dell'IA in funzione di ausilio o supporto all'emissione di decisioni giurisdizionali siano essenzialmente limitate ai provvedimenti connotati da un elevato

[47] Nota G. Canzio, *Intelligenza artificiale, algoritmi e giustizia penale*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, cit., p. 131, come «[sia] cresciuta nella società la legittima pretesa che il giudice, nell'esercizio dell'arte del giudicare e nella pratica giudiziaria, sia un buon ragionatore e un decisore di qualità. Sicché la professionalità, l'etica e l'implementazione del grado di *expertise* accumulata dal giudice nell'utilizzo delle tecniche inferenziali del ragionamento e nella verifica degli schemi statistico-probabilistici, acquisiti con l'ausilio della tecnologia digitale, di *software* informatici e algoritmi predittivi o con l'apporto della robotica e della logica dell'IA, potrebbero certamente contribuire a restituire al funzionamento della giustizia penale una più adeguata immagine di efficienza e qualità».

[48] Nel medesimo senso, in tempi ormai risalenti, M. Taruffo, *Judicial Decisions and Artificial Intelligence*, in *Artificial Intelligence and Law*, 1998, n. 2-4, p. 316: «If one considers the evident features of complexity, variability, flexibility and discretion that are typical of judicial decisions, any approach aimed at interpreting the judicial reasoning according to logical rules and models may appear as doomed to failure … The distrust in the possibility of logical fomalization of judicial reasoning may be even more intense when the problem is whether such a reasoning may be interpreted and formalized in terms of computerized logic or, more generally, in terms of AI models».

[49] «Tradizionalmente, i dati vengono elaborati sintatticamente, mentre le informazioni vengono elaborate semanticamente: gli agenti digitali superano gli agenti umani nell'analisi sintattica; gli esseri umani, invece, eccellono nella funzione semantica, estranea alle tecnologie digitali. E proprio in tale aspetto risiede il profilo più critico di ogni possibile tentativo di digitalizzazione del ragionamento giuridico: le variabili semantiche, che dominano questa area cognitiva umana, ne rendono particolarmente complessa la traduzione in un affidabile modello computazionale»: S. Quattrocolo, *Per un'intelligenza artificiale utile al diritto penale*, in *BioLaw Journal – Rivista di biodiritto*, 2021, n. 2, p. 393.

grado di standardizzazione[50]. Si pensi, per quanto concerne il processo penale, al decreto penale di condanna, alla sospensione del procedimento con messa alla prova, all'oblazione e all'applicazione della pena su richiesta delle parti[51].

Ciò, peraltro, appare consonante con quanto si è già osservato in precedenza circa le innovazioni che hanno interessato, in special modo, il giudizio cosiddetto "ordinario", costringendo il legislatore a valorizzare le ipotesi di *diversion* processuale in funzione deflativa del carico giudiziario[52].

5. Intelligenza artificiale e "contesti" processuali

Delineata la cornice normativa entro la quale si collocano le decisioni automatizzate, tenuto conto delle specificità tipiche della giustizia penale, è possibile ora proseguire nell'analisi per comprendere l'incidenza delle tecnologie di IA sulla dimensione propria del ragionamento probatorio.

A tal fine, è necessario svolgere una premessa di carattere metodologico, utile per orientare analiticamente l'indagine. Com'è noto, nel corso del procedimento penale si susseguono una pluralità di giudizi funzionali alla creazione delle condizioni giuridiche ed epistemiche necessarie per l'emissione del provvedimento giurisdizionale definitivo. Pertanto, an-

[50] In tal senso, v. già M. Taruffo, *Judicial Decisions and Artificial Intelligence*, cit., p. 319, il quale affermava: «the standardization of procedures in terms of software programs may be applied in the field of judicial practice. Roughly speaking, these are the areas in which the administratrion of justice is more similar to the bureaucratic administration with regard to the procedures employed and to the repetitiveness of concrete cases».

[51] Nello stesso senso, v. anche S. Quattrocolo, *Per un'intelligenza artificiale utile al diritto penale*, cit., pp. 396 ss., la quale nota un'interessante convergenza tra la struttura tipica del rito monitorio nel processo penale e un'ipotetica decisione sanzionatoria automatizzata, emessa *inaudita altera parte* e suscettibile di divenire irrevocabile, in assenza di opposizione da parte del soggetto destinatario del provvedimento (*ivi*, p. 397).

[52] Sul ruolo "promozionale" che i meccanismi di predizione decisoria basati sull'intelligenza artificiale potrebbero svolgere nell'ambito della giustizia penale deflativa, v. le considerazioni di R.E. Kostoris, *Predizione decisoria e diversion processuale*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, cit., pp. 103 ss.

che il ragionamento probatorio, che in ultima istanza costituisce indubbiamente appannaggio del giudice – cioè del soggetto istituzionalmente deputato alla verifica sulla fondatezza dell'ipotesi accusatoria – si nutre delle argomentazioni e delle prospettazioni fornite dalle parti nel corso del procedimento[53].

Per distinguere i momenti in cui si esplicano le attività cognitive funzionali alla ricostruzione dei fatti, la dottrina si riferisce tradizionalmente alla cosiddetta "teoria dei contesti", che gli studi giuridici hanno mutuato dalla filosofia della scienza.

L'attenzione si concentra, in particolar modo, sulla distinzione fra il *contesto di decisione*, generalmente identificato con la fase di deliberazione della sentenza, e il *contesto di giustificazione*; dedicato, invece, all'elaborazione della giustificazione posta a sostegno della decisione medesima[54].

Nel periodo anteriore all'emanazione del provvedimento finale si colloca, invece, il *contesto di ricerca*, che coincide con la fase dell'istruzione probatoria, in cui vengono acquisiti gli elementi utili per l'emissione della decisione giurisdizionale[55]. Infine, risalendo ancora all'indietro, si trova il *contesto della scoperta*, che coincide con la cosiddetta "istruzione primaria": quest'ultima si realizza normalmente nel corso delle indagini preliminari ed è finalizzata all'individuazione delle fonti e degli elementi di prova utili per le determinazioni concernenti l'esercizio dell'azione penale[56].

Le distinzioni sommariamente illustrate risultano congeniali allo sviluppo dell'indagine, visto che i *software* di IA saranno chiamati a svolgere compiti differenti nei diversi contesti interessati e, di conse-

[53] Ciò, naturalmente, è tanto più vero, quanto più forte sia la tutela del contraddittorio e del diritto alla prova nell'ambito della singola tipologia procedimentale.

[54] Sulla problematica trasposizione nella materia processuale della distinzione tra *context of discovery* e *context of justification*, cfr. le osservazioni di E. Amodio, *Motivazione della sentenza penale*, in *Enc. Dir.*, XXVII, Milano, 1977, pp. 216 ss.; T. Mazzarese, *Forme di razionalità delle decisioni giudiziali*, Torino, 1996, pp. 105 ss.; M. Taruffo, *La motivazione della sentenza civile*, cit., pp. 214 ss.; G. Ubertis, *Fatto e valore nel sistema probatorio penale*, cit., pp. 52 ss.

[55] Sulla distinzione in esame e per l'utilizzo della terminologia adoperata nel testo, v. G. Ubertis, *Profili di epistemologia giudiziaria*, Milano, 2021, pp. 28 ss.

[56] Sul punto, anche per gli opportuni riferimenti bibliografici, v. ancora G. Ubertis, *Profili di epistemologia giudiziaria*, cit., p. 30.

guenza, dovrebbero essere progettati e sviluppati in coerenza con gli obiettivi e la funzione tipica – volendo, con la "logica" – che governa ciascuna fase[57].

In particolare, nei contesti di scoperta e di ricerca le tecnologie di *artificial intelligence* dovrebbero svolgere una funzione euristica diretta, in primo luogo, all'individuazione delle fonti di prova e, successivamente, all'assunzione degli elementi rilevanti e pertinenti per la ricostruzione dei fatti oggetto della controversia. Invece, nei contesti di decisione e di giustificazione – i quali appaiono dialetticamente collegati, senza che fra di essi sia possibile operare una netta cesura – i *tool* di IA dovrebbero essere orientati alla valutazione degli elementi di prova legittimamente acquisiti, dapprima singolarmente e, successivamente, nel loro complesso.

5.1. Il contesto di scoperta e di formulazione dell'ipotesi

Procedendo con ordine, a partire dalle fasi iniziali del procedimento penale, si può osservare che diversi *software* di IA dedicati alle esigenze tipiche dell'istruzione primaria sono già operativi o in corso di sperimentazione. Essi, infatti, trovano il loro ambito di applicazione elettivo nella fase delle indagini preliminari, poiché sono in grado di svolgere simulazioni di eventi complessi (per esempio, simulazioni della scena del crimine tramite programmi di realtà aumentata; analisi cinematiche dei sinistri stradali, ecc.), indagini documentali oppure, ancora, elaborazioni di dati che possono aiutare le parti ad individuare o raccogliere elementi utili per suffragare le proprie affermazioni probatorie. Questi strumenti risultano particolarmente incisivi laddove sia necessario scandagliare una grossa mole di informazioni estratte dai dispositivi elettronici poiché, in tali evenienze, «è con l'ausilio della capacità computazionale de-

[57] Analogamente, secondo M. Gialuz, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, cit., p. 62, «l'impiego del dispositivo basato sull'intelligenza artificiale può servire sostanzialmente in due fasi della dinamica probatoria: da un lato può essere impiegato per la ricerca dell'elemento di prova e della fonte di prova …; dall'altro lato, può essere utilizzato nella fase della valutazione dell'elemento di prova». Analogamente, J. Nieva-Fenoll, *Intelligenza artificiale e processo*, Torino, 2019, pp. 14-15, distingue tra «programmi che aiutano a ricostruire i fatti sulla base degli indizi», da quelli che supportino i soggetti del processo nelle attività di «localizzazione delle prove, vale a dire nell'individuazione dei posti in cui è più probabile rinvenire delle tracce».

gli strumenti tecnologici che si contemperano, in concreto, le esigenze di completezza e di celerità delle indagini»[58].

Del resto, come è stato efficacemente osservato, «fino ad oggi l'individuazione degli indizi si è fondata essenzialmente sull'intuizione, sull'immaginazione e sull'esperienza della polizia investigativa»[59]. Sono, infatti, le abilità degli organi inquirenti che influenzano in modo decisivo il contesto della "scoperta" e indirizzano la formulazione delle ipotesi d'accusa. Non si vede, dunque, il motivo per cui si dovrebbe rinunciare agli apporti dell'IA, ove quest'ultima – senza vincolare rigidamente gli operatori – si limitasse a suggerire ipotesi ricostruttive sulla scorta delle esperienze maturate in precedenza ("tesaurizzate" nell'algoritmo) oppure delle elaborazioni dei dati che vengono in rilievo nel caso di specie.

Rispetto a questa modalità di utilizzo delle tecnologie di IA, vi sono essenzialmente due profili problematici che producono ricadute notevoli sulla dimensione del ragionamento probatorio[60]. Da un lato, si tratta di garantire trasparenza e affidabilità in merito all'origine dei dati mediante i quali viene addestrato l'algoritmo; dall'altro lato, occorre salvaguardare il principio di parità delle armi, che potrebbe essere posto a repentaglio nel caso in cui solamente una tra le parti processuali (verosimilmente la pubblica accusa) fosse posta nella condizione di utilizzare determinati *software* di analisi[61]. Nel prossimo futuro, invero, la disponibilità di alcune tecnologie di IA potrebbe rientrare anche fra le «condizioni necessarie per preparare la sua difesa», di cui l'imputato deve potersi giovare ai sensi dell'art. 111, co.3 Cost. e dell'art. 6, co.3 lett. b) Conv. eur. dir. uomo[62].

---

[58] In questi termini, M. Pisati, *op. cit*., p. 959. Per alcuni esempi pratici, v. anche E. Nissan, *Digital technologies and artificial intelligence's present and foreseeable impact on lawyering, judging, policing and law enforcement*, in *Artificial Intelligence & Society*, 2017, n. 3, pp. 441 ss., cui si deve un'interessante panoramica dei *software* di intelligenza artificiale suscettibili di impiego nel contesto processuale.

[59] J. Nieva-Fenoll, *op. cit.*, p. 15.

[60] Si prescinde, dunque, dalla questione circa l'inquadramento giuridico che deve essere assegnato alle attività investigative e probatorie compiute con l'ausilio delle tecnologie di intelligenza artificiale. Su questa tematica, si soffermano con cospicue notazioni sia M. Gialuz, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, cit., pp. 63 ss.; sia M. Pisati, *op. cit*., pp. 961 ss.

[61] Per gli opportuni riferimenti bibliografici, v. *supra*, § 2 nt. 20.

[62] Su questo profilo del diritto di difesa ha richiamato l'attenzione anche la giurisprudenza della Corte di Strasburgo. In alcune recenti pronunce, infatti, è stata evidenziata

In conclusione, nella fase delle indagini preliminari, l'impegno dell'IA può risultare utile: a) per incrementare l'efficienza nei processi di analisi della *digital evidence*, evidenziando rapidamente correlazioni e contenuti significativi rispetto alle ipotesi ricostruttive formulate dagli inquirenti; b) per assicurare uno *standard* investigativo omogeneo nei diversi contesti geografici, fornendo gli strumenti necessari per analizzare scenari complessi, effettuare simulazioni oppure, ancora, suggerendo una serie di ipotesi dotate di efficacia esplicativa rispetto alle circostanze del caso concreto. Naturalmente, tali funzionalità potrebbero rivelarsi utili anche per l'esercizio della funzione difensiva[63], anche se – nella maggior parte dei casi – la difesa potrebbe giovarsi dei dati necessari per l'applicazione dei *software* di *artificial intelligence* solo in seguito alla *discovery* degli atti d'indagine[64].

5.2. Il contesto di ricerca

Occorre, poi, soffermarsi sull'istruzione probatoria in senso stretto, vale a dire quella che si svolge, in linea di principio, di fronte al giudice competente a pronunciarsi sul merito dell'accusa.

In questa fase, sembra che l'IA possa svolgere compiti assai diversificati fra loro. In primo luogo, essa potrebbe fungere da strumento di supporto per una corretta ed esauriente esplicazione del contraddittorio nella formazione della prova. In particolare, la capacità di modellizzazione tipica della *artificial intelligence* potrebbe supportare le parti nello svolgimento della *cross examination* dei soggetti che rendono dichiarazioni nel processo; suggerendo temi di prova che sarebbero altrimenti trascu-

---

la necessità che, nelle ipotesi di *full collection of data* da parte della pubblica accusa, sia garantito al soggetto accusato la possibilità di usufruire dei tempi e delle facilitazioni necessarie al fine di preparare adeguatamente la propria difesa: C. eur. dir. uomo, sent. 25 luglio 2019, Rook c. Germania; C. eur. dir. uomo, sent. 4 giugno 2019, Einarsson e altri c. Islanda. Per ulteriori approfondimenti sul punto, v. M. Pisati, "Full collection of data" *e diritto di difesa*, in *Riv. it. dir. proc. pen.*, 2019, n. 4, pp. 2239 ss.

[63] V. *supra*, cap. II, spec. § 3 e 4.

[64] Sulla cosiddetta "*e-discovery*", che ha suscitato un vivace interesse nell'ambito del sistema giuridico statunitense, v., anche per alcuni riferimenti bibliografici, F. Santagada, *Intelligenza artificiale e processo civile*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, cit., pp. 827 ss.

rati (art. 506 c.p.p.) oppure segnalando tempestivamente la presenza di domande suggestive o nocive per la sincerità delle risposte (art. 499 co.2 e 3 c.p.p.)[65]. Questa modalità operativa, peraltro, potrebbe favorire indirettamente anche la stesura di una motivazione completa e persuasiva in ordine alla valutazione delle fonti di prova dichiarative, agevolando pure la funzione di controllo esercitata in sede d'impugnazione.

Nella medesima direzione si muovono anche alcune recenti proposte dottrinali che – sulla scorta delle prime esperienze applicative – suggeriscono l'adozione dei *tool* di IA per coadiuvare le parti e il giudice nell'attività di escussione e di valutazione della attendibilità dei testimoni oculari[66]. Questa tipologia di prova, infatti, può essere apprezzata sulla base di una serie di criteri "oggettivi" (come, ad esempio, le condizioni atmosferiche e di luminosità, la distanza dall'osservatore rispetto al luogo di svolgimento dei fatti narrati, le condizioni soggettive del dichiarante al momento dell'osservazione ecc.), che la rendono suscettibile di un'efficace modellizzazione[67]. D'altronde, un'evoluzione in questo senso favorirebbe anche una certa omogeneità nelle modalità di escussione e di valutazione della prova dichiarativa, instaurando *best practices* virtuose, a patto che la predisposizione di una griglia dei parametri di valutazione, cui il giudice dovrebbe in linea di principio attenersi, non si converta in un'operazione meramente burocratica.

È possibile, inoltre, immaginare applicazioni analoghe anche per quanto concerne la cosiddetta "prova scientifica", laddove i *tool* di *artificial intelligence* potrebbero rivelarsi utili sia per individuare i soggetti più idonei allo svolgimento delle operazioni peritali, sia per giungere proficuamente alla formulazione dei quesiti da sottoporre loro[68]. In particolare, per quanto riguarda la scelta dei soggetti cui conferire l'incari-

[65] Per un accenno in questa direzione, v. J. Nieva-Fenoll, *op. cit.*, p. 78.

[66] Per gli opportuni approfondimenti sul punto, cfr. J. Nieva-Fenoll, *op. cit.*, pp. 70 ss.; nonché, con osservazioni sostanzialmente sovrapponibili, E. Fabiani, *op. cit.*, pp. 67 ss.

[67] Cfr., sul punto, E. Nissan, *op. cit.,* p. 443, il quale riporta l'esempio del sistema esperto scozzese "*Advokate*". Si tratta di un *software* ideato per stabilire il grado di attendibilità dei testimoni oculari muovendo da una serie di criteri giurisprudenziali, estratti dalle sentenze che si sono occupate della materia. Il problema, come si può facilmente intuire, è quello di configurare tali criteri e di stabilire le modalità della loro interazione da un punto di vista computazionale.

[68] Cfr. J. Nieva-Fenoll, *op. cit.*, pp. 83 ss.; E. Fabiani, *op. cit.*, pp. 62 ss.

co, è agevole comprendere che un *software* potrebbe immagazzinare una grande quantità di informazioni, compresi i *curricula* e le pubblicazioni dei soggetti interessati, elaborando – ove richiesto – una serie di proposte in base agli ambiti di specializzazione di ciascun esperto[69].

D'altra parte, non si può escludere che siano gli stessi soggetti designati in qualità di periti o di consulenti tecnici a decidere di avvalersi di tecnologie fondate sull'IA per adempiere il loro mandato ed effettuare le relative valutazioni: si pensi, a titolo puramente esemplificativo, alle indagini foniche compiute con l'ausilio di sistemi automatizzati, funzionali all'identificazione del soggetto parlante[70].

Infine, l'impiego delle tecnologie di IA sarebbe auspicabile anche in relazione alla prova documentale, specialmente per quanto riguarda le verifiche tese ad accertare l'autenticità di un determinato documento oppure la sua provenienza (cfr. gli art. 239, 240 e 241 c.p.p.)[71]. Questo ambito di applicazione sembra particolarmente promettente, considerate

[69] Come è stato osservato in relazione al processo civile, ciò consentirebbe anche «di colmare, seppur in via di fatto, la lacunosità da cui è affetta, nel nostro ordinamento, la disciplina della consulenza tecnica sotto il profilo della scelta del consulente»: E. Fabiani, *op. cit.*, p. 66. Scettico al riguardo, J. Nieva-Fenoll, *op. cit.*, p. 85, il quale ritiene, invece, che «l'intelligenza artificiale potrebbe aiutare in futuro a scoprire meriti apparenti, piuttosto che esserne vittima», traendo ispirazione dai programmi antiplagio utilizzati da molte istituzioni accademiche.

[70] Sul punto, sottolineando la necessità di un controllo giurisdizionale approfondito in ordine all'affidabilità dello strumento impiegato per l'identificazione vocale e delle fonti di addestramento del relativo algoritmo, v. M. Biral, *L'identificazione della voce nel processo penale: modelli, forme di accertamento, tutela dei diritti individuali*, in *Riv. it. dir. proc. pen.*, 2015, n. 4, pp. 1863 ss.

[71] In termini generali, v. ancora J. Nieva-Fenoll, *op. cit.*, pp. 80 ss.; E. Fabiani, *op. cit.*, pp. 74 ss. Per un'applicazione specifica, v. anche M. Caianiello, *Dangerous Liaisons. Potentialities and Risks Deriving from the Interaction between Artificial Intelligence and Preventive Justice*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2021, n. 1, p. 6, il quale ritiene che il settore della criminalità economica e finanziaria possa costituire un terreno privilegiato per verificare l'impatto della rivoluzione digitale nella materia probatoria, proprio perché «this kind of crimes – that also includes fraud against the EU budget – has been usually committed by faksifying documents, or manipulating other real evidence, with the aim to hide unlawful purposes pursued by the perpetrators to the competent authorities … It is not wrong to affirm that, by tradition, fact-finding in trials concerning crimes against the EU interests is prevailingly based on documents: in other words, on written evidence».

le potenzialità dei *software* informatici nelle attività di analisi del linguaggio e nel raffronto tra molteplici documenti per stabilire eventuali similitudini o divergenze.

5.3. Intelligenza artificiale e valutazione della prova

Se queste sono le prospettive più interessanti per quanto concerne l'utilizzo di strumenti di IA in funzione euristica, occorre adesso chiedersi quale ruolo potrebbero rivestire le tecnologie in esame ai fini della valutazione della prova. Si tratta del momento conclusivo del procedimento probatorio, che assume rilievo sia nel contesto di decisione – salvo ritenere che sia possibile pervenire a quest'ultima tramite un processo del tutto irrazionale – sia per la giustificazione del relativo provvedimento.

Occorre, naturalmente, distinguere la valutazione del singolo elemento di prova da quella che viene effettuata sull'intero compendio probatorio e dalla quale deriva il giudizio di fatto nel suo complesso[72].

Dal primo punto di vista – tralasciando le ipotesi, cui si è già accennato nel paragrafo precedente, in cui l'IA funge direttamente da strumento di ausilio per l'assunzione e la valutazione probatoria – si tratta di comprendere come dovrebbe essere apprezzato il singolo elemento di prova, generato o raccolto mediante le tecnologie in esame.

Per rispondere a questo quesito, occorre muovere dal condivisibile orientamento dottrinale, secondo cui la prova fondata sulla *artificial intelligence* appartiene al *genus* della prova scientifica e, in particolare, alla categoria della "prova digitale", altrimenti detta "*electronic evidence*"[73]. Per la sua corretta valutazione, dunque, assume un ruolo

---

[72] Cfr., sul punto, G. Ubertis, *Profili di epistemologia giudiziaria*, cit., pp. 111 ss., il quale distingue il «giudizio assertorio di concludenza probatoria», concernente il singolo mezzo di prova, dalla «valutazione probatoria complessiva», connotata «dall'utilizzo combinato dell'intero patrimonio conoscitivo giudiziario ai fini dell'emissione della pronuncia» (*ivi*, p 117). La distinzione è accolta anche da O. Mazza, *op. cit.*, pp. 363 ss. e viene implicitamente utilizzata anche nel contributo di E. Fabiani, *op. cit*., spec. pp. 49 e 60.

[73] In questo senso, v. M. Gialuz, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, cit., pp. 61-62, il quale sostiene che la riconducibilità della prova fondata sull'IA al *genus* della prova scientifica riproponga le problematiche tipiche di quest'ultima categoria probatoria (in particolare: necessità di ragionare in termini di probabilità e guardarsi dall'illusione di giungere a una conoscenza oggettiva; esigenza di ricostruire

decisivo il cosiddetto "strumento di prova"[74], vale a dire l'apparato conoscitivo, fondato su leggi scientifiche o tecniche, che consente l'elaborazione di un determinato elemento di prova[75].

Da questa constatazione, emergono anche le informazioni che assumono rilievo per la valutazione degli elementi probatori generati o raccolti tramite gli strumenti fondati sull'IA. È necessario, infatti, che le parti e il giudice siano posti nella condizione di conoscere, apprezzare e dibattere circa: a) la base di dati utilizzata dallo strumento probatorio; b) il *set* di istruzioni che costituiscono la funzione dell'algoritmo; c) il tasso di errore insito nello strumento (che potrebbe rivelarsi più alto di quello che ci si attende, sollevando legittime perplessità in ordine alla attendibilità e alla rilevanza del singolo elemento di prova così ottenuto); d) la catena di custodia dell'elemento raccolto[76].

---

con precisione la catena di custodia per garantire la genuinità dell'elemento di prova); affermando, comunque, che la prova algoritmica presenta alcune peculiarità che denotano altrettanti profili problematici (in particolare: l'origine e la scelta dei dati su cui l'algoritmo viene addestrato; nonché la trasparenza e la conoscibilità delle istruzioni di cui consiste l'algoritmo medesimo).

[74] Per la definizione e l'individuazione del concetto in esame, v. O. Dominioni, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Milano, 2005, pp. 25 ss.

[75] Si pensi, per fare un esempio banale, all'etilometro, cioè lo strumento di misurazione normalmente utilizzato nell'esame spirometrico per determinare il valore di etanolo presente nel sangue di un determinato soggetto.

[76] Al riguardo, cfr. anche il decalogo elaborato da G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, cit., p. 23, il quale – in modo ancor più analitico – sostiene che l'impiego di tecnologie di IA nel contesto propriamente processuale («l'impiego della macchina in sede giurisdizionale») dovrebbe essere subordinato alle seguenti condizioni: a) controllo pubblico sul funzionamento dell'algoritmo, tramite meccanismi di *peer review*; b) precisazione del tasso di errore; c) spiegazione delle formule tecniche costitutive dell'algoritmo, comprensiva del collegamento con le regole giuridiche ad esso sottese; d) contraddittorio tra le parti sulla scelta dei dati archiviati, sui loro raggruppamenti e sulle loro correlazioni, elaborate dal *tool* di intelligenza artificiale, in particolare in relazione all'oggetto della controversia; e) valutazione dell'elemento di prova generato o raccolto tramite strumenti di intelligenza artificiale secondo il canone del libero convincimento del giudice». Secondo l'a., in assenza di queste condizioni, la prova algoritmica non sarebbe sottoposta a un «controllo umano significativo» e, di conseguenza, dovrebbe essere considerata radicalmente inutilizzabile nel giudizio, potendo – al massimo – essere impiegata per finalità strettamente investigative (*ibidem*). Per S. Quattrocolo, *Quesiti nuovi a soluzioni antiche? Consolidati paradigmi normativi vs ri-*

In caso contrario, «la struttura sillogistica che tradizionalmente orienta il ragionare giudiziale, anche nella fase istruttoria, verrebbe arricchita, ricalibrata e progressivamente sostituita – assecondando inevitabili tappe obbligate – alla luce dei parametri e dei criteri-guida elaborati nell'attività di auto-apprendimento e successiva selezione posta in essere dalla macchina»[77]. Ciò renderebbe di fatto impossibile l'esplicazione di un confronto dialettico e, in ultima istanza, la redazione di una vera e propria motivazione da parte del giudice in merito all'attendibilità e alla persuasività della prova algoritmica: un esito, evidentemente, inaccettabile alla luce dei parametri normativi attualmente vigenti in materia (art. 111, co.6 Cost., art. 192 c.p.p.).

Ferma restando, dunque, la necessità di tenere in considerazione tali circostanze, come dovrebbero essere valutati gli elementi di prova ottenuti mediante strumenti di IA? Non è, ovviamente, possibile delineare regole universalmente valide, poiché la valutazione probatoria deve essere sempre effettuata in relazione al singolo elemento considerato, alla luce delle circostanze del caso concreto. In dottrina, come anticipato in precedenza[78], si è proposto di sussumere le prove algoritmiche entro la categoria degli indizi – sottoponendole, pertanto, alla regola di valutazione sancita dall'art. 192, co.2 c.p.p. – muovendo dalle disposizioni che, a livello europeo e nazionale, garantiscono il diritto a non essere sottoposti a decisioni fondate esclusivamente su trattamenti automatizzati.

Anche se la proposta sconta un certo tasso di rigidità – comune, peraltro, a tutte le regole di valutazione della prova – bisogna riconoscere che

---

schi e paure della giustizia digitale "predittiva", in *Cass. pen*., 2019, n. 4, pp. 1756 ss., le parti processuali debbono poter efficacemente interloquire in ordine alla validità della teoria scientifica posta alla base dell'algoritmo, alla sua traduzione nel linguaggio digitale e alla sua applicabilità ai fatti oggetti di prova: in caso contrario, infatti, sarebbe difficile, se non impossibile, «criticare l'attendibilità della prova generata automaticamente» (*ivi*, p. 1758), con una inevitabile violazione della parità delle armi. Nella medesima direzione si pone, da ultima, anche D. Perrone, *La prognosi postuma tra distorsioni cognitive e* software *predittivi*. *Limiti e possibilità del ricorso alla "giustizia digitale integrata" in sede di accertamento della colpa*, Torino, 2021, pp. 105 ss.

[77] In questi termini, A. Merone, *Le prove digitali e l'uso dell'intelligenza artificiale per finalità istruttorie*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, cit., p. 918.

[78] V. *supra*, § 3 nota 35.

la sussunzione entro la categoria della prova indiziaria riflette due caratteristiche piuttosto comuni tra gli elementi generati o raccolti mediante dispositivi di IA e, pertanto, non si pone in contrasto con un elementare criterio di ragionevolezza ermeneutica. Invero, nella maggior parte dei casi, tali elementi di prova forniscono alternativamente:

a) informazioni di carattere generale, utili soprattutto per descrivere il contesto in cui si ipotizza si siano svolti i fatti controversi, ma prive di un'autonoma capacità dimostrativa in ordine a condotte specifiche, oggetto dell'imputazione[79];

b) informazioni assai specifiche che, analogamente alla prova genetica, sono assistite – ove non siano inficiate da significativi tassi di errore – da un elevato grado di precisione ma colgono tendenzialmente "porzioni di realtà" piuttosto ridotte.

In entrambi i casi, dunque, sembra plausibile affermare che tali informazioni sarebbero idonee a dimostrare la sussistenza di determinati fatti soltanto con il concorso di ulteriori elementi di prova, in grado di bilanciarne – rispettivamente – l'eccessiva genericità o specificità.

Vale, in ogni caso, il limite generale stabilito dal nostro codice di rito (cfr. gli art. 64, co. 2 e 188 c.p.p.), che vieta l'utilizzo di metodi o tecniche – comprese, ovviamente, quelle di IA – idonee a limitare la libertà di autodeterminazione delle persone oppure ad alterare la capacità di ricordare o valutare i fatti[80]. Per esemplificare, sotto la scure di questo divieto

[79] Si pensi, ad esempio, alle operazioni di profilazione funzionali a creare informazioni sulle abitudini di consumo dell'imputato o sulle sue condizioni patrimoniali in un determinato momento storico: anche nel caso in cui questi dati fossero considerati pertinenti e rilevanti nell'ambito di un procedimento per reati fallimentari o contro il patrimonio, sarebbero comunque privi di autonoma concludenza probatoria rispetto alle condotte contestate. Un ragionamento analogo può essere effettuato in merito alle analisi dirette a individuare il *modus operandi* di un certo sodalizio criminale: una correlazione tra le diverse condotte illecite potrebbe assurgere ad elemento di natura indiziaria nei confronti dei soggetti coinvolti (dovendosi, eventualmente, discutere della gravità e della precisione di tale elemento), ma ovviamente non sarebbe sufficiente a sorreggere autonomamente l'ipotesi d'accusa.

[80] «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.»: M. Gialuz, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, cit., p. 64.

ricadono tutti quegli strumenti che promettono, attraverso misurazioni in tempo reale dei parametri corporei o dei tempi di reazione di un soggetto, di misurare la credibilità soggettiva di un testimone o, addirittura, di individuarne con esattezza il mendacio.

Una sfida ancor più impegnativa è quella legata all'utilizzo dei *tools* di IA a supporto del giudice per la valutazione complessiva del patrimonio gnoseologico disponibile all'esito dell'attività istruttoria. In questa prospettiva, l'IA potrebbe supportare il giudice nel porre in relazione diversi elementi di prova, evidenziando i nessi logici e le catene inferenziali necessarie per la composizione del giudizio di fatto, suggerendo eventualmente se sia stato oltrepassato lo *standard* probatorio richiesto ai fini della condanna.

È difficile negare che gli strumenti in questione potrebbero contribuire ad arginare alcuni errori cognitivi tipici dei decisori umani. Questi ultimi, una volta considerato attendibile (o inattendibile) un determinato elemento, tendono ad eliminare mentalmente il grado di conferma che inizialmente gli avevano attribuito. In tal modo, la valutazione giudiziale procede secondo uno schema binario, con il rischio di "occultare" le sorgenti di incertezza insite nei singoli elementi di prova e nelle relative inferenze, sopravvalutando (o sottovalutando) il peso probatorio di determinati elementi[81]. Del resto, quando nella medesima vicenda processuale si riscontra la presenza sia di prove scientifiche che di prove tradizionali, la valutazione probatoria complessiva risulta pericolosamente esposta all'intimo convincimento del giudice, in virtù della fisiologica difficoltà

[81] Sul punto, v. O. Mazza, *op. cit*., p. 364, il quale sostiene che «il giudice, nella valutazione della singola prova, non sia tenuto a raggiungere una conclusione vincolata in termini di concludenza probatoria, ossia di affermazione o negazione della proposizione fattuale che costituisce il singolo tema di prova. Egli può anche ritenere relativamente persuasivo l'esperimento probatorio, quindi giungere a un grado di conferma dell'ipotesi fattuale non del tutto soddisfacente, senza perciò escludere il conseguimento di un risultato di prova, sia pure incerto». Sulla scorta di queste premesse, l'a. conclude nel senso che «il singolo risultato di prova, ancorché, in ipotesi, connotato da ampi margini di incertezza, entrerà comunque nella valutazione complessiva di tutte le evidenze disponibili nel momento decisorio, potendo in questa seconda fase essere oggetto di una nuova valutazione alla luce di tutti gli altri elementi nel frattempo raccolti, che magari possono innalzare o abbassare il livello di persuasività del risultato di prova originario» (*ivi*, p. 365).

di configurare i nessi logici tra le diverse informazioni disponibili[82]. Di conseguenza, una delle applicazioni più interessanti dei sistemi di IA potrebbe essere proprio quella di coadiuvare gli organi giurisdizionali nella corretta impostazione dei ragionamenti probabilistici, al fine di governare le sorgenti di incertezza che si annidano nelle pieghe del ragionamento probatorio. In particolare, l'utilizzo dei *software* di *artificial intelligence* sarebbe auspicabile soprattutto nei cosiddetti *hard cases*, vale a dire nei processi indiziari caratterizzati da un compendio probatorio complesso, per arginare l'arbitrio soggettivo del giudice, garantire sin dove è possibile la parità di trattamento tra gli imputati e, soprattutto, prevenire gli errori giudiziari.

Vi sono, però, diversi ostacoli che si frappongono alla proposta di utilizzare le tecnologie in esame nel contesto della valutazione probatoria complessiva.

Il primo consiste nella forte resistenza culturale che, fino ad oggi, ha inibito la penetrazione degli strumenti tipici del calcolo delle probabilità nel dominio delle decisioni giurisdizionali e, in particolare, per quanto attiene alla ricostruzione dei fatti[83]. Non si tratta solamente di una disputa teorica, bensì di una vera e propria avversione nei confronti dei metodi quantitativi, dovuta probabilmente anche alla formazione tradizionale dei giuristi e alle reminiscenze storiche dei sistemi di prova legale. Del resto, bisogna ammettere che non sussiste uniformità di vedute in dottrina circa i risultati che potrebbero essere conseguiti sul piano della valutazione delle prove ricorrendo al teorema di *Bayes* che, tra i vari strumenti teoretici disponibili, è indubbiamente quello che

[82] Sul punto, cfr. F. Taroni, S. Bozzi, *Il significato delle evidenze: l'importanza dello scienziato forense nella prevenzione dell'errore*, in L. Luparia Donati (a cura di), *L'errore giudiziario*, Milano, 2021, pp. 696 ss.

[83] Sulle ragioni di questo "ritardo culturale" e per un'accorata esortazione a non abbandonare questo campo di studi, v. L. Luparia, Trial by probabilities. *Qualche annotazione eretica*, in *La Corte d'assise – Rivista quadrimestrale di scienze criminalistiche integrate*, 2012, n. 1-2 pp. 155 ss., il quale conclude affermando: «non possiamo accettare che nel giudizio si possa fare a meno di un bagaglio conoscitivo che è patrimonio sedimentato di altri importanti domini e che, peraltro, non priva il magistrato della sua individualità di apprezzamento, ma semplicemente ne agevola un uso, e un successivo controllo, in linea con la garanzia di logicità delle decisioni» (*ivi*, p. 164)

«sembrerebbe prestarsi maggiormente ad una possibile automazione del giudizio di fatto»[84].

Il secondo ostacolo deriva, invece, dal fatto che la costruzione di un modello di inferenze, comprensivo di una molteplicità di prove, costituisce inevitabilmente «un atto creativo»[85], a prescindere dallo schema logico cui tale modello si ispira: di conseguenza, lo schema computazionale non potrebbe essere esteso oltre il caso concreto in relazione al quale è stato concepito e realizzato. In tal caso, dunque, viene meno una delle principali ragioni a sostegno dell'impiego delle tecnologie di IA nel contesto processuale, cioè quella di consentire una trattazione più rapida delle singole vicende giudiziarie, incrementando l'efficienza dei sistemi di giustizia. Si potrebbe, comunque, sostenere che l'impiego dei *tool* di *artificial intelligence* sia giustificato dalla possibilità di addivenire a una ricostruzione dei fatti maggiormente accurata, ma non è difficile prevedere che ciò sarebbe vissuto dagli operatori come un ulteriore aggravio delle attività di competenza degli organi giurisdizionali. Peraltro, non si può fare a meno di notare che l'impiego dell'IA per l'elaborazione di schemi logici di inferenze probatorie avrebbe conseguenze rilevanti pure sul piano dell'organizzazione giudiziaria, le cui strutture dovrebbero essere modificate per accogliere personale dotato di competenze informatiche e attuariali.

In conclusione, nel prossimo futuro sembra più realistico attendersi che, nei diversi contesti epistemologici in cui si articola il procedimento penale, si verifichi l'affidamento progressivo ai *software* di IA di alcuni compiti specifici, suscettibili di ripetizione in una serie indefinita di casi, secondo un approccio tipico della *narrow artificial intelligence*.

---

[84] L'osservazione è di E. Fabiani, *op. cit.*, p. 56. Per una recente riproposizione della vivace *querelle* fra i sostenitori della probabilità logica (o baconiana) e quelli della probabilità quantitativa (o pascaliana), cfr. P. Garbolino, *A cosa serve il teorema di Bayes? Replica a Michele Taruffo*, in *Riv. dir. process.*, 2016, n. 4-5, pp. 1127 ss.; M. Taruffo, *Note sparse su probabilità e logica della prova*, in *Riv. trim. dir. e proc. civ.*, 2014, n. 4, pp. 1507 ss. Sul punto, da ultimi, F. Taroni, S. Bozza, J. Vuille, *La probabilità come strumento per una coerente valutazione della prova scientifica*, in G. Canzio, L. Luparia Donati (a cura di), *Prova scientifica e processo penale*, Milano, 2022, pp. 21 ss.

[85] Lo riconosce espressamente P. Garbolino, *Probabilità e logica della prova*, Milano, 2014, p. 310.

6. La collaborazione tra uomo e macchina nelle decisioni giurisdizionali: quale modello per il giudizio di fatto?

L'analisi condotta fino a questo momento ha consentito di esaminare il rapporto fra IA e ragionamento probatorio nel contesto del processo penale. Fra le molteplici applicazioni possibili, si è cercato di individuare un percorso virtuoso, funzionale ad esaltare il confronto dialettico tra le parti, nella prospettiva di un incremento nella qualità delle decisioni giurisdizionali. Per concludere, bisogna provare a delineare le tendenze evolutive del ragionamento probatorio, alla luce dei cambiamenti indotti dalla tumultuosa evoluzione tecnologica in atto.

Secondo l'opinione di chi scrive, due sono gli scenari principali da tenere in considerazione.

Il primo scenario deriva dalla «creazione di strumenti di catalogazione e di valutazione della prova penale»[86]. L'utilità di questi strumenti appare evidente, se l'obiettivo che si persegue è orientato ad ottenere una semplificazione del compito del giudice nella ricostruzione dei fatti. Si intravedono, però, anche gravi rischi. In particolare, l'esigenza di tradurre nel linguaggio informatico le informazioni acquisite in sede giurisdizionale, per sfruttare al meglio la capacità computazionale tipiche dell'IA, potrebbe innescare un processo di irrigidimento delle categorie probatorie, delle loro interazioni e dei corrispondenti nessi inferenziali[87]. Come si è osservato correttamente in dottrina, con precipuo riferimento alla *digital evidence*, «di qui alla restaurazione di un sistema di prove legali riveduto e corretto il passo non sarebbe, alla fin fine, molto lungo»[88]. In altri termini: se è vero che un sistema orientato alle prove legali

[86] In questi termini, v. C. Parodi, V. Sellaroli, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco, in Diritto penale contemporaneo*, 2019, n. 6, p. 48.

[87] Cfr. A. Carcaterra, *Machinae autonome e decisione robotica*, in A. Carleo (a cura di), *Decisione robotica*, cit., p. 39: «Per poter essere trattabile attraverso metodi algoritmici, cioè attraverso una sequenza non ambigua di operazioni finite, l'informazione relativa ai dati deve necessariamente essere impoverita … L'unica possibilità per noi di incamerare l'informazione del mondo analogico è il taglio di questa informazione che avviene attraverso la digitalizzazione dell'informazione stessa, ossia attraverso la sua riduzione a un elenco finito di informazioni numeriche».

[88] G. Paolozzi, *Relazione introduttiva*, in L. Luparia, L. Marafioti, G. Paolozzi (a cura di), *Dimensione tecnologica e prova penale*, cit., p. 11.

sarebbe piuttosto congeniale alla realizzazione delle modalità operative tipiche dell'IA[89]; ciò, tuttavia, non significa che il percorso non possa realizzarsi in senso inverso. Non è detto, cioè, che la disponibilità e l'impiego delle tecnologie in esame non possa contribuire a ridimensionare, in modo più o meno surrettizio e consapevole, lo spazio riservato al libero convincimento del giudice.

Si tratta di una mutazione che appare non solo poco auspicabile, ma anche essenzialmente in contrasto con le "ideologie" del processo penale contemporaneo[90]. Quest'ultimo, almeno nel nostro Paese, sembra complessivamente orientato a privilegiare le istanze di concretezza e di razionalità dell'accertamento fattuale, rifiutando l'instaurazione di presunzioni assolute e di rigide gerarchie tra le fonti probatorie a disposizione del giudice[91].

Dove si colloca, dunque, il limite invalicabile, che non potrebbe esse-

[89] Sul punto, v. anche E. Fabiani, *op. cit.*, p. 55, il quale osserva che «un sistema imperniato sul libero convincimento del giudice si presta molto di meno del sistema di prova legale (contraddistinto dall'essere imperniato su criteri rigidi ed oggettivi e dalla totale assenza di discrezionalità del giudice in sede di valutazione della prova) ad essere automatizzato attraverso il ricorso ad algoritmi». Nella medesima direzione, J. Nieva-Fenoll, *op. cit*., p. 96, afferma icasticamente che «il sistema [di prova legale] era così semplice e così assurdo che avrebbe fatto la felicità dell'intelligenza artificiale».

[90] Si utilizza il termine "ideologie", nel significato attribuito ad esso da M. Cappelletti, *Le grandi tendenze evolutive del processo civile nel diritto comparato*, in *Processo e ideologie*, Bologna, 1964, p. IX, il quale interpretava le ideologie del processo come l'insieme delle «ragioni e [dei] condizionamenti sociali e culturali che in un determinato contesto storico stanno e operano nella norma e nell'istituto, nella legge e nell'ordinamento, come pure nell'interpretazione e in genere nell'attività dei giudici e dei giuristi».

[91] Sul punto, cfr. le cospicue notazioni di G. Carlizzi, *Libero convincimento e ragionevole dubbio nel processo penale. Storia prassi teoria*, San Lazzero di Savena, 2018, pp. 35 ss., il quale propugna la tesi secondo cui il principio del libero convincimento del giudice sarebbe dotato di fondamento costituzionale. In particolare, l'autore ricava dall'art. 3, co.2 Cost. il principio di ragionevolezza della legge, «il quale impone al legislatore di garantire la costante aderenza delle sue regole alle peculiarità delle situazioni che ne formano oggetto» (*ivi*, p. 43) e dall'art. 111, co.6 Cost., il principio di razionalità della giurisdizione, «il quale esige che [essa] si esprima sempre, non solo sul versante interpretativo, ma anche su quello probatorio, secondo canoni intersoggettivamente collaudati» (*ivi*, p. 44). In precedenza, v. anche M. Daniele, *Regole di esclusione e regole di valutazione della prova*, *op. cit*., pp. 113 ss., con riferimento alle ragioni che depongono in favore della progressiva scomparsa delle regole positive di valutazione della prova nei sistemi di giustizia penale contemporanei.

re oltrepassato senza alterare il volto del sistema processuale? Secondo l'opinione di chi scrive, sarebbe legittimo ricorrere a strumenti artificiali di raccolta, catalogazione e valutazione della prova, nella misura in cui il giudice rimanesse, comunque, libero di determinarsi in ordine:

a) alla sussunzione di un determinato elemento probatorio entro la fattispecie processuale che egli reputa corretta (ad esempio: prova indiziaria, dichiarazione di persona imputata in un procedimento connesso o collegato, dichiarazioni della persona offesa, elemento di riscontro, ecc.);

b) all'individuazione dei criteri (leggi scientifiche, leggi logiche, massime di esperienza) da impiegare per la valutazione di ogni singolo elemento, i quali debbono essere esposti nella motivazione del provvedimento sulla *quaestio facti*[92].

Il secondo scenario, invece, trae origine dalla necessità – unanimemente riconosciuta – di mantenere sempre un «controllo umano significativo»[93] sugli strumenti di IA impiegati nella sede processuale. Ciò che preme sottolineare, tuttavia, è che – al di là di questa fondamentale enunciazione di principio – ciascuno ha il suo modo di concepire i termini della collaborazione tra uomo e macchina, da cui dovrebbe sorgere una nuova forma di "intelligenza aumentata", idonea ad incrementare l'efficienza e la qualità delle decisioni giurisdizionali.

Per comprendere al meglio la questione, giova richiamare alcune tra le riflessioni più significative emerse sinora in dottrina, tenendo presente che su questo terreno si combatte la battaglia per la conservazione dell'autonomia e del controllo umano effettivo sulle decisioni giurisdizionali.

In una prima direzione, si è proposto di coniare regole probatorie ido-

[92] Nel medesimo senso, v. anche G. Padua, *op. cit*., p. 1507: «gli algoritmi [possono] fare il loro ingresso nel processo solo come *strumenti* dell'inferenza probatoria, ovvero in qualità di applicativi che si inseriscono – in campo investigativo – come mezzo di raccolta di dati conoscitivi e – in ambito istruttorio – come elemento cognitivo oggetto del confronto dialettico tra le parti e della valutazione del giudice. Il riferimento è, dunque, a quel gruppo di applicazioni (quali, ad esempio, i programmi di riconoscimento facciale) che si atteggiano a fonti di prova algoritmiche. Viceversa, l'intelligenza artificiale non potrebbe mai diventare una *regola* di inferenza probatoria, tale da sostituire quell'approccio individualizzato e soggettivo tipico del ragionamento umano».

[93] Per l'impiego di questa efficace locuzione, v. G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, cit., p. 23.

nee a limitare il potere del giudice di condannare in assenza di una *scientific corroboration of evidence*, nei casi in cui il provvedimento si fonda in modo esclusivo o determinante su alcuni mezzi di prova tradizionali, la cui attendibilità è stata posta ripetutamente in discussione (ad esempio, testimonianza della persona offesa, ricognizione o individuazione di persone, ecc.). Si tratterebbe, in altre parole, di introdurre delle «*corroboration rules* in virtù delle quali – in relazione a un certo catalogo di prove – il convincimento del giudice non potrebbe essere, di per sé, sufficiente a condannare, in assenza di una serie di elementi di conferma provenienti dalla intelligenza artificiale»[94].

Una seconda proposta nasce, invece, dall'idea secondo cui, «con un impiego massivo di tecniche probatorie di cui sia noto il tasso di errore, potremmo avere un incentivo a usare *standard* di prova qualificati»[95]. In astratto, è possibile concordare con questa affermazione, a patto di distinguere il grado di conferma della singola valutazione probatoria dalle regole di decisione che disciplinano la persuasione del giudice in ordine alla ricostruzione fattuale complessiva[96]. Infatti, mentre nel primo caso sarebbe possibile stabilire soglie numeriche idonee ad esprimere in termini quantitativi il grado di conferma che può essere attribuito al singolo risultato di prova, con riferimento alla valutazione probatoria complessiva si potrebbe solamente «immaginare che in tale contesto vengano forniti algoritmi in grado di computare i valori rilevanti e offrirli al giudice a fini decisori»[97]. Ciò, poiché «spetta sempre al giudice definire in ultima istanza il valore persuasivo del patrimonio gnoseologico acquisito al processo e decidere, quindi, se sia stato rag-

[94] Così, L. Luparia Donati, *Notazioni controintuitive su intelligenza artificiale e libero convincimento*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, cit., pp. 120-121. Analogamente, secondo V. Manes, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, p. 565, «si potrebbe prevedere un percorso dove l'algoritmo possa essere impiegato come strumento di verifica della scelta operata dal giudice, e di confronto con l'esito offerto da una valutazione informatizzata e verificata attraverso i dati». L'a. giunge a ipotizzare anche un obbligo di motivazione rafforzata, che incomberebbe sul giudice, nel caso in cui egli intenda confermare la sua decisione a dispetto del "parere contrario" espresso dall'algoritmo (*ibidem*).

[95] G. Tuzet, *op. cit*., p. 52.

[96] V. *supra*, § 5.3.

[97] In questi termini, v. ancora G. Tuzet, *op. cit*., p. 53.

giunto il 'traguardo probatorio' normativamente disposto»[98]. Tuttavia, non si può ignorare il rischio di un "effetto ancoraggio", che potrebbe indurre il giudice a non discostarsi dal risultato fornito dalla macchina. Per questa ragione, ad avviso di chi scrive, la prima proposta – orientata all'introduzione di regole di prova legale negativa – risulta preferibile rispetto a quella illustrata per ultima.

Infine, muovendo dal presupposto secondo cui contestare nel merito le valutazioni offerte da un sistema di IA costituisce impresa particolarmente ardua, si propugna l'introduzione nel processo penale di un diritto a far riesaminare le valutazioni in questione da un diverso sistema automatizzato[99]. Questo approccio si fonda sul cosiddetto "principio di ridondanza", il quale richiede che «le stesse informazioni [siano] elaborate simultaneamente da un certo numero di sistemi diversi ma con le medesime funzioni»[100], al fine di aumentare l'affidabilità dei singoli sistemi e ridurre al minimo il rischio di errori. In effetti, l'adozione di tecnologie ridondanti nel settore probatorio sembra meritevole di particolare attenzione, soprattutto perché – allo stato attuale ma, con ogni probabilità, anche in futuro – non vi è uniformità di vedute sui modelli logici che dovrebbero governare il giudizio di fatto nel contesto processuale. Vi sarebbe, dunque, lo spazio per l'adozione di approcci alternativi nello sviluppo degli algoritmi da parte di diversi *team* di programmatori, i quali dovrebbero auspicabilmente coinvolgere cultori delle differenti discipline interessate.

---

[98] G. Ubertis, *Profili di epistemologia giudiziaria*, cit., p. 180.

[99] In questa direzione si muovono 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, n. 4, pp. 631 ss. Per gli opportuni approfondimenti sul punto, v. anche *supra*, cap. II, § 2 e ss.

[100] G. Contissa, G. Lasagni, G. Sartor, *op. cit*., p. 634. Gli autori riconoscono che «l'applicazione del *redundancy approach* alle decisioni automatizzate nel processo penale richiederebbe di rendere disponibili, presso ogni distretto giudiziario, una gamma di sistemi A/IA certificati e validati (ad esempio, tramite la creazione di un apposito albo). Questo ventaglio di opzioni dovrebbe essere sufficientemente ampio da consentire ai giudici di appello di scegliere, per la falsificazione della valutazione prodotta in primo grado (o durante le indagini preliminari) un sistema diverso da quello già applicato».

7. Segue: *notazioni conclusive*

Quale valutazione può essere offerta in merito alle proposte sinteticamente illustrate? Anzitutto, si può rilevare che esse potrebbero combinarsi tra loro nell'ambito di un medesimo ordinamento, visto che non sembrano escludersi reciprocamente.

Per quanto concerne il merito delle singole posizioni, la prima proposta tende a utilizzare l'IA in funzione ancillare al ragionamento umano, introducendo limitazioni al libero convincimento del giudice, laddove il rischio di errori giudiziari appare maggiormente elevato. Si tratta di un approccio prudente che, peraltro, si inserisce coerentemente nella tradizione giuridica italiana, visto che la nostra legislazione processuale penale conosce già alcune regole di valutazione negativa della prova, che vietano al giudice di trarre un certo tipo di convincimento da alcune prove giudicate carenti di efficacia persuasiva, se non in presenza di ulteriori elementi di corroborazione.

La seconda proposta, invece, insiste su una delle promesse fondamentali dell'IA, vale a dire quella di rendere maggiormente oggettive le valutazioni compiute dagli organi giurisdizionali, in ossequio al principio di legalità e di uguaglianza formale. Naturalmente, è auspicabile che le inferenze giudiziali siano dotate di un solido fondamento – in particolare quando il provvedimento risulta sfavorevole all'imputato – ma l'idea di prestabilire soglie numeriche di conferma sembra, per un verso, utopica e, per altro verso, eccessivamente restrittiva. A scanso di equivoci, si può comunque precisare che strumenti di prova connotati da tassi di errore piuttosto significativi non dovrebbero nemmeno essere considerati «idonei ad assicurare l'accertamento dei fatti», come recita l'art. 189 c.p.p.

Infine, l'ultima proposta considerata è indubbiamente assai originale e ciò contribuisce entro certi termini a renderla controversa. Essa ha il pregio di adattarsi alle caratteristiche di fondo degli strumenti di IA, ricercando una soluzione innovativa e pragmatica per un problema inedito (come garantire il diritto a un rimedio giurisdizionale effettivo, rispetto alle decisioni algoritmiche). Essa ha anche il merito di sfruttare le esperienze maturate in settori differenti rispetto a quello giudiziario e di adattare la proposta fondata sul principio di ridondanza alle necessità tipiche di tale delicato contesto. Traspare, però, anche una certa tendenza a privilegiare il confronto tra le risultanze algoritmiche in funzione pretta-

mente decisoria, relegando in secondo piano l'esigenza di giustificazione tipica dei provvedimenti giurisdizionali, in particolare negli ordinamenti – come il nostro – in cui l'obbligo di motivazione è sancito a livello costituzionale. Il rischio, in altre parole, è quello di ricadere in una decisione priva di giudizio, poiché ciò che rileva è il confronto tra i *software* disponibili nel contesto processuale, piuttosto che la comprensione profonda del significato e delle ragioni che hanno condotto alla produzione di un determinato *output*. Non a caso, gli autori che propugnano questo tipo di approccio, hanno avuto cura di precisare che i *software* di *artificial intelligence* utilizzabili in sede giudiziaria dovrebbero essere dapprima sottoposti a un procedimento di certificazione e di validazione da parte delle autorità competenti[101]; riconoscendo, in tal modo, che un eventuale contrasto tra le risultanze algoritmiche rappresenterebbe solamente il riflesso di una controversia sul "metodo" con cui dovrebbero essere progettati e sviluppati i *software* "incaricati" di svolgere un determinato compito.

Da questa angolazione visuale riemerge, ancora una volta, l'interazione tra decisione, giustificazione e IA. Difatti, se una sentenza annoverasse tra le proprie premesse fattuali elementi generati, raccolti o elaborati tramite le tecnologie di *artificial intelligence*, la motivazione del relativo provvedimento dovrebbe necessariamente indicare (art. 546, co. 1 lett. e) i risultati acquisiti e i criteri di valutazione adottati nei confronti della "prova algoritmica", nonché le ragioni per le quali il giudice ritiene non attendibili le prove contrarie, eventualmente ricavate da un elaboratore artificiale differente.

[101] V. supra, nt. 100.

Bibliografia

E. Amodio, *Motivazione della sentenza penale*, in *Enc. Dir.*, XXVII, Milano, 1977, pp. 181 ss.

E. Ancona, *All'origine della svolta epistemologica della sentenza Franzese. ricerche sulla probabilità logica o baconiana*, in *Rivista internazionale di filosofia del diritto*, 2017, n. 4, pp. 679 ss.

G. Barone, *Intelligenza artificiale e processo penale: la linea dura del Parlamento europeo. Considerazioni a margine della Risoluzione del Parlamento europeo del 6 ottobre 2021*, in *Cass. pen*., 2022, n. 3, pp. 1180 ss.

M. Biral, *L'identificazione della voce nel processo penale: modelli, forme di accertamento, tutela dei diritti individuali*, in *Riv. it. dir. proc. pen.*, 2015, n. 4, pp. 1842 ss.

A. Bonafine, *L'intelligenza artificiale applicata al ragionamento probatorio nel processo civile. È davvero possibile e/o auspicabile?*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, Milano, 2022, pp. 923 ss.

M. Caianiello, *Dangerous Liaisons. Potentialities and Risks Deriving from the Interaction between Artificial Intelligence and Preventive Justice*, in *European Journal of Crime, Criminal Law and Criminal Justice* 29 (2021), n. 1, pp. 1 ss.

G. Canzio, *La motivazione della sentenza e la prova scientifica:* "reasoning by probabilities", in G. Canzio, L. Luparia Donati (a cura di), *Prova scientifica e processo penale*, Milano, 2022, pp. 3 ss.

G. Canzio, *Intelligenza artificiale, algoritmi e giustizia penale*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, pp. 131 ss.

A. Capone, *La motivazione della sentenza*, in L. Giuliani, R. Orlandi (a cura di), *Indagini preliminari e giudizio di primo grado*. *Commento alla legge 23 giugno 2017, n.* 103, pp. 297 ss.

F. Caprioli, *Tecnologia e prova penale: nuovi diritti e nuove garanzie*, L. Luparia, L. Marafioti, G. Paolozzi, *Dimensione tecnologica e prova penale*, Torino, 2019, pp. 45 ss.

F. Caprioli, *Verità e giustificazione nel processo penale*, in G. Forti, G. Varraso, M. Caputo (a cura di), *«Verità» del precetto e della sanzione alla prova del processo*, Napoli, 2014, pp. 199 ss.

A. Caratta, *Decisione robotica e valori del processo*, in *Riv. dir. process.*, 2020, n. 2, pp. 491 ss.

G. Carlizzi, *Libero convincimento e ragionevole dubbio nel processo penale. Storia prassi teoria*, San Lazzero di Savena, 2018.

C. Casonato, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Diritto pubblico comparato ed europeo – Rivista web*, Speciale 2019, pp. 101 ss.

M. Caterini, *Verso un diritto penale inumano*, in A. Bondi, G. Fiandaca, G.P. Fletcher, G. Marra, A.M. Stile, C. Roxin, K. Volk (a cura di), *Studi in onore di Lucio Monaco*, Urbino, 2020, pp. 199 ss.

M. Cecchi, *Sfogliando* Justice Machines*: evocazioni antesignane su diritto e intelligenza artificiale*, in *Cass. pen.*, 2021, n. 12, pp. 4172 ss.

P. Comanducci, *La motivazione in fatto*, in *La conoscenza del fatto nel processo penale*, in G. Ubertis (a cura di), Milano, 1992, pp. 215 ss.

C. Conti, *Al di là del ragionevole dubbio*, in A. Scalfati (a cura di), *Novità su impugnazioni penali e regole di giudizio. Legge 20 febbraio 2006, n. 46 "legge Pecorella"*, Torino, 2006, pp. 87 ss.

F. Cordero, *Diatribe sul processo accusatorio* (1966), in *Ideologie del processo penale (con un'appendice)*, Roma, 1997, pp. 189 ss.

F. Cordero, *Prove illecite* (1961), in *Tre studi sulle prove penali*, 1963, pp. 145 ss.

F. Cordero, *Giudizio*, in *Nov. Digesto It.*, VIII, Torino, 1961, pp. 881 ss.

C. Costanzi, *La matematica del processo: oltre le colonne d'Ercole della giustizia penale*, in *Questione giustizia*, 2018, n. 4, pp. 166 ss.

M. Daniele, *Regole di esclusione e regole di valutazione della prova*, Torino, 2009.

G. Di Paolo, *L'art. 546, comma 1, lett. e): verso un nuovo modello normativo di motivazione "in fatto" della sentenza penale?*, in G.M. Baccari, C. Bonzano, K. La Regina, E.M. Mancuso (a cura di), *Le recenti riforme in materia penale. Dai decreti di depenalizzazione (d.lgs n. 7 e n. 8/2016 alla legge Orlando (l. n. 103/2017)*, Milano, 2017, pp. 241 ss.

F. D'Alessandro, *Spiegazione causale mediante leggi scientifiche, a dieci anni dalla sentenza Franzese*, in *Criminalia. Annuario di scienze penalistiche*, 2012, pp. 331 ss.

O. Di Giovine, *Il* judge-bot *e le sequenze giuridiche in materia penale (intelligenza artificiale e stabilizzazione giurisprudenziale)*, in *Cass. pen.*, 2020, n. 3, pp. 951 ss.

F.R. Dinacci, *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia: luci europee e ombre legislative*, in *Processo penale e giustizia*, 2022, n. 2, pp. 301 ss.

O. Dominioni, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Milano, 2005.

E. Fabiani, *Intelligenza artificiale e accertamento dei fatti nel processo civile*, in *Il giusto processo civile*, 2021, n. 1, pp. 45 ss.

M. Fasan, *Intelligenza artificiale e pluralismo: uso delle tecniche di profilazione nello spazio pubblico democratico*, in *BioLaw Journal – Rivista di Biodiritto*, 2019, n. 1, pp. 101 ss.

P. Ferrua, *La prova nel processo penale*, I, *Struttura e procedimento*, 2017.

P. Ferrua, *Il giudizio penale: fatto e valore giuridico*, in AA.VV., *La prova nel dibattimento penale*, Torino, 2007, pp. 315 ss.

P. Ferrua, *La colpevolezza oltre ogni ragionevole dubbio*, in L. Filippi (a cura di*), Il nuovo regime delle impugnazioni tra Corte costituzionale e sezioni unite*, Padova, 2007, pp. 137 ss.

E. Gabellini, *Algoritmi decisionali e processo civile*, in *Riv. trim. dir. e proc. civ.*, 2022, n. 1, pp. 59 ss.

E. Gabellini, *La «comodità del giudicare»: la decisione robotica*, in *Riv. trim. dir. e proc. civ.*, 2019, n. 4, pp. 1305 ss.

P. Garbolino, *A cosa serve il teorema di Bayes? Replica a Michele Taruffo*, in *Riv. dir. process.*, 2016, n. 4-5, pp. 1127 ss.

P. Garbolino, *Probabilità e logica della prova*, Milano 2014.

M. Gialuz, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, pp. 51 ss.

M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Diritto penale contemporaneo – Archivio web*, 29 maggio 2019 (disponibile *online* all'indirizzo https://archiviodpc.dirittopenaleuomo.org/, ultimo accesso il 30 giugno 2022).

R.E. Kostoris, *Predizione decisoria e* diversion *processuale*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, pp. 93 ss.

F.M. Iacoviello, *La "Franzese": ovvero quando buone teorie producono cattiva giustizia*, in *Critica del diritto*, 2014, n. 3, pp. 241 ss.

N. Irti, *Il tessitore di Goethe (per la decisione robotica)*, in A. Carleo (a cura di), *Decisione robotica*, Bologna, 2019, pp. 17 ss.

L. Luparia, G. Fiorelli, *Diritto probatorio e giudizi criminali ai tempi dell'intelligenza artificiale*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, Milano, 2022, pp. 779 ss.

L. Luparia Donati, *Notazioni controintuitive su intelligenza artificiale e libero convincimento*, in Aa.Vv, *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, pp. 113 ss.

L. Luparia, Trial by probabilities*. Qualche annotazione eretica*, in *La Corte d'assise – Rivista quadrimestrale di scienze criminalistiche integrate*, 2012,

n. 1-2, pp. 155 ss. (pubblicato anche in M. Cucci, G. Gennari, A. Gentilomo (a cura di), *L'uso della prova scientifica nel processo penale*, Santarcangelo di Romagna, 2012, pp. 95 ss.).

L. Luparia, *Introduzione. Prova giudiziaria e ragionamento artificiale: alcune chiavi di lettura*, in J. Sallantin, J.J. Szczeciniarz (a cura di), *Il concetto di prova alla luce dell'intelligenza artificiale*, Milano, 2005, pp. VII ss.

V. Maffeo, *La motivazione della sentenza. Art. 1, co. 52, l. n. 103 del 2017*, in *Archivio penale – Rivista web*, *Speciale* 2018, pp. 599 ss.

V. Manes, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, pp. 547 ss.

A.A. Martino, *Chi teme i giudici robot*, in *Riv. it. dir. proc. pen.*, 2020, n. 2, pp. 15 ss.

O. Mazza, *Il ragionevole dubbio nella teoria della decisione*, in *Criminalia. Annuario di scienze penalistiche*, 2012, pp. 357 ss.

T. Mazzarese, *Forme di razionalità delle decisioni giudiziali*, Torino, 1996.

A. Merone, *Le prove digitali e l'uso dell'intelligenza artificiale per finalità istruttorie*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, Milano, 2022, pp. 905 ss.

I. Neroni Rezende, *Facial recognition in police hands: Assessing the Clearview case from a European perspective*, in *New Journal of European Criminal Law*, 2020, n. 3, pp. 375 ss.

E. Nissan, *Digital technologies and artificial intelligence's present and foreseeable impact on lawyering, judging, policing and law enforcement*, in *Artificial Intelligence & Society* 32 (2017), n. 3, pp. 441 ss.

J. Nieva-Fenoll, *Intelligenza artificiale e processo* (2018), Traduzione e prefazione di Paolo Comoglio, Torino, 2019, p. 15.

M. Nobili, *Esiti, errori, arbitrii dietro un'illustre formula: gli ultimi trent'anni*, in *Il libero convincimento del giudice penale. Vecchie e nuove esperienze*, Milano, 2004, pp. 33 ss.

U. Pagallo, S. Quattrocolo, *The impact of AI on criminal law, and its twofold procedures*, in W. Barfield, U. Pagallo (a cura di), *Research Handbook on the Law of Artificial Intelligence*, Cheltenham-Northampton, 2018, pp. 385 ss.

G. Paolozzi, *Relazione introduttiva*, in L. Luparia, L. Marafioti, G. Paolozzi (a cura di), *Dimensione tecnologica e prova penale*, Torino, 2019, pp. 1 ss.

C. Parodi – V. Sellaroli, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco, in Diritto penale contemporaneo*, 2019, n. 6, pp. 47 ss.

G. Padua, *Intelligenza artificiale e giudizio penale: scenari, limiti, prospettive*, in *Processo penale e giustizia*, 2021, n. 6, pp. 1479 ss.

T. Padovani, *Diritto penale*, XII edizione, Milano, 2019.

F. Palmiotto, *The Black Box on Trial: The Impact of Algoritmic Opacity on Fair Trial Rights in Criminal Proceedings*, in M. Ebers, M. Cantero Gamito (a cura di), *Algorithmic Governance and Governance of Algorithms. Legal and Ethical Challenges*, Cham, 2021, pp. 49 ss.

L. Passanante, *Le sezioni unite riducono al "minimo costituzionale" il sindacato di legittimità sulla motivazione della sentenza civile*, in *Riv. trim. dir. e proc. civ.*, 2015, n. 1, pp. 179 ss.

D. Perrone, *La prognosi postuma tra distorsioni cognitive e* software *predittivi. Limiti e possibilità del ricorso alla "giustizia digitale integrata" in sede di accertamento della colpa*, Torino, 2021.

C. Piergallini, *La regola dell'"oltre ragionevole dubbio" al banco di prova di un ordinamento di Civil Law*, in M. Bargis, F. Caprioli (a cura di), *Impugnazioni e regole di giudizio nella legge di riforma del 2006: dai problemi di fondo ai primi responsi costituzionali*, Torino, 2007, pp. 361 ss.

M. Pisati, *Indagini preliminari e intelligenza artificiale: efficienza e rischi per i diritti fondamentali*, in *Processo penale e giustizia*, 2020, n. 4, pp. 957 ss.

M. Pisati, "Full collection of data" *e diritto di difesa*, in *Riv. it. dir. proc. pen.*, 2019, n. 4, pp. 2239 ss.

R. Poli, *Logica e razionalità nella ricostruzione giudiziale dai fatti*, in *Riv. dir. process.*, 2020, n. 2, pp. 515 ss.

A. Punzi, Judge in the Machine. *E se fossero le macchine a restituirci l'umanità del giudicare?*, in A. Carleo (a cura di), *Decisione robotica*, Bologna, 2019, pp. 319 ss.

S. Quattrocolo, *Per un'intelligenza artificiale utile al giudizio penale*, in *BioLaw Journal – Rivista di biodiritto*, 2021, n. 2, pp. 387 ss.

S. Quattrcolo, *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *Media Laws – Rivista di diritto dei Media*, 2020, n. 3, pp. 121 ss.

S. Quattrocolo, *Quesiti nuovi a soluzioni antiche? Consolidati paradigmi normativi vs rischi e paure della giustizia digitale "predittiva"*, in *Cass. pen.*, 2019, n. 4, pp. 1748 ss.

S. Quattrcolo, *Equità del processo penale e* automated evidence *alla luce della Convenzione europea dei diritti dell'uomo*, in *Revista italo-Española de Derecho Procesal*, 2019, n. 2, pp. 1 ss.

K. Quezada-Tavárez, P. Vogiatzoglou, S. Royer, *Legal challanges in bringing AI evidence to the criminal courtroom*, in *New Journal of European Criminal Law* 12 (2021), n. 4, pp. 531 ss.

C. Rasia, *La crisi della motivazione nel processo civile*, Bologna, 2016.

G. Riccio, *Ragionando su intelligenza artificiale e processo penale*, in *Archivio penale – Rivista web*, 2019, n. 3, pp. 1 ss. (ora anche in A.F. Uricchio, G. Riccio, U. Ruffolo (a cura di), *Intelligenza artificiale tra etica e diritto. Prime riflessioni a seguito del libro bianco dell'Unione europea*, Bari, 2021, pp. 19 ss.).

F. Santagada, *Intelligenza artificiale e processo civile*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, Milano, 2022, pp. 815 ss.

P. Sorbello, *Banche dati, attività informativa e predittività. La garanzia di un diritto penale del fatto*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2019, n. 2, pp. 374 ss.

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. process.*, 2021, n. 1, pp. 101 ss.

S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018.

G. Spangher, *Le prove che utilizzano dati raccolti mediante strumenti digitali (inoltre: captatore informatico; perquisizioni* on line*)*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, Milano, 2022, pp. 759 ss.

F. Taroni, S. Bozza, J. Vuille, *La probabilità come strumento per una coerente valutazione della prova scientifica*, in G. Canzio, L. Luparia Donati (a cura di), *Prova scientifica e processo penale*, II edizione, Milano, 2022, pp. 21 ss.,

F. Taroni, S. Bozzi, *Il significato delle evidenze: l'importanza dello scienziato forense nella prevenzione dell'errore*, in L. Lupária Donati (a cura di), *L'errore giudiziario*, Milano, 2021, pp. 661 ss.

M. Taruffo, *Brevi note sulla motivazione della sentenza* (2018), in Id., *Verso la decisione giusta*, Torino, 2020, pp. 409 ss.

M. Taruffo, *Note sparse su probabilità e logica della prova*, in *Riv. trim. dir. e proc. civ.*, 2014, n. 4, pp. 1507 ss.

M. Taruffo, *Judicial Decisions and Artificial Intelligence*, in *Artificial Intelligence and Law* 6 (1998), n. 2-4, pp. 311 ss.

M. Taruffo, *Giudizio (teoria generale)*, in *Enc. Giur. Treccani*, XVI, Roma, 1989, pp. 1 ss.

M. Taruffo, *La motivazione della sentenza civile*, Padova, 1975.

P. Tonini, *L'influenza della sentenza Franzese sul volto attuale del processo penale*, in *Dir. pen. proc.*, 2012, n. 10, pp. 1225 ss.

G. Tuzet, *L'algoritmo come pastore del giudice? Diritto, tecnologie, prova scientifica*, in *Media Laws – Rivista di diritto dei Media*, 2020, n. 1, pp. 45 ss.

G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, pp. 9 ss.
G. Ubertis, *Profili di epistemologia giudiziaria*, Milano, 2021.
G. Ubertis, *Fatto e valore nel sistema probatorio penale*, Milano, 1979.
A. Venanzoni, *La valle del perturbante: il costituzionalismo alla prova delle intelligenze artificiali e della robotica*, in *Politica dir.*, 2019, n. 2, pp. 237 ss.
D. Vicoli, *La "ragionevole durata" delle indagini*, Torino, 2012.
E. Vincenti, *Il «problema» del giudice-robot*, in A. Carleo (a cura di), *Decisione robotica*, Bologna, 2019, pp. 111 ss.

RISK AND NEED ASSESSMENT TOOLS E RIFORMA DEL SISTEMA SANZIONATORIO: STRATEGIE COLLABORATIVE E NUOVE PROSPETTIVE

Lucia Maldonato

1. Ambientamento

La rivoluzione digitale e l'imporsi delle tecniche di *Artificial intelligence* (d'ora in avanti, AI) sullo scenario del diritto e del processo penale hanno determinato uno "*shock* da modernità"[1], uno smarrimento ancora in atto per il penalista, che deve adattarsi a un nuovo linguaggio e conformare istituti e categorie tradizionali a una realtà nuova e in costante mutamento[2].

L'impiego crescente di strumenti di intelligenza artificiale pone profondi interrogativi per lo studioso di diritto[3] e, allo stesso tempo, di-

[1] Sui problemi della modernità o della post-modernità si rimanda alle sempre attuali riflessioni di F. STELLA, *Giustizia e modernità. La protezione dell'innocente e la tutela delle vittime*, Milano, 2003.

[2] In argomento, è d'obbligo rinviare all'opera di A. GARAPON, J. LASSÈGUE, *Justice digital. Révolution grafique et rupture antropologique*, Parigi, 2018. Sul punto, v. anche E. FRONZA, C. CARUSO*, Ti faresti giudicare da un algoritmo? Intervista a Antoine Garapon*, in *Questione giustizia*, 2018, n. 4, pp. 196-199.

[3] Per una panoramica generale sull'utilizzo degli strumenti di intelligenza artificiale

schiude scenari inesplorati. Questi ultimi, sebbene riguardino tematiche oggetto di risalente dibattito da parte della dottrina – come potrà apprezzarsi di qui a breve – assumono oggi nuove fattezze[4], rendendo necessaria l'assunzione di una prospettiva inedita, capace di integrare e porre in relazione i diversi saperi coinvolti.

Pare opportuno iniziare le riflessioni oggetto del presente contributo dando una prima definizione di intelligenza artificiale, consapevoli del fatto che già su questo punto si registrano posizioni discordanti.

L'art. 3 § 1 della Proposta di regolamento sull'intelligenza artificiale elaborata dalla Commissione europea[5] definisce quale "sistema di intelligenza artificiale" «un *software* sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I che può, per una determinata serie di obiettivi definiti dall'uomo, generare *output*, quali contenuti, previsioni, raccomandazioni o decisioni».

---

nell'ambito del sistema penale, cfr. F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Diritto penale e uomo- Archivio web*, 29 settembre 2019; 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*, 2014, n. 4, in part. p. 620; V. Manes, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in U. Ruffolo, *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, p. 547; C. Parodi, V. Sellaroli, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Diritto penale contemporaneo – Archivio web*, 29 maggio 2019; P. Severino, *Intelligenza artificiale e diritto penale*, in U. Ruffolo, *Intelligenza artificiale*, cit., pp. 531-545; G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2020, n. 4, pp. 75-88. Sulle nuove prospettive di utilizzabilità dell'IA nel giudizio penale e, nello specifico, come ausilio alla costruzione del libero convincimento del giudice, cfr. L. Luparia Donati, *Notazioni controintuitive su intelligenza artificiale e libero convincimento*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, pp. 113 ss. Si vedano, altresì, le considerazioni di E. Nissan, *Digital technologies and artificial intelligence's present and foreseeable impact on lawyering, judging, policing and law enforcement*, in *Artificial Intelligence & Society*, 2017, n. 3, pp. 441-464.

[4] Per la posizione di chi sembra escludere, seppur provvisoriamente, uno «sconvolgente e non auspicabile mutamento di paradigma della struttura e della funzione della giurisdizione penale», cfr. G. Canzio, *Intelligenza artificiale e processo penale*, in *Cass. pen.,* 2021, n. 3, p. 803.

[5] Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi dell'Unione, Bruxelles, 21 aprile 2021, COM (2021) 206 final.

Nella Relazione di accompagnamento al testo normativo, l'accento cade, in particolare, sugli effetti prodotti dall'impiego dei sistemi in questione, precisando che l'IA consiste «in una famiglia di tecnologie in rapida evoluzione che può contribuire al conseguimento di un'ampia gamma di benefici […] garantendo un miglioramento delle previsioni, l'ottimizzazione delle operazioni e dell'assegnazione di risorse e la personalizzazione delle soluzioni digitali disponibili per i singoli e le organizzazioni».

Nel complesso, dunque, la Proposta di Regolamento della Commissione europea enfatizza una delle aspirazioni tipiche dell'IA, vale a dire quella di risolvere i problemi in maniera più efficiente di quanto potrebbe fare l'essere umano[6]. Difatti, i *software* di AI simulano i *pattern* del ragionamento umano mirando, però, a ottenere un miglioramento esponenziale delle relative *performances*.

Un utilizzo efficiente e adeguato di tali strumenti, pertanto, impone che sia individuato preliminarmente il problema da risolvere, così da determinare precisamente la domanda cui lo strumento deve rispondere.

È ormai noto che, soprattutto nell'esperienza nord-americana, sono stati sviluppati dei *tools* di intelligenza artificiale costruiti proprio al fine di fornire una stima attendibile sul rischio di recidiva da parte del reo, vale a dire sul rischio che il soggetto interessato ricada nella commissione di nuovi fatti di reato[7].

---

[6] Il pericolo insito in questa visione dell'algoritmo è che, come contraltare, vi è un rischio per la conoscenza umana: quest'ultima, assuefatta dall'efficienza dell'algoritmo, potrebbe pigramente accettarne gli esiti senza investigare adeguatamente sul suo funzionamento. Su queste tematiche si rinvia a T. Numerico, *Big data e algoritmi. Prospettive critiche*, Roma, 2021, pp. 126 ss. Sui limiti del giudizio umano e delle decisioni fondate su dati quantitativi, cfr. le riflessioni di O. Di Giovine, *Dilemmi morali e diritto penale. Istruzioni per un uso giuridico delle emozioni*, Bologna, 2022, spec. pp. 19 ss.

[7] Si tratta dei cosiddetti "algoritmi predittivi" del rischio di recidiva: su questo tema, si vedano in particolare M. Caianiello, *Dangerous Liasons. Potentialities and Risks Deriving from the Interaction between Artificial Intelligence and Preventive Justice*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2021, n. 1, pp. 1-23; B. Galgani, *Considerazioni sui "precedenti" dell'imputato e del giudice al cospetto dell'IA nel processo penale*, in *Sistema penale – Rivista web*, 2020, n. 4, pp. 81-94; M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Diritto penale contemporaneo – Archivio web*, 29 maggio 2019.

Come si può intuire, la domanda che si pone all'algoritmo è di particolare delicatezza, poiché riguarda la probabilità che si verifichi un evento futuro ed incerto, determinato da una molteplicità di fattori che, in quanto tale, rappresenta un accadimento difficilmente prevedibile.

Se di estrema delicatezza è la domanda, la risposta non è di minore complessità. In che modo potrebbe tradursi in linguaggio binario l'oggetto della predizione in esame? In effetti, analizzando i molteplici algoritmi già esistenti[8], è agevole osservare come ciascuno di essi agganci la propria predizione a un diverso "oggetto". L'*output* "rischio di ricaduta nel reato", infatti, a volte viene fatto coincidere con un nuovo arresto per un delitto (è l'esempio costituito dall'algoritmo ORAS); altre volte, invece, con una nuova condanna (un esempio è fornito dall'algoritmo COMPAS); altre volte, ancora, con una semplice nuova violazione dell'ordine dell'autorità di polizia che comporti la revoca della *probation* (è il caso dell'algoritmo OST). Se queste sono le premesse, è chiaro quanto sia complesso ricondurre a unità una categoria di strumenti che servono a illuminare valutazioni tra loro profondamente diverse, funzionali all'emanazione di provvedimenti che intervengono anche in fasi processuali differenti[9].

Ai fini del presente contributo, interessa analizzare quegli algoritmi che tentano di fornire un dato generale sulla futura commissione di un fatto di reato, in seguito all'accertamento della responsabilità per un illecito penale che sia già stato commesso e accertato in quanto tale. Tale questione è di grande interesse per il penalista, poiché il rischio di commissione di illeciti futuri costituisce uno degli elementi sulla base del quale definire una reazione adeguata al reato, nel senso di un trattamento sanzionatorio che possa dirsi individualizzato[10]. In questa prospettiva, si

[8] Per un ampio ed esaustivo compendio di tutti tali strumenti si rinvia a J.P. Singh, D.G. Kroner, J.S. Wormith, S.L. Dermarais, Z. Hamilton (a cura di), *Handbook of recidivism Risk/Needs Assessment*, 2018, *passim*.

[9] Evidenzia la necessità di differenziare la valutazione sugli strumenti di *risk assessment* a seconda del differente obiettivo cui tende il provvedimento che si basa sui risultati dello stesso, S. Quattrocolo, *Sui rapporti tra pena, prevenzione del reato e prova nell'era dei modelli computazionali psico-criminologici,* in *Teoria e critica della regolazione sociale*, 2021, n. 1, p. 264.

[10] L'individualizzazione della sanzione penale è da sempre al centro del dibattito scientifico, costituendo oramai un principio fondamentale del diritto penale. Pur non es-

cercherà, dapprima, di comprendere se (e come) gli algoritmi predittivi del rischio di recidiva possano entrare a far parte dell'arsenale a disposizione del giudice nel complesso giudizio sul rischio posto dal condannato; in seguito se, a livello sistematico, essi possano davvero costituire un ausilio per risolvere un problema endemico del sistema di giustizia penale, ossia quello di definire una reazione adeguata rispetto alla commissione di determinati fatti di reato.

2. Risk assessment, risk management *e algoritmi: qualcosa di nuovo sotto il sole?*

A bene vedere, pur con tutte le cautele del caso, rimane comunque possibile individuare un fondamento unitario degli strumenti in questione. Essi, infatti, sono tutti preordinati a effettuare un *risk assessment*, ossia a fornire indicazioni di massima su un evento futuro e incerto. In particolare, per quanto interessa in questa sede, si tratta della stima in ordine alla probabilità della ricaduta nella commissione di un fatto di reato

---

sendo espressamente incluso nella Carta costituzionale, esso entra a far parte della stessa a seguito di numerose sentenze della Consulta che, ragionando sulla portata degli articoli 25 e 27 Cost., hanno affermato che la legalità della pena non può prescindere dall'individualizzazione di questa. L'individualizzazione, infatti «si pone come naturale attuazione e sviluppo di principi costituzionali, tanto di ordine generale (principio di uguaglianza) quanto attinenti direttamente alla materia penale»: C. cost., sent. 2 aprile 1980 n. 50. Di recente, la C. cost. ha approfondito il principio di individualizzazione della pena soprattutto con riferimento alla concessione dei benefici penitenziari (cfr. C. cost., sent. 15 febbraio 2022 n. 33). Tale principio è stato inoltre utilizzato come strumento per scardinare i restanti automatismi sanzionatori presenti all'interno del sistema (v., di recente, C. cost., sent. 31 marzo 2021 n. 56). In argomento si vedano le riflessioni di A. Carcano, *Automatismi: tra ragionevolezza e individualizzazione della pena*, in *Forum di Quaderni costituzionali – Rassegna*, 2021, 4. Il principio di individualizzazione della pena è stato, peraltro, oggetto di un recentissimo e ricco approfondimento, in dottrina, di M. Venturoli, *Modelli di individualizzazione della pena. L'esperienza italiana e francese nella cornice Europea*, Torino, 2020; sul tema cfr. anche M. Pifferi, *L'individualizzazione della pena: difesa sociale e crisi della legalità penale tra Otto e Novecento*, Milano, 2013. Sulla individualizzazione della sanzione penale, con particolare riferimento agli strumenti di *risk assessment*, si vedano le considerazioni di S. Quattrocolo, *Artificial intelligence*, *Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Cham, 2020, p. 143.

da parte di un soggetto che è già condannato in precedenza. Com'è noto, valutazioni di questo genere innervano il processo penale in diverse fasi, trovando la massima espansione nel momento di esecuzione della pena[11]. La necessità di effettuare una prognosi circa le future condotte dell'imputato costituisce, dunque, già allo stato attuale un passaggio obbligato nelle valutazioni del giudice e le tecnologie di IA, attraverso la loro potenza di calcolo e la disponibilità di *data-set* potenzialmente sterminati, potrebbero offrire nuova linfa per questa tipologia di giudizi, segnando l'evoluzione verso modelli "computazionali" di valutazione del rischio[12].

Occorre, tuttavia, sgombrare subito il campo da un pericoloso equivoco, che costituisce il principale fondamento delle riserve espresse da più parti nei confronti dell'impiego dei *tools* di predizione del rischio nel settore della giustizia penale. Tra gli operatori, invero, si registra uno scetticismo diffuso, poiché molti ritengono che tali strumenti potrebbero rivelarsi fatali per i diritti e le garanzie dell'imputato. Si tratta di un pericolo concreto, che non deve essere sottovalutato, motivo per cui occorre adottare un approccio improntato alla massima cautela, in modo da consentire l'implementazione di tali strumenti nel rispetto delle dovute guarentigie.

A ben vedere, la radice di questo fraintendimento alligna nello stesso concetto di *risk assessment*, che non sempre viene adeguatamente compreso. È necessario, difatti, tenere presente che il *risk assessment* è un processo di valutazione del rischio e non un metodo in grado di fornire una predizione esatta[13]. Si tratta, dunque, di uno strumento utile per stimare il rischio e i bisogni criminogenici del singolo, al fine di gestire

[11] Si pensi a quanto accade in tema di trattamento penitenziario del *sex offender*. In argomento la letteratura è copiosa: per gli opportuni approfondimenti si rinvia a P. Giulini, *Il reato sessuale. Problematica, epidemiologia e principi generali di trattamento*, in P. Giulini, C.M. Xella (a cura di), *Buttare la chiave? La sfida del trattamento per gli autori di reati* sessuali, Milano, 2011; M. Bertolino, *Il trattamento del delinquente sessuale tra legislazione e prassi. Introduzione al focus*, in *Rivista italiana di medicina legale*, 2013, pp. 1805-1821. Si vedano altresì le considerazioni di D. Petrini, *Il trattamento del delinquente sessuale, tra esigenze securitarie e controllo della recidiva*, *ivi*, pp. 1823 ss.

[12] Cfr. S. Quattrocolo, *Sui rapporti tra pena, prevenzione del reato e prova*, cit., p. 259.

[13] Diffusamente, in tema, cfr. G. Zara, D.P. Harrington, *Criminal Recidivism: explanation, prediction and prevention*, Londra, 2016, pp. 148 ss. Sul punto, v. anche S. Quattrocolo, *Sui rapporti tra pena, prevenzione del reato e prova*, cit., p. 258.

adeguatamente una situazione pericolosa: un mezzo e non un fine in sé stesso[14]. In altre parole, poiché il *risk score* costituisce una "fotografia" del rischio, esso può rivelarsi utile soltanto nella misura in cui fornisca le informazioni necessarie per individuare le misure di intervento e di prevenzione più adeguate in relazione al caso concreto, nella prospettiva, dunque, del cosiddetto *risk management*.

La precisazione di questo profilo può concorrere a mitigare i sospetti nei confronti degli algoritmi predittivi, che non sono altro che strumenti preformati di *risk assessment*[15]: una sequenza di istruzioni in base alle quali il calcolatore elabora un processo, che consente di addivenire a un risultato concreto (*output*). Quest'ultimo, tuttavia, non realizza una predizione finale, ma offre soltanto un valore grezzo; sul quale si deve immancabilmente innestare una nuova valutazione.

È importante, inoltre, effettuare alcune precisazioni sul concreto funzionamento degli algoritmi predittivi, al fine di maturare una visione completa sulla reale consistenza delle informazioni ottenute mediante il loro impiego e sul relativo significato.

Il coefficiente di rischio oggetto del calcolo viene generato dall'incrocio tra le diverse categorie di dati inseriti nella base dell'algoritmo, che possono essere suddivisi in dati "di gruppo" (attinenti ai comportamenti di individui arrestati o condannati) e "dati personali" (che si riferiscono al reo e alla sua storia individuale).

Gli strumenti classificano il soggetto interessato in base alla interazione fra questi dati e, in tal modo, l'algoritmo fornisce una stima circa la probabilità che un imputato si impegni in un comportamento criminale *qualsiasi*, in un *futuro più o meno prossimo*[16]. Anche da questo punto di

---

[14] Su questo aspetto, cfr. S. Quattrocolo, *Artificial Intelligence, Computational Modelling*, cit., pp. 131 ss.; Ead., *Sui rapporti tra pena, prevenzione del reato e prova*, cit., pp. 272 ss.

[15] In argomento si vedano le considerazioni effettuate in *Harvard Law Review*, 2017, pp. 1530 ss.

[16] Per una approfondita analisi delle modalità di costruzione ed utilizzo dei software di intelligenza artificiale, si rinvia a J. Eaglin, *Constructing recidivism risk*, in *Emory Law Journal*, 2017, n. 1, pp. 59-122. Si vedano, nella prospettiva di una maggiore apertura all'utilizzo degli strumenti di predizione del rischio di recidiva, sul presupposto della riduzione dei *biases* che attualmente li connotano, R. Simmons, *Quantifying criminal procedure: how to unlock the potential of Big Data in our criminal justice system*, in *Michigan State Law Review*, 2016, pp. 947-1017.

vista, dunque, emergono i limiti connaturati all'utilizzo degli algoritmi predittivi; che, ovviamente, si riflettono sullo stesso concetto di *risk score*, quale *output* del relativo processo. Questi limiti meritano di essere ulteriormente approfonditi, soprattutto per comprendere l'atteggiamento da tenere rispetto alle potenzialità (e ai rischi) degli strumenti in esame.

3. Risk assessment, Artificial intelligence *e processo penale:* networks *e* hubs

La rivoluzione linguistica e culturale che il recepimento delle tecnologie di IA ha realizzato nell'ambito del diritto conferma ciò che i filosofi sostengono già da tempo, ossia il fatto che la centralità delle *new technologies* – categoria cui l'IA indiscutibilmente appartiene – modella l'attuale volto della società e genera riflessi non soltanto in ambito antropologico ma anche sulla sfera socio- giuridica[17].

Specialmente in ambito giuridico, la diffusione delle *new technologies* ha determinato l'affermazione di categorie e di modelli di ragionamento fondati essenzialmente sui concetti di rete e di *network*. Tali categorie si prestano a descrivere la sfera giuridica nel suo complesso, in quanto l'odierno tessuto sociale e le norme che lo disciplinano sfuggono ad una lettura imperniata su categorie tradizionali. La sfera giuridica, dunque, si connota come rete e i soggetti si trovano ad agire in un contesto ad elevata complessità, fatto di intersezioni, di nodi, attraverso i quali la rete si espande in maniera progressiva e rizomatica.

A voler allargare l'angolo prospettico, potrebbe sembrare che la "rete" diritto e la "rete" costituita dal sapere scientifico scontino un'incomunicabilità strutturale, non esistendo nodi (o *hub*) che riescano a far intersecare le rispettive strutture.

Tuttavia, a voler considerare anche il sistema penale come una rete, pare possibile individuare una dimensione in cui tale sistema e il sapere scientifico anche connotato in termini di incertezza possono intersecarsi, identificando un luogo concettuale di composizione delle diversità, ossia

[17] Cfr. G. Bombelli, *Sfera giuridica e scenari contemporanei: intorno al diritto come "rete"*, in *L'Ircocervo. Rivista elettronica italiana di metodologia giuridica, teoria generale del diritto e dottrina dello stato*, 2011.

quello in cui tali diversi saperi si trovano a dover collaborare per trovare nuove soluzioni, che necessitano appunto di apporti multidisciplinari[18].

In tale prospettiva, il concetto di *hub* è particolarmente utile, in quanto fotografa bene quelle intersezioni sulle quali è necessario lavorare, al fine di risolvere i problemi senza le chiusure tipiche delle singole discipline di appartenenza.

Ebbene, gli *hubs* di interesse per l'argomento che qui ci occupa, sono costituiti dalle intersezioni tra tecniche di *risk assessment* e processo penale che, già allo stato attuale, sono presenti nel sistema processuale. Tali aree di intersezione, di cui si procederà a una rapida ricognizione, si prestano ad essere interessate dall'avvento dei *risk assessment tools*, con problemi che si andranno di qui a poco ad analizzare.

Valutazioni sul concreto rischio di commissione di ulteriori reati vengono infatti ordinariamente compiute dal giudice, per esempio, allorché si trovi a decidere sull'applicabilità di una misura cautelare, dovendo valutare il cosiddetto "pericolo di reiterazione del reato" *ex* art. 274, co.1, lett. c) c.p.p.

In maniera non dissimile, nell'ipotesi di messa alla prova ai sensi dell'art. 168 *bis* c.p., si richiede un'indagine sull'imputato per la definizione del programma costituente l'oggetto della *probation*. La decisione sui contenuti del progetto presuppone una vera e propria "radiografia" dell'imputato[19] e contempla, tra i diversi fattori da considerare, anche il rischio di recidiva posto dal reo.

Ancora, considerazioni sul potenziale rischio di nuova offesa vengono effettuate in sede di commisurazione della pena. Come è noto, l'art. 133 c.p. richiede che, oltre alla gravità del reato, si valuti anche la capacità a delinquere del colpevole, desunta dai motivi a delinquere, dal carattere del reo, dai precedenti penali e giudiziari, dalla condotta contemporanea o susseguente al reato e dalle condizioni di vita individuale, familiare e sociale del reo.

A ben vedere la capacità a delinquere possiede una marcata ambi-

[18] In tale prospettiva deve richiamarsi quanto affermava, in una prospettiva epistemologica, K. Popper, *Postscript to the Logic of Scientific Discovery,* London, 1982, trad. it. *Poscritto alla logica della conoscenza scientifica*, vol. I, Milano, 1984, p. 35: «non ci sono discipline; ci sono soltanto problemi e l'esigenza di risolverli».

[19] L'espressione è di L. Bartoli, *La sospensione del procedimento con messa alla prova*, Milano, 2020, p. 256.

valenza, potendo essere interpretata tanto in ottica retributiva, come componente rivolta al passato, quanto in ottica special-preventiva, intesa dunque come attitudine del soggetto a commettere nuovi reati, secondo una visione prognostica[20]. La dottrina prevalente, in effetti, considera la capacità a delinquere proprio come attitudine del soggetto a commettere in futuro nuovi reati, in analogia con il concetto di "pericolosità", presupposto applicativo delle misure di sicurezza[21].

Particolarmente esplicativo da questo punto di vista è l'indice costituito dal carattere del reo, che implica una considerazione complessiva della personalità dell'agente e delle sue componenti "innate", idonee a orientare il comportamento futuro di quest'ultimo: in questa prospettiva dovranno essere valutate le capacità di autocontrollo del reo, la sua stabilità emotiva, la percezione della realtà[22].

Così intesa la capacità a delinquere, risulta meglio comprensibile come, proprio in relazione alla valutazione di questo parametro – che ingloba il concreto rischio di reiterazione del reato – gli strumenti di IA potrebbero non soltanto coadiuvare il giudice ma, più in generale, traghettare l'intero sistema penalistico verso nuovi scenari, capaci di garantire all'imputato un'esecuzione della pena conforme al canone dell'individualizzazione.

3.1. I problemi con particolare riferimento alla commisurazione della pena

Sennonché l'esperienza americana, che vale la pena di anticipare, evidenzia una serie di problematiche indefettibilmente connesse all'utilizzo degli algoritmi predittivi.

Difatti, l'utilizzo di strumenti di *risk assessment* in sede di commisu-

[20] In questo senso, si sottolinea come tale parametro possa dare ingresso in fase di commisurazione della pena alla categoria della colpevolezza per tipo d'autore e alla colpevolezza per condotta di vita o per carattere. Su questi temi si rinvia, a L. Goisis, *sub* Art. 133 c.p., in E. Dolcini, G.L. Gatta, *Codice penale commentato*, Milano, 2021, pp. 2010 ss.

[21] Su tale aspetto, nella manualistica, si rinvia alle considerazioni di G. Fiandaca, E. Musco, *Diritto penale. Parte generale*, Bologna, 2019, pp. 802-803.

[22] In relazione a tali profili si rinvia a M. Romano, G. Grasso, *Commentario sistematico del codice penale*, II, IV ed., Milano, 2012, pp. 354 ss. Da ultimo, cfr. L. Goisis, *sub* Art. 133 c.p., cit., p. 2025.

razione della pena è oramai invalso nell'ordinamento statunitense. Pionieristico è stato il caso di Eric Loomis, che ha aperto il dibattito globale in tema di algoritmi predittivi. Nel 2013 Loomis era stato dichiarato colpevole dei reati di ricettazione e di resistenza a pubblico ufficiale ed era stato condannato alla pena di sei anni di reclusione e di cinque anni di *extended supervision*, irrogate anche sulla base del coefficiente di rischio di recidiva posto dallo stesso come risultante dall'algoritmo denominato COMPAS[23].

Loomis aveva contestato tale decisione, lamentando la violazione del suo diritto a un giusto processo, asserendo nello specifico che fosse stato frustrato il proprio diritto a ottenere una sentenza individualizzata. Il caso, arrivato sino alla Corte suprema del Wisconsin, si era concluso con il rigetto delle doglianze di Loomis, ritenute infondate: la Corte suprema, infatti, aveva ritenuto che, per scongiurare il pericolo di una decisione basata unicamente su un trattamento automatizzato, fosse sufficiente il controllo umano operato dalla corte di merito sul dato algoritmico[24].

Dalla vicenda Loomis emergono diversi problemi, che spaziano dalla stessa struttura del *software*, alla sua comprensibilità, fino alle problematiche attinenti alla possibilità per il giudice di rimanere imparziale nella valutazione del dato prodotto dal *software*.

Iniziando dalla questione principale, è noto che tutti i software di *risk assessment*, ivi compreso COMPAS, producono un risultato frutto dell'elaborazione di dati che si riferiscono a gruppi di persone, pertanto un risultato intrinsecamente statistico. Come evidenziato dalla dottrina più avveduta, non si può fare completo affidamento su strumenti che predicono il comportamento del singolo sulla base di metodologie statistiche[25],

[23] COMPAS è l'algoritmo predittivo che, sulla base dei dati inseriti nel sistema e di un questionario di 137 domande che si sottopone al reo, attribuisce allo stesso uno *score*, un punteggio che esprime il rischio di ricaduta nella commissione di reati. COMPAS è però un algoritmo coperto da *trade secret*; conseguentemente, alla Corte era stato fornito il nudo dato matematico espressivo del rischio di recidiva, senza alcuna delucidazione circa i meccanismi di funzionamento del software. Su questi temi si rinvia alle considerazioni di L. D'Agostino, *Gli algoritmi predittivi per la commisurazione della pena*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2019, n. 2, pp. 354-373.

[24] Cfr. Wisconsin Supreme Court, *State v. Loomis*, case 2015AP157-CR, Judgement July 13th 2016, in *Harvard Law Review* 130 (2017), pp. 1530 ss.

[25] Cfr. D.J. Cooke, C. Mitchie, *Limitation of diagnostic precision and predictive utility in the individual case: a challenge for forensic practice*, in *Law and Human be-*

proprio perché la condotta individuale è determinata da variabili che non sono ponderabili né possono essere oggetto di un'esatta previsione. La natura probabilistica di questa valutazione, insomma, impedisce di affidarsi esclusivamente a tali strumenti, pena il rischio di ridurre la persona a una mera entità numerica, producendo una sorta di "reificazione" dell'imputato, in palese contrasto con le garanzie del giusto processo[26].

Se, in primo luogo, è la connotazione essenzialmente probabilistica del dato algoritmico a preoccupare lo studioso, non si può trascurare che, pure volendo utilizzare tali strumenti in sede processuale, si pone comunque un problema di comprensibilità dell'algoritmo stesso[27]. Questi strumenti sono infatti costruiti principalmente attraverso tecniche di *machine learning*, o di apprendimento automatico, tali per cui il programmatore si occupa della raccolta dei dati, compendiati in *training set*, che sono funzionali all'addestramento del modello computazionale[28]. I dati già presenti all'interno dell'algoritmo si fondono con quelli relativi al caso concreto secondo dinamiche che non sono note nemmeno ai programmatori, rendendo di fatto il risultato del calcolo non intellegibile.

Come se non bastasse, alla incomprensibilità ontologica del *tool* si somma la sua natura privatistica: gran parte dei *software* predittivi del

---

haviour, 2010, 34, pp. 259-74, ove si evidenzia quanto segue: «*on the basis of empirical findings, statistical theory, and logic, it is clear that predictions of future offending cannot be achieved, with any degree of confidence, in the individual case*».

[26] In questo senso, cfr. le riflessioni di 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. process.*, 2021, n. 1, pp. 101-110.

[27] Si tratta della cosiddetta "opacità" dell'algoritmo. In generale, su questo tema, cfr. F. Palmiotto, *The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, in M. Ebers, M. Cantero Gamito (a cura di), *Algorithmic Governance and Governance of Algorithms. Legal and Ethical Challanges*, Cham, 2021, pp. 49-70.

[28] Sulla tecnica di *machine learning* e sulle differenze con il *Model base* AI si rinvia alle considerazioni di F.C. La Vattiata, *La responsabilità penale per danni da intelligenza artificiale alla prova del processo*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, Milano, 2022, p. 696. Diffusamente, sull'argomento, cfr. B. Panattoni, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale*, in *Il diritto dell'informazione e dell'informatica,* 2021, n. 2, pp. 317 ss.

rischio di recidiva sono, infatti, coperti dal segreto industriale[29]; circostanza che preclude la conoscenza del relativo codice sorgente.

È evidente che tali caratteristiche rendono lo strumento inutilizzabile all'interno del processo, in quanto non sarebbe possibile in alcun modo controllarne i risultati né, tantomeno, esercitare il contraddittorio sulle sue modalità di funzionamento (e, dunque, sull'attendibilità e sulla rilevanza delle informazioni da esso prodotte)[30].

Occorre, peraltro, ancora considerare che il tasso di errore immanente alle tecniche algoritmiche di *risk assessment* è tutt'altro che irrilevante, nonostante le promesse di oggettività e certezza sottese all'utilizzo di un linguaggio altamente formalizzato, come quello matematico. Non solo, con riferimento specifico all'algoritmo COMPAS la società *no profit* Pro Publica ha condotto un interessante studio che ha evidenziato come l'algoritmo in questione sia affetto da un *racial bias*[31], cioè da un errore sistemico in base al quale gli imputati di colore vengono automaticamente classificati tra i soggetti con il più alto rischio di recidiva in ragione della propria etnia di provenienza. Ciò avviene perché i dati raccolti riflettono la composizione della popolazione carceraria dello Stato di riferimento, ove la maggior parte dei soggetti reclusi appartengono alla minoranza di colore[32].

---

[29] Sulla praticabilità dell'imposizione del segreto industriale sui software di predizione del rischio, si veda S. Quattrocolo, *Artificial intelligence*, cit., p. 177.

[30] Sul problema dell'esercizio di un adeguato contraddittorio e sulla necessità che anche lo strumento algoritmico soggiaccia allo scrutinio di scientificità secondo le cadenze del c.d. *Daubert test*, cfr. C. Costanzi, *La matematica del processo: oltre le colonne d'Ercole della giustizia penale*, in *Questione giustizia*, 2018, n. 4, pp. 166-188.

[31] L'organizzazione *Pro Publica* ha condotto l'indagine anzidetta sullo stesso campione di persone utilizzato per costruire l'algoritmo COMPAS. *ProPublica* ha operato una valutazione dei dati scomposti per gruppi etnici e ha appurato così che l'algoritmo è particolarmente fallace nell'etichettare i giovani di colore come futuri criminali, con un tasso di errore doppio rispetto ai soggetti bianchi. L'analisi normalizzata ha evidenziato infatti che gli accusati di colore risultavano avere il 77% di probabilità in più di essere indicati a rischio maggiore di commettere futuri crimini violenti. Lo studio è reperibile al seguente indirizzo: www.propublica.org/article/technical-response-to-northpointe.

[32] L'indagine di *Pro Publica* ha svelato l'elevatissimo tasso di errore degli algoritmi: dei potenziali recidivi individuati dal software solo il 20% aveva effettivamente commesso un nuovo crimine. Allargando l'analisi ai reati minori, poi, è stato evidenziato che il tasso di accuratezza degli algoritmi raggiungeva appena il 61%, l'equivalente del lancio di una moneta.

A tutto ciò occorre aggiungere che uno degli ostacoli maggiori all'utilizzabilità di un algoritmo predittivo, così come evidenziato in precedenza[33], sta nel fatto che il dato numerico è, per il suo nitore e la sua asetticità, in grado di affascinare il giudice, che potrebbe inconsapevolmente rimanere vittima di tale dato e non metterlo nemmeno in discussione, decidendo nel senso indicato da quest'ultimo[34].

Tuttavia, l'ostacolo fondamentale e di carattere generale che si frappone all'ammissibilità di strumenti di *risk assessment* all'interno del nostro ordinamento è quello che deriva dal loro retroterra concettuale, che pone in discussione, seppur in modo sottile, il principio della presunzione di non colpevolezza[35]. Tale ostacolo è ben colto dalla Risoluzione

[33] V. *supra*, cap. II., spec. § 2.1.

[34] È il fenomeno che in psicologia cognitiva viene definito *anchoring*, ossia la tendenza comune degli individui ad affidarsi al dato disponibile, senza prestare adeguato riguardo alla debolezza esplicativa dello stesso. Sul fenomeno dell'*anchoring* e sui diversi *biases* presenti al momento della decisione si rinvia all'indagine di A. Tversky, D. Kanheman, *Judgement under uncertainty: Heuristics and biases*, Cambridge, 1982. Di recente, si vedano le interessanti considerazioni, soprattutto in tema di *anchoring*, di A. Forza, G. Menegon, R. Rumiati, *Il giudice emotivo. La decisione tra ragione ed emozione*, Bologna, 2017, p. 144. Evidenzia il pericolo che vi sia un «acritica sottomissione alla predizione algoritmica» M. Caianiello, *Dangerous Liasons*, cit., p. 15. Il medesimo pericolo di adesione fideistica al dato probatorio si è posto anche con riferimento al sapere neuroscientifico, in argomento cfr. M. Bertolino, *Il vizio di mente tra prospettive neuroscientifiche e giudizi di responsabilità penale*, in *Rassegna italiana di criminologia*, 2015, pp. 84-98 e in part. p. 88. Estremamente interessante, poi è quella giurisprudenza che apre alla considerazione del dato proveniente dalle indagini neuroscientifiche sulla premessa che questo venga inserito e si raccordi al compendio probatorio complessivo a disposizione dell'organo giudicante. In tema si rinvia a Trib. Como, 20 maggio 2011, Gup Lo Gatto, in *Riv. it. dir. med. leg.*, 2012, pp. 246-267. Sul punto cfr. anche le riflessioni di S. Signorato, *Il diritto a decisioni penali non basate esclusivamente su trattamenti automatizzati*, cit., p. 107. La dottrina specialistica, assai di frequente, ammonisce circa il pericolo che gli strumenti *di risk assessment* possano essere utilizzati non per identificare il rischio, quanto più per giustificare decisioni già prese, v. G. Zara, D.P. Harrington, *Criminal Recidivism: explanation, prediction and prevention*, cit., p. 152. Si veda, ancora, l'interessante contributo di C. Canullo, *Chi decide? Intelligenza artificiale e trasformazioni del soggetto nella riflessione filosofica*, in E. Calzolaio (a cura di), *La decisione nel prisma dell'intelligenza artificiale*, Milano, 2020, pp. 25-35.

[35] Evidenzia assai efficacemente come esista un collegamento sottile tra la presunzione di innocenza e la predizione dei comportamenti futuri dell'imputato, S. Quattrocolo, *Artificial Intelligence*, cit., p. 136. D'altra parte, in dottrina si osserva da tempo

del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e sul suo utilizzo da parte delle autorità di polizia e giudiziarie, ove si afferma quanto segue (Considerando Q):

> considerando che la diffusione dell'IA nel settore delle attività di contrasto e nel settore giudiziario non dovrebbe essere considerata una mera questione di realizzabilità tecnica ma piuttosto una decisione politica riguardante la progettazione e gli obiettivi dei sistemi di attività di contrasto e di giustizia penale; che il moderno diritto penale si basa sull'idea che le autorità reagiscono a un reato dopo che è stato commesso, senza supporre che le persone siano pericolose e debbano essere sorvegliate costantemente per prevenire possibili illeciti; che le tecniche di sorveglianza basate sull'IA mettono in dubbio profondamente tale approccio e impongono ai legislatori in tutto il mondo di valutare con attenzione le conseguenze derivanti dalla diffusione delle tecnologie che riducono il ruolo dell'essere umano nelle attività di contrasto e di giudizio.

Alla luce di tutte le criticità evidenziate parrebbe, dunque, impossibile riconoscere uno spazio di operatività agli strumenti di *risk assessment* in fase di commisurazione della pena. Anche a voler imporre un "controllo umano significativo" sullo strumento algoritmico, non sembra che alcuna verifica sul dato numerico possa essere realmente esperibile, dato che esso si impone alla mente del giudice con la forza derivante dalla sua (pretesa) oggettività.

Nondimeno, sarebbe affrettato escludere qualsiasi possibilità di utilizzo degli strumenti predittivi del rischio; dovendosi, piuttosto, ragionare sulle guarentigie da rafforzare per poter fare affidamento sul contributo offerto dall'IA, senza scadere in facili riduzionismi.

Se questo è l'obiettivo, si può iniziare a ragionare muovendo dalla for-

---

come risulti di dubbia costituzionalità l'impiego di misure cautelari a fini di tutela della collettività, come prevede l'art. 274 lett. c) c.p.p., considerato che «proprio il principio del rifiuto di considerare l'imputato colpevole, anche in presenza di 'gravi indizi' a suo carico per un reato relativamente al quale non abbia riportato una condanna definitiva, non sembra consentire un giudizio di pericolosità concernente la commissione da parte sua di futuri reati, fondato sulla valutazione dei suoi non ancora acclarati comportamenti riguardanti il fatto (in corso di ricostruzione giudiziaria) per cui si procede»: G. Ubertis, *Sistema di procedura penale*, I, *Principi generali*, Milano, 2017, p. 235. A tal riguardo, v. però l'orientamento espresso da Corte cost., sent. 23 gennaio 1980 n. 1.

mulazione di un'ipotesi controfattuale: chiedendosi, cioè, cosa potrebbe accadere se, nonostante le criticità evidenziate, agli algoritmi predittivi si desse concreta operatività nella fase di commisurazione della pena.

Allo stato attuale, nel contesto del processo penale italiano, la conoscenza del coefficiente di rischio di recidiva posto dal condannato potrebbe essere utile al giudice esclusivamente per una finalità: aumentare o diminuire la pena in linea con il tasso di recidiva espresso dall'algoritmo. È un dato di fatto che il sistema italiano di giustizia penale si struttura come una ''clessidra'', tale per cui il condannato passa sempre e comunque da una condanna determinata in senso aritmetico a una permanenza, anche minima, nell'istituto carcerario e/o marginalmente a una pena pecuniaria[36]. Solo in un momento successivo alla decisione, infatti, risulta possibile effettuare una valutazione in merito al ricorso a modalità esecutive della pena diverse da quelle già fissate con la sentenza di condanna.

Tale passaggio è tuttavia necessitato in quanto, come la dottrina più accorta segnala ormai da tempo, il sistema sanzionatorio italiano è affetto da un'endemica limitatezza, che concentra tutte le forza sulla reclusione inframuraria, secondo un'opzione radicalmente carcero-centrica.

La "limitatezza" della reazione punitiva, poi, si spiega ancora meglio se si considera che il giudice della cognizione non possiede informazioni sul carattere e sulla personalità del condannato: ai sensi dell'art. 220 c.p.p., infatti, si fa divieto di esperire una perizia psicologica o qualsiasi analisi sulla personalità del reo in fase di cognizione[37]. Se tale divieto trovava la sua giustificazione (almeno nelle intenzioni originarie del legislatore) nella necessità di evitare condizionamenti del giudice sulla base delle caratteristiche personologiche dell'autore di reato, non si può trascurare come la completa ignoranza di tali caratteristiche precluda una ricostruzione esaustiva di quanto si è verificato con la commissione del reato. Di conseguenza, risulta assai difficile anche predisporre un tratta-

[36] Su questi temi si rinvia alla recente indagine di L. Eusebi, *La pena tra necessità di strategie preventive e nuovi modelli di risposta al reato*, in *Riv. it. dir. proc. pen.*, 2021, n. 3, pp. 823 ss.

[37] Sulle problematiche relative al divieto di perizia psicologica in fase di cognizione e sulla necessità di un superamento di tale sbarramento, si vedano le riflessioni di P. Moscarini, *La perizia psicologica e il "giusto processo*", in *Dir. pen. proc*., 2006, n. 8, pp. 929 ss.

mento sanzionatorio autenticamente individualizzato, cioè parametrato sulle esigenze concrete e sulle necessità del reo.

Se queste sono le problematiche all'ordine del giorno, non ci si può più limitare a ragionare su di esse ovvero sulle prospettive di mutamento del sistema senza nemmeno provare a offrire soluzioni inedite e supporti che contribuiscano a produrre tale mutamento. È in questa prospettiva, dunque, che intendiamo guardare anche agli algoritmi predittivi, in quanto strumenti in grado di fornire un contributo in termini di efficienza alla risoluzione del problema costituito dalla coerenza del trattamento sanzionatorio rispetto alle esigenze tipiche dell'autore di reato.

4. Rischi e bisogni criminogenici: risk and need assessment tools *e* responsivity principle

Nella discussione in tema di algoritmi predittivi del rischio di recidiva vi è sempre la tendenza a enfatizzare il carattere "oscuro" di questi strumenti, in una prospettiva che rievoca gli scenari del "*Big brother*" di orwelliana memoria. Tale tendenza, nondimeno, rende più complesso apprezzare il contributo conoscitivo che, seppur con tutte le cautele necessarie per la loro corretta utilizzazione, gli algoritmi predittivi sono in grado di offrire. In questa prospettiva, suscitano particolare interesse i cosiddetti *risk and need assessment tools*.

Questi ultimi sono strumenti che, attraverso la valutazione dei fattori di rischio, dei bisogni criminogenici[38] e della responsività del soggetto (secondo il c.d. *responsivity principle*) mettono in luce le caratteristiche della persona a tutto tondo, riuscendo così a fornire la base informativa più completa per la definizione di strategie di gestione del rischio posto dal singolo individuo[39].

[38] Per bisogni criminogenici si intendono gli aspetti di una persona o della situazione che tale persona vive, che, alterandosi, possono implicare un cambiamento nel suo comportamento criminale, quali ad esempio l'impiego del soggetto o l'attitudine antisociale. La dottrina usa di frequente in maniera alternativa le locuzioni bisogni criminogenici e fattori di rischio dinamici. Su tutti questi punti si rinvia a S. Quattrocolo, *Sui rapporti tra pena, prevenzione del reato e prova,* cit., p. 277.

[39] Gli strumenti sono diversi a seconda dei principi in base ai quali li si costruisce, difatti la considerazione, nel *data set*, di alcuni dati e non di altri riflette una scelta di prin-

A fondamento di tali strumenti stanno alcune teorie psico-criminologiche[40] che spiegano il comportamento criminale come effetto dell'interazione di diversi fattori, biologici e biografici, che sono specifici e variano a seconda dell'*offender*. Da tali teorie sembra, dunque, emergere come i fattori di rischio posti dal reo altro non siano se non la manifestazione di una necessità, di un'esigenza dello stesso, che non può essere ignorata nel momento della definizione della reazione sanzionatoria.

Non si deve pensare che, alla base di queste riflessioni, vi sia la considerazione "lombrosiana" dell'uomo come essere predeterminato. Né si vuole negare l'autodeterminazione individuale, ritenendo possibile ed opportuno classificare gli autori di reato in pericolosi/bisognosi (da sorvegliare) e non pericolosi, come avviene nell'esperienza del *targeting* americano[41]. Concezioni di questo tipo scivolano inesorabilmente verso un'idea riduzionista, che considera l'uomo alla stregua di una variabile «misurabile», «controllabile», «dipendente»[42].

Senza assumere prese di posizione aprioristiche in relazione ai fattori che possono influire sul comportamento criminale, occorre invece valorizzare tutti quei saperi, adeguatamente corroborati, che possano essere utili alla risoluzione dei problemi. In definitiva, gli strumenti di

---

cipio del programmatore. Su questi temi cfr. J. Eaglin, *Constructing recidivism risk*, cit., p. 87; cfr. altresì le considerazioni di S. Quattrocolo, *Sui rapporti tra pena, prevenzione del reato e prova,* cit. pp. 280 ss., ove evidenzia che i principali rischi per l'imputato nei cui confronti vengono applicati tali strumenti derivano dall'attendibilità dell'approccio criminologico adottato e, sulla scorta di questo, delle modalità di costruzione dello stesso. Effetti discriminatori potrebbero infatti derivare dall'irrilevanza criminologica dei fattori considerati o dalla duplicazione nel calcolo del medesimo fattore.

[40] Di particolare interesse sono le teorie di J. Bonta, D.A. Andrews, *Risk-Need Responsivity Model for Offender Assessment and Rehabilitation*, Ottawa, 2007, pp. 1-22.

[41] Il meccanismo del *targeting*, di origine americana, costituisce uno strumento per un più efficace controllo sulla *compliance* degli enti in ambito ambientale. I controlli delle agenzie si concentrano, infatti, su un ristretto numero di imprese, che in più occasioni hanno commesso violazioni della normativa in tema di tutela delle componenti ecologiche. In generale, sul tema, cfr. E. Helland, *The enforcement of pollution control Laes: inspections, violations and self-reporting*, in *The review of economics and statistics*, 1998, n. 1, pp. 141 ss. Assume una posizione di scetticismo nei confronti di tali teorie M. Caianiello, *Dangerous Liasons.* cit., p. 13.

[42] Su tale questione si rinvia alle riflessioni di E. Greco, *Profili di responsabilità penale del controllore del traffico aereo. Gestione del rischio e imputazione dell'evento per colpa nei sistemi a interazione complessa*, Torino, pp. 3 ss.

cui si parla consentono prima di tutto di individuare potenziali fattori in grado di influire su di un comportamento e, in seconda battuta, di comprendere come la persona condannata possa essere sostenuta, attraverso un programma individualizzato e coerente con le sue specifiche necessità.

In tale ottica, al fine di meglio comprendere ruolo e contributo che i *risk and need assessment tools*[43] possono fornire, è opportuno analizzarne la struttura, fondata essenzialmente sui principi del *risk*, del *need* e della *responsivity*.

Attraverso l'analisi del rischio, si individua il soggetto da trattare, in quanto individuo che presenta un'elevata probabilità di commettere un nuovo reato. Essenziale è, pertanto, la caratterizzazione e la raccolta dei dati che siano realmente espressivi dei fattori di rischio correlati alla recidiva. È evidente il rilievo che, per tali fini, assume la corretta selezione dei dati, tanto dal punto di vista della loro correlazione con la recidiva, tanto dal punto di vista della genuinità del campione, al fine di evitare che si producano risultati pregiudizievoli, espressivi di *biases*[44].

I più forti fattori predittivi sono stati per esempio individuati nell'attitudine criminale, nelle relazioni con soggetti appartenenti a contesti criminali, nella personalità antisociale.

Se la considerazione del rischio posto è importante per individuare i soggetti su cui concentrarsi, centrale è la caratterizzazione del *"need"*, ossia delle concrete esigenze del reo, che costituiscono il contraltare di quel rischio: sono, infatti, tali esigenze l'oggetto su cui dovrà focalizzarsi il trattamento e alle quali dovrà riferirsi la gestione del rischio[45].

A tale fine è necessario disporre delle informazioni più ampie possibili sulle effettive esigenze del condannato. Tali informazioni possono

---

[43] Tali strumenti rientrano nel c.d. *structured professional judgment*, che sfrutta un approccio anamnestico, basandosi su un esame accurato della vita e della carriera criminale dell'individuo, sul punto cfr. G. Zara, D.P. Harrington, *Criminal Recidivism: explanation,* cit., pp. 164 ss.

[44] Sul tema dell'errore algoritmico, si rinvia a A. Carlson, *The Need for Trasparency in the Age if Predictive Sentencing Algorithms*, in *Iowa Law Reiew.*, 2017, n. 1, p. 319; A. Chander, *The Racist algorithms*, in *Michigan Law Review*, 2017, n. 6, p. 1028.

[45] È questa l'essenza del *risk principle* di Andrew Bonta, secondo cui «*supervision should address the offender's need that are directly linked to criminal behaviour*»: cfr. J. Bonta, D.A. Andrews, *Risk-Need Responsivity Model for Offender,* cit., p. 5.

essere reperite tanto attraverso un questionario *self report*[46], quanto attraverso un'intervista *face to face*[47], in modo da ricostruire la personalità, la storia, l'esperienza del reo, per meglio comprendere sia i cosiddetti "fattori criminogenici", sia i fattori non criminogenici, senza trascurare i cosiddetti "fattori protettivi".

Tra i fattori criminogenici possono annoverarsi il luogo dove la persona conduce la propria vita, lo *status* occupazionale, la dipendenza da sostanze stupefacenti, la tipologia e l'intensità delle relazioni familiari o coniugali, il livello di istruzione e di integrazione del reo.

Tra i fattori non criminogenici rientrano invece quei tratti della personalità che, seppure non direttamente collegati ad una eventuale commissione di un reato, costituiscono comunque l'indice di un carattere che potrebbe, con l'esperienza, incorrere nella commissione di fatti di rilevanza penale. Tratti simili, da individuare e trattare adeguatamente, sono ad esempio l'autostima carente, la presenza di sentimenti di ansia e malinconia, l'eventuale presenza di disturbi mentali o una debole salute fisica.

Nel compendio di informazioni relative al reo non bisogna poi trascurare i c.d. *protective factors*[48], ossia quei fattori che fungono da freno inibitorio alla ricaduta nel fatto reato; i quali risultano profondamente diversi da persona a persona[49].

Individuare i fattori da trattare, tuttavia, non è sufficiente, dovendosi comprendere i meccanismi migliori attraverso cui approcciarsi al reo. Di questo aspetto si cura il c.d. *responsivity principle*, ossia quel principio in base al quale si suggeriscono le modalità attraverso le quali strutturare il trattamento in ragione delle caratteristiche personali del soggetto, quali

---

[46] Un esempio di algoritmi di questo genere è quello costituito da COMPAS, cfr. *supra*, nota 19.

[47] Si evidenzia come sia fondamentale condurre un'intervista professionale con l'*offender*, condotta da un *trained assessment administrator* soprattutto ai fini della caratterizzazione delle esigenze criminogeniche in AA.VV., *Offender Risk & Need Assessment Instruments: A Primer for Courts*, National Center for State Courts, 2014, p.11.

[48] Su tale principio D.A. Andrews, J. Bonta, R.D. Hoge, *Classification for effective rehabilitation: Rediscovering psycology*, in *Criminal Justice and Behaviour*, 1990, n. 1, pp. 19-52.

[49] Tra i fattori protettivi possono annoverarsi la presenza di un contesto familiare che possa accogliere il reo, il grado di istruzione e tutti quei fattori in grado di ridurre o neutralizzare l'incidenza dei fattori di rischio, migliorando la resilienza del soggetto.

ad esempio lo stato di salute fisico o mentale o l'eventuale presenza di disturbi di ansia, in maniera tale da offrire più incoraggiamenti e meno punizioni[50]. Tale approccio, insomma, prova a cogliere e sfruttare positivamente le (già presenti) abilità di apprendimento del reo, attraverso la definizione di trattamenti cognitivo-comportamentali e approcci che siano disegnati sullo stile di apprendimento, le motivazioni, le abilità e le forze specifiche dell'*offender*.

Un esempio assai interessante in tal senso è fornito dall'*Offender Screening Tool* (OST)[51], fondato sulle teorie di Andrew Bonta. Dal 1996 tale strumento viene utilizzato presso la Contea di Maricopa ed è tutt'ora utilizzato nelle decisioni sul *probation* in Virginia. Interessante è anche l'*Ohio Risk Assessment System* (ORAS)[52], utilizzato nello Stato dell'*Ohio* per strutturare il trattamento sanzionatorio per soggetti arrestati per un nuovo crimine.

Non bisogna commettere l'errore di trascurare l'obiezione che si fonda sulla natura profondamente eccentrica dei *risk assessment tools* rispetto al nostro sistema e alla nostra tradizione giuridica, poiché essi vengono ritenuti espressivi di un diritto penale dell'autore e non di un diritto penale del fatto. D'altronde, non si può negare che i *tools* in questione nascono e si sviluppano in un sistema, come quello nord-americano, profondamente diverso da quello europeo, maggiormente informato al principio del *command and control* che non alla prospettiva della risocializzazione attraverso la persuasione[53].

Allo stesso tempo, non si può, sulla base di tali ragioni di principio,

---

[50] Su queste tematiche si rinvia alle riflessioni di J.L. Ferguson, *Putting the "what work" research into practice. An Organizational Perspective*, in *Criminal Justice and Behaviour*, 2002, n. 4, pp. 472-492.

[51] In tema, cfr. AA.VV., *Offender Risk & Nedd Assessment Instruments*, cit., p. A-44. Si veda anche l'indagine di C. Valerio, *Predicting recidivism using the Offender Screening Tool*, The University of Arizona, 2020, reperibile all'indirizzo http://hdl.handle.net/10150/645760.

[52] Cfr. E.J. Latessa, B. Lovins, J. Lux, *The Ohio Risk Assessment System,* in AA.VV., *Handbook of Recidivism Risk*, cit., pp. 147 ss.; v. anche AA.VV., *Offender Risk & Need Assessment Instruments*, cit., p. A-52.

[53] Su tali tematiche e, in particolare, sulla necessità che il sistema promuova un approccio che consenta al condannato la revisione critica del fatto commesso, in modo da consentire allo stesso di riappropriarsi del valore violato, cfr. L. Eusebi, *La riforma ineludibile del sistema sanzionatorio penale*, in *Riv. it. dir. proc. pen.*, 2013, pp. 1307-1328.

andare dimentichi del contributo decisivo che questi strumenti possono apportare sul piano informativo. La forza degli algoritmi potrebbe, in questa prospettiva, costituire presupposto e occasione per ragionare con serietà sulla necessità di cambiare prospettiva sulla questione del trattamento dell'autore di reato e sulla necessità ormai indifferibile per il giudice di cognizione di poter disporre di un adeguato compendio di informazioni sulla persona coinvolta nel fatto, al fine di dialogare con maggiore consapevolezza[54], già nella fase di commisurazione della pena, su un trattamento sanzionatorio che sia *tailored made* sulle caratteristiche del reo.

Soltanto in questa maniera risulterà possibile strutturare un programma di intervento efficace ed efficiente. Un trattamento sanzionatorio sproporzionato, difatti, finisce per danneggiare anziché favorire il processo rieducativo: una condanna eccessiva, per esempio, allontana il reo dal valore violato, anziché riavvicinarlo ad esso, ostacolando in tal modo il suo pieno recupero. È altrettanto evidente che ciò costituirebbe il riflesso di un utilizzo improprio del *tool*, e la definizione, sulla base di questo, di un progetto sanzionatorio eccessivamente severo o, al contrario, eccessivamente lasco potrebbe apportare più danni che benefici in capo al reo, nonché un'ingente perdita di risorse.

5. Risk and need assessment tools *e l'insostenibile limitatezza dell'apparato di pene principali*

In conclusione, siamo ancora ben lontani dalla possibilità di utilizzare gli algoritmi di predizione del rischio all'interno del nostro ordinamento, nonostante ampi siano i margini – come si è avuto modo di vedere – entro cui tali strumenti potrebbero trovare applicazione. Tuttavia, è

[54] Sul punto, cfr. L. Eusebi, *La pena tra necessità di strategie preventive e nuovi modelli*, cit., p. 828, ove evidenzia «Nel sistema punitivo odierno, l'instaurarsi di un'interlocuzione (di un dialogo) tra ordinamento giuridico e destinatario della condanna risulta posticipato, per quanto concerne la pena detentiva, alla fase dell'esecuzione in carcere, secondo ciò che prevede l'articolo 13, terzo comma, o.p.p, comunque, alla fase del rapporto con il servizio sociale, nel caso in cui sia applicata una misura alternativa senza ingresso in carcere. Assume rilievo, cioè, in un momento assai tardivo rispetto alla commissione del reato».

evidente come lo scenario prospettato sia assolutamente irrealizzabile, allo stato attuale, atteso che il nostro sistema punitivo presenta una serie di criticità, che impediscono di considerare la pena come un progetto di intervento realmente rieducativo, un *case planning* orientato al recupero del condannato. Ciò accade, come anticipato, soprattutto in ragione della limitatezza dell'arsenale delle pene principali, da anni oramai oggetto di aspre critiche della dottrina penalistica e, di recente, oggetto dell'attenzione del legislatore riformista[55].

Il problema del sovraffollamento carcerario[56], stigmatizzato dalla Corte europea dei diritti dell'uomo sin dal noto caso Torreggiani[57], costituisce ancora oggi uno dei nodi più urgenti da sciogliere per garantire la legalità della pena così come delineata dalla giurisprudenza costituzionale.

Ciò è frutto anche di quella logica che pone al centro della reazione punitiva l'istituzione carceraria, sulla quale si riversano le aspettative securitarie del contesto sociale. L'opzione carcerocentrica, tuttavia, si è rivelata non più sostenibile, poiché neutralizza e dimentica il condannato, obliterando la condizione tutta umana del cambiamento[58]. Se si guarda a

---

[55] Il riferimento è alla l. 27 settembre 2021 n. 134 («Delega al Governo per l'efficienza del processo penale nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari») con la quale, tra le altre cose, si impone al legislatore di procedere a una revisione complessiva del sistema sanzionatorio, cfr. *infra*.

[56] Sui numeri effettivi del sovraffollamento e sulle condizioni a seguito della pandemia Covid-19, si rinvia ai dati del XVII Rapporto Antigone, consultabile al sito www.antigone.it.

[57] Corte eur. dir. uomo, sent. 8 gennaio 2013, Torreggiani e altri c. Italia.

[58] Evidenzia l'importanza di ricordare che la condizione umana di cambiamento debba essere tenuta in considerazione soprattutto quando si utilizzano valutazioni statiche di rischio, che «tendono a dipingere l'individuo come immutabile, senza tener conto che una possibile evoluzione della sua condizione influenzerebbe significativamente il rischio di recidiva», S. Quattrocolo, *Sui rapporti tra pena, prevenzione del reato*, cit., p. 274. La necessità di tenere sempre in considerazione la prospettiva di un possibile cambiamento del reo è messa in luce da C. cost., sent. 11 luglio 2018 n. 149, in www.cortecostituzionale.it, ove si evidenzia che tale prospettiva è «sottes[a] allo stesso art. 27, co.3 Cost. – secondo cui la personalità del condannato non resta segnata in maniera irrimediabile dal reato commesso in passato, foss'anche il più orribile; ma continua ad essere aperta alla prospettiva di un possibile cambiamento. Prospettiva, quest'ultima, che chiama in causa la responsabilità individuale del condannato nell'intraprendere un cam-

tale scelta dal punto di vista strettamente economico, tale convincimento trova forza ancora maggiore, stante il forte impatto sulla spesa pubblica della componente carceraria.

Il problema del carcerocentrismo è stato, tra l'altro, preso in considerazione dalla recentissima riforma Cartabia, seppur tangenzialmente. Come è noto, la legge delega n. 134/2021 ha imposto al legislatore di procedere alla revisione delle sanzioni penali, *ex* art. 1, co.14-17 e co.21-23. Nonostante a questi fosse stato affidato il compito di rivitalizzare il sistema sanzionatorio, nel tentativo di allontanarlo dalla logica della neutralizzazione del reo e di concretizzare il carattere di *extrema ratio* della pena, anche sulla scorta della giustizia riparativa, la strada percorsa è stata quella della sostituzione sanzionatoria, già sperimentata con la l. 24 novembre 1981 n. 689. Si è così rinunciato a sperimentare la strada, certamente più complessa e coraggiosa, della previsione di nuove tipologie sanzionatorie, già al livello astratto della comminatoria edittale.

Di conseguenza, ancora oggi e nonostante l'afflato riformatore, il nostro sistema di giustizia penale continua a presentare la caratteristica conformazione a clessidra, già evidenziata in precedenza, ove passaggio obbligato per ogni condannato è la definizione in primo luogo di una pena carceraria.

Non si può, da ultimo, dimenticare quanto la dottrina specialistica evidenzia ormai da tempo: la pena detentiva ignora la fondamentale condizione umana di cambiamento, rinunciando così a un trattamento strutturato sulle caratteristiche specifiche del soggetto, che potrebbe avere maggiori *chances* di successo.

Alla luce di tutto ciò, la necessità di poter dialogare sulla pena *prima* dell'irrogazione della stessa continua ad essere persistente. Sembra che i tempi siano oramai maturi per iniziare a pensare a reazioni sanzionatorie che si svincolino dallo schema della reclusione inframuraria come

---

mino di revisione critica del proprio passato e di ricostruzione della propria personalità, in linea con le esigenze minime di rispetto dei valori fondamentali su cui si fonda la convivenza civile; ma che non può non chiamare in causa – assieme – la correlativa responsabilità della società nello stimolare il condannato ad intraprendere tale cammino, anche attraverso la previsione da parte del legislatore – e la concreta concessione da parte del giudice – di benefici che gradualmente e prudentemente attenuino, in risposta al percorso di cambiamento già avviato, il giusto rigore della sanzione inflitta per il reato commesso, favorendo il progressivo reinserimento del condannato nella società».

principale opzione e che lo facciano già in sede di irrogazione della pena nei confronti del reo. Sembra, insomma, giunto il momento di pensare all'individualizzazione della sanzione penale non soltanto come dosimetria di una pena tra minimi e massimi edittali, ma come reazione contro una specifica manifestazione criminale, e cioè come risposta all'unicità dell'esperienza umana che si è verificata con la commissione del fatto di reato oggetto del giudizio.

Muovendo da queste premesse, pare proprio che gli strumenti di intelligenza artificiale e nello specifico i *risk and need assessment tools* possano offrire un utile ausilio in funzione del cambiamento di paradigma di cui si discute, in particolare per la definizione di progetti di sanzioni strutturati sulle concrete esigenze criminogeniche poste dal reo.

5.1. La pena come progetto

Al riguardo, occorre ricordare che la dottrina già da qualche tempo discorre del significato della pena come progetto e, in particolare, del precipitato di tale prospettiva teorica, vale a dire la pena prescrittiva.

La discussione sulla pena prescrittiva, intesa come un programma di intervento sulla frattura prodotta dal reato e non come un'inflizione di male corrispondente al disvalore ravvisato nel fatto colpevolmente prodotto, nasce sulla scorta di quegli orientamenti di giustizia restaurativa, che vogliono costruire un percorso «che promuova la responsabilizzazione dell'autore di reato con riguardo ai beni aggrediti e consenta una previsione affidabile di comportamento conforme alla legalità, da parte del medesimo, per il futuro»[59]. La responsabilizzazione di cui si è detto potrebbe essere più efficacemente promossa, a parere della dottrina di riferimento, con un programma prescrittivo, rispetto alla condanna a una pena detentiva.

Non a caso, la possibilità di rispondere al reato tramite la definizione di un progetto con il consenso del reo viene ammessa – anzi, incentivata – sia in seguito alla condanna (ad esempio, attraverso la misura alternativa dell'affidamento in prova al servizio sociale), sia prima che quest'ulti-

[59] Così L. Eusebi, *La pena tra necessità di strategie preventive e nuovi modelli*, cit., p. 829.

ma sia intervenuta (tramite l'istituto della sospensione del procedimento con messa alla prova).

Anche alla luce di tutti questi argomenti, il Gruppo di lavoro dell'Associazione italiana dei Professori di Diritto penale, incaricato di avanzare proposte in tema di riforma del sistema sanzionatorio, ha formulato un interessante articolato che prevede l'innesto di un nuovo catalogo di pene principali, strutturato sulla pena pecuniaria, sulla pena prescrittiva e, come *extrema ratio*, sulla reclusione[60].

La pena prescrittiva, in particolare, si caratterizza come una sanzione a contenuto progettuale, volta a consentire al condannato la revisione critica del fatto commesso. Essa non costituisce una mera flessibilizzazione della condanna originaria al carcere, bensì un mezzo radicalmente nuovo, costruito per evitare l'ingresso nello stesso, attraverso la definizione di un progetto di reazione al reato conforme agli obiettivi di contrasto di quella specifica manifestazione criminale.

Per raggiungere tali fini, la pena prescrittiva presenta dei contenuti assai peculiari: dall'art. 3 del Progetto del Gruppo di lavoro, dedicato ai contenuti della pena prescrittiva, si evince che quest'ultima consiste nell'adempimento di un programma la cui esecuzione è seguita dal servizio sociale e che comprende, congiuntamente o disgiuntamente, obblighi di fare, divieti ed eventuali obblighi di presentazione.

Tra i diversi obblighi previsti vi è la partecipazione a programmi rieducativi, consistenti in incontri con operatori dell'Ufficio per l'esecuzione penale esterna, le restituzioni, i risarcimenti e l'impegno teso a eliminare le conseguenze del reato, la prestazione di lavori di pubblica utilità e lo svolgimento di un programma terapeutico e socio-riabilitativo.

Di particolare interesse è, inoltre, il riferimento all'adempimento di un programma, un progetto di sanzione, che può contemplare attività aventi rilievo rieducativo con riguardo al reato commesso, in favore del bene giuridico offeso, della persona offesa dal reato o delle vittime di analoghi reati; come anche la partecipazione a una procedura di mediazione penale con la persona offesa dal reato.

[60] Tutta la documentazione relativa alle proposte di riforma del sistema sanzionatorio formulate in seno all'Associazione italiana dei professori di diritto penale è reperibile e liberamente consultabile al seguente link: https://www.aipdp.it/aipdp-documenti/La-riforma-del-sistema-sanzionatorio.

Ebbene, a fronte di una pena dai contenuti così diversificati, gli algoritmi potrebbero svolgere un ruolo importante sin dal momento della irrogazione di tale sanzione. Tra l'altro – sia detto per inciso – le modalità di irrogazione della pena prescrittiva paiono saldare le istanze provenienti dalla dottrina penalistica sostanziale e processuale, nella misura in cui entrambe sottolineano l'importanza di separare la fase della decisione sulla responsabilità da quella di commisurazione della pena, sulla falsariga di quanto avviene negli ordinamenti che conoscono la scissione tra i momenti, rispettivamente, del giudizio in senso stretto e del *sentencing*[61].

Con particolare riferimento al procedimento applicativo, nella proposta formulata dal Gruppo di lavoro si prevede che, quando il giudice decide di applicare una pena prescrittiva, pronuncia sentenza di condanna senza determinazione della pena, proseguendo nella medesima udienza o in udienze successive, ai fini della suddetta determinazione. È in tale frangente, ed è questo il punto rilevante, che l'imputato può formulare proprie proposte circa il contenuto della pena prescrittiva e può, soprattutto, documentare la propria condizione personale, familiare o sociale.

La decisione, infatti, avviene dopo che il giudice abbia ascoltato il difensore, le valutazioni del pubblico ministero, eventuali ulteriori interlocuzioni tra le parti, nonché, se lo richiede, l'imputato.

Alla luce di tutto ciò, appare evidente che il giudice potrà portare a termine il proprio compito più efficacemente se potrà giovarsi di un ampio e dettagliato apparato informativo su rischi e sulle esigenze del reo, per inquadrare le condizioni di questo e strutturare così prescrizioni adeguate. In tale contesto, a bene vedere, uno strumento in grado di poter apportare un ricco compendio di notizie sul reo potrebbe essere proprio l'algoritmo di *risk assessment*.

Se correttamente utilizzato, infatti, l'algoritmo di *risk assessment* potrebbe costituire uno strumento per guidare il giudice nel determinare con cognizione di causa la pena *irroganda*, fornendogli uno spettro di elementi circa la personalità dell'autore di reato e le sue condizioni di vita, così da meglio definire i contenuti della pena prescrittiva, ponendosi

[61] In questo senso, si vedano le considerazioni di S. Quattrocolo, *Artificial intelligence*, cit., p. 139. Nella dottrina penalistica, cfr. L. Eusebi, *La pena tra necessità di strategie preventive e nuovi modelli*, cit., p. 838.

come argine al «rumore»[62] e ai *biases*[63] inevitabilmente presenti nelle decisioni giudiziali.

Utilizzato in tal senso, il *tool* di IA sarebbe in grado di diventare un reale supporto per il giudice, senza sostituirsi allo stesso[64], in quanto potrebbe costituire lo strumento in grado di riempire di contenuto la pena prescrittiva. Inoltre, attraverso una caratterizzazione più precisa della situazione da gestire, si potrebbe anche rispondere al fiume di critiche che hanno investito tale nuovo modello sanzionatorio, tacciato di eccessiva indeterminatezza nei contenuti e dunque sospettato di essere affidato alla discrezionalità assoluta del giudice nella sua determinazione, con uno svuotamento surrettizio del principio di legalità della pena.

La preoccupazione, insomma, è che la pena prescrittiva non assicuri adeguati limiti garantistici dell'intervento penale, in considerazione degli ambiti di discrezionalità applicativa che affida al giudice[65], preoccupazione che può essere però arginata attraverso una maggiore collaborazione e integrazione tra le diverse discipline, di cui a breve si dirà.

In conclusione, i contenuti della pena prescrittiva riposano su una chiara premessa: la commissione di un fatto di reato riflette l'esistenza di fattori economici, sociali e culturali che contribuiscono a determinare la commissione dell'illecito e, in forza di ciò, si comprende come un trattamento sanzionatorio realmente orientato al recupero del reo e alla sua risocializzazione non possa trascurare la necessità di incidere su tali fattori. L'introduzione di strumenti di questo tipo costituisce, a ben vedere, un'o-

---

[62] Per "rumore" sistemico si intende la dispersione casuale, tutti quegli errori inevitabilmente presenti all'interno di un sistema o di una procedura che ne minano l'efficienza. Su questi temi, si rinvia all'opera di D. Kahneman, O. Sibony, C. Sunstein, *Rumore. Un difetto del ragionamento umano*, Milano 2021.

[63] Sul particolare profilo dei *biases* e delle *fallacies* che contaminano la decisione giudiziale in fase decisoria, cfr. R. Rumiati, C. Bona, *Dalla testimonianza alla sentenza. Il giudizio tra mente e cervello,* Bologna, 2018, pp. 133 ss. Più n generale, sul problema dell'errore e del suo innestarsi nella logica giudiziaria, si vedano le riflessioni di G. Carlizzi, *Errore giudiziario e logica del giudice nel processo penale*, in L. Luparia (a cura di), *L'errore giudiziario*, Milano, 2021, pp. 93 ss.

[64] Più in generale, parla di un affiancamento del giudice, di una sorta di tecno-umanesimo ove vanno a contaminarsi *humanitas* e *techne*, M. Caterini, *Il giudice penale robot*, in *La legislazione penale – Rivista web*, 19 dicembre 2020.

[65] Per una puntuale contestazione di tutte le critiche anzidette, si rinvia a L. Eusebi, *La pena tra necessità di strategie preventive e nuovi modelli*, cit., pp. 839-840.

pera di "prevenzione primaria", ossia una strategia che interviene in primo luogo sui fattori determinanti il crimine e che rappresenta il presupposto per qualsiasi strategia politico criminale che possa considerarsi effettiva[66].

6. Un nodo da sciogliere: tsunami digitale e strategie collaborative

Non resta a questo punto che domandarsi quali potrebbero essere le prospettive futuribili. Come la dottrina più sensibile ha evidenziato, dinanzi allo "tsunami digitale" che ha investito le nostre società è incontestabile come l'impiego dell'AI nel settore giudiziario non possa essere

> ridotta a mera massimizzazione delle risorse, a puro efficientamento economico, ma debba piuttosto essere concepita quale volano atto a trasformare infrastrutture e procedure decisorie nell'ottica di una miglior salvaguardia dei canoni del giusto processo[67].

A bene vedere, dunque, l'algoritmo predittivo potrebbe costituire uno strumento che, fornendo una base conoscitiva più ampia in ordine allo stato del condannato, arricchirebbe le modalità di risposta al reato nel rispetto dei principi fondamentali di proporzionalità e di dignità della persona[68], realizzando le istanze di individualizzazione della pena e dando concretezza alla sua funzione rieducativa.

In questa prospettiva, inoltre, potrebbe inverarsi quel "controllo umano significativo"[69] che, secondo la dottrina e la giurisprudenza, risulta

---

[66] Si vedano ancora le considerazioni di L. Eusebi, *La pena tra necessità di strategie preventive e nuovi modelli*, cit., pp. 843 ss. con particolare riferimento al profilo della reazione ai reati colposi.

[67] Cfr. B. Galgani, *Considerazioni sui "precedenti" dell'imputato*, cit., p. 82.

[68] In questo senso, v. M. Bertolino, *Il vizio di mente*, cit., p. 220.

[69] Sottolinea la necessità, sulla scorta della Carta etica europea sull'intelligenza artificiale, di rimanere saldamente ancorati a una visione non solo etica ma antropocentrica dell'impiego delle tecniche di IA nel processo penale, per «riconoscere alle medesime una funziona esclusivamente ausiliare e complementare della giustizia amministrata dagli uomini, volta a rafforzare e ad amplificarne l'efficacia e le potenzialità», R.E. Kostoris, *Predizione decisoria,* diversion *processuale e archiviazione*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, pp. 93 ss. Sulla centralità del controllo umano significativo, cfr. anche G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, cit., p. 83, il quale ritiene che esso possa

essenziale per assicurare che l'algoritmo non si ponga in contrasto con le garanzie dell'imputato, come precisato anche nel caso Loomis dalla Corte Suprema del Wisconsin per affermare la legittimità della sentenza emessa sulla scorta dei risultati di COMPAS.

È evidente che simili risultati possono essere raggiunti soltanto sul presupposto di una reale e fattiva collaborazione tra giudici ed esperti[70], assieme all'apprestamento di adeguate risorse tanto nella prospettiva della formazione degli operatori tecnici e dei giudici, quanto nella prospettiva di stimolare maggiori investimenti nella digitalizzazione, che sembrano oggi realizzabili a seguito delle recenti proposte di riforma conseguenti all'approvazione del PNRR.

Al ricorrere di determinati accorgimenti, dunque, pare che la strada per gli algoritmi non sia affatto sbarrata: sarà necessario, come si è visto, prestare attenzione ai dati oggetto della base algoritmica, individuando i fattori che si pongono realmente in collegamento con la recidiva, porre allo strumento una domanda chiara sull'oggetto della previsione, dando centralità al *training*, alla formazione degli operatori del sistema di giustizia penale, nell'ottica di una più ampia collaborazione nella risoluzione dei problemi che travalicano i limiti delle singole discipline e necessitano di essere affrontati con un approccio integrato.

---

essere realizzato al ricorrere di alcune condizioni, tra le quali: il funzionamento pubblico e vagliato conformemente ai criteri di *peer review*, la conoscenza del potenziale tasso d'errore e la salvaguardia del contraddittorio. Nell'esperienza italiana, particolarmente interessante è la vicenda analizzata da TAR Lazio, sez. III, sent. 13 settembre 2019, n. 10963, che si è trovato a dover giudicare della legittimità della decisione di trasferimento per alcuni docenti dalla Puglia alla Lombardia, decisione presa da un algoritmo in uso al Ministero dell'Istruzione per gestire il processo di mobilità nazionale straordinaria della docenza scolastica. La sentenza si è pronunciata stigmatizzando l'inaffidabilità dell'algoritmo, che deve essere utilizzato secondo il principio di non esclusività della decisione. È necessario, infatti, garantire che l'esito del processo di valutazione non sia esclusivamente nelle mani della macchina e che vi sia un controllo umano sul risultato, essendo l'essere umano l'unico soggetto cui poter attribuire la responsabilità per la scelta compiuta. Su tale decisione, cfr. le riflessioni di T. Numerico, *Big data e algoritmi*, cit., pp. 204-205.

[70] Sulla imprescindibilità di tale collaborazione, cfr. già S. Quattrocolo, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *La legislazione penale – Rivista web*, 18 dicembre 2018. Più in generale, sulla necessaria integrazione tra saperi, cfr. M. Bertolino, *Le parole del diritto e le parole della scienza: un difficile dialogo su questioni di prova penale*, in *Jus – on line*, 2017, fasc. 2, pp. 2-34.

Bibliografia

AA.VV., *Offender Risk & Need Assessment Instruments: A Primer for Courts*, National Center for State Courts, 2014.

D.A. Andrews, J. Bonta, R.D. Hoge, *Classification for effective rehabilitation: Rediscovering psycology*, in *Criminal Justice and Behaviour* 17 (1990), n. 1, pp. 19 ss.

L. Bartoli, *La sospensione del procedimento con messa alla prova*, Milano, 2020.

F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Diritto penale e uomo – Archivio web*, 29 settembre 2019 (disponibile *online* al seguente indirizzo: https://archiviodpc.dirittopenaleuomo.org/upload/3089-basile2019.pdf, ultimo accesso il 30 giugno 2022).

M. Bertolino, *Le parole del diritto e le parole della scienza: un difficile dialogo su questioni di prova penale*, in *Jus – on line*, 2017, n. 2, pp. 2 ss.

M. Bertolino, *Il vizio di mente tra prospettive neuroscientifiche e giudizi di responsabilità penale*, in *Rassegna italiana di criminologia*, 2015, pp. 84 ss.

M. Bertolino, *Il trattamento del delinquente sessuale tra legislazione e prassi. Introduzione al focus*, in *Rivista italiana di medicina legale*, 2013, pp. 1805 ss.

G. Bombelli, *Sfera giuridica e scenari contemporanei: intorno al diritto come "rete"*, in *L'Ircocervo. Rivista elettronica di metodologia giuridica, teoria generale del diritto e dottrina dello stato*, 2011.

J. Bonta, D.A. Andrews, *Risk-Need Responsivity Model for Offender Assessment and Rehabilitation*, *Rehabilitation*, Ottawa, 2007, pp. 1 ss.

M. Caianiello, *Dangerous Liasons. Potentialities and Risks Deriving from the Interaction between Artificial Intelligence and Preventive Justice*, in *European Journal of Crime, Criminal Law and Criminal Justice* 29 (2021), n. 1, pp. 1 ss.

C. Canullo, *Chi decide? Intelligenza artificiale e trasformazioni del soggetto nella riflessione filosofica*, in E. Calzolaio (a cura di), *La decisione nel prisma dell'intelligenza artificiale*, Milano, 2020, pp. 25 ss.

G. Canzio, *Intelligenza artificiale e processo penale*, in *Cass. pen.,* 2021, n. 3, pp. 797 ss.

A. Carcano, *Automatismi: tra ragionevolezza e individualizzazione della pena*, in *Forum di Quaderni costituzionali – Rassegna*, 2021, n. 4, pp. 192 ss.

G. Carlizzi, *Errore giudiziario e logica del giudice nel processo penale*, in L. Luparia (a cura di), *L'errore giudiziario*, Milano, 2021, pp. 93 ss.

A.M. Carlson, *The Need for Trasparency in the Age of Predictive Sentencing Algorithms*, in *Iowa Law Review* 103 (2017), n. 1, p. 319.

M. Caterini, *Il giudice penale robot*, in *La legislazione penale – Rivista web*, 19 dicembre 2020 (disponibile online al seguente indirizzo: https://www.lalegislazionepenale.eu/wp-content/uploads/2020/12/Caterini-Il-giudice-penale-robot.pdf, ultimo accesso il 30 giugno 2022).

A. Chander, *The Racist algorithms*, in *Michigan Law Review* 115 (2017), n. 6, pp. 1028 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*, 2014, n. 4, pp. 619 ss.

D.J. Cooke, C. Mitchie, *Limitation of diagnostic precision and predictive utility in the individual case: a challenge for forensic practice*, in *Law and Human Behavior* 34 (2010), pp. 259 ss.

C. Costanzi, *La matematica del processo: oltre le colonne d'Ercole della giustizia penale*, in *Questione giustizia*, 2018, n. 4, pp. 166 ss.

L. D'Agostino, *Gli algoritmi predittivi per la commisurazione della pena*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2019, n. 2, pp. 354 ss.

O. Di Giovine, *Dilemmi morali e diritto penale. Istruzioni per un uso giuridico delle emozioni*, Bologna, 2022.

J. Eaglin, *Constructing recidivism risk*, in *Emory Law Journal* 67 (2017), n. 1, pp. 59 ss.

L. Eusebi, *La pena tra necessità di strategie preventive e nuovi modelli di risposta al reato*, in *Riv. it. dir. proc. pen.*, 2021, pp. 823 ss.

L. Eusebi, *La riforma ineludibile del sistema sanzionatorio penale*, in *Riv. it. dir. proc. pen.*, 2013, pp. 1307 ss.

J.L. Ferguson, *Putting the "what work" research into practice. An Organizational Perspective*, in *Criminal Justice and Behaviour* 29 (2002), n. 4, pp. 472 ss.

G. Fiandaca, E. Musco, *Diritto penale. Parte generale*, Bologna, 2019.

A. Forza, G. Menegon, R. Rumiati, *Il giudice emotivo. La decisione tra ragione ed emozione*, Bologna, 2017.

E. Fronza, C. Caruso, *Ti faresti giudicare da un algoritmo? Intervista a Antoine Garapon*, in *Questione giustizia*, 2018, n. 4, pp. 196 ss.

B. Galgani, *Considerazioni sui "precedenti" dell'imputato e del giudice al cospetto dell'IA nel processo penale*, in *Sistema penale – Rivista web*, 2020, n. 4, pp. 81 ss.

A. Garapon, J. Lassègue, *Justice digital. Révolution grafique et rupture antropologique*, Parigi, 2018.

M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Diritto penale contemporaneo – Archivio web*, 29 maggio 2019 (disponibile *online* al se-

guente indirizzo https://archiviodpc.dirittopenaleuomo.org/, ultimo accesso il 30 giugno 2022).

P. Giulini, *Il reato sessuale. Problematica, epidemiologia e principi generali di trattamento*, in P. Giulini, C.M. Xella (a cura di) *Buttare la chiave? La sfida del trattamento per gli autori di reati* sessuali, Milano, 2011.

L. Goisis, *sub* Art. 133 c.p., in E. Dolcini, G.L. Gatta, *Codice penale commentato*, Milano, 2021, pp. 2010 ss.

E. Greco, *Profili di responsabilità penale del controllore del traffico aereo. Gestione del rischio e imputazione dell'evento per colpa nei sistemi a interazione complessa*, Torino, 2021.

E. Helland, *The enforcement of pollution control Laes: inspections, violations and self-reporting*, in *The review of economics and statistics* 80 (1998), n. 1, pp. 141 ss.

D. Kahneman, O. Sibony, C. Sunstein, *Rumore. Un difetto del ragionamento umano*, Milano 2021.

R.E. Kostoris, *Predizione decisoria,* diversion *processuale e archiviazione*, in AA.VV*., Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, pp. 93 ss.

F.C. La Vattiata, *La responsabilità penale per danni da intelligenza artificiale alla prova del processo*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, Milano, 2022, pp. 695 ss.

L. Luparia Donati, *Notazioni controintuitive su intelligenza artificiale e libero convincimento*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, pp. 113 ss.

V. Manes, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, pp. 547 ss.

P. Moscarini, *La perizia psicologica e il "giusto processo*", in *Dir. pen. proc*., 2006, n. 8, pp. 929 ss.

E. Nissan, *Digital technologies and artificial intelligence's present and foreseeable impact on lawyering, judging, policing and law enforcement*, in *Artificial Intelligence & Society. Journal of Knowledge, Culture and Communication* 32 (2017), n. 3, pp. 441 ss..

T. Numerico, *Big data e algoritmi. Prospettive critiche*, Roma, 2021.

F. Palmiotto, *The Black Box on Trial: The Impact of Algorithmic Opacity on Fait Trial Rights in Criminal Proceedings*, in M. Ebers, M. Cantero Gamito (a cura di), *Algorithmic Governance and Governance of Algorithms. Legal and Ethical Challenges.* Cham, 2021, pp. 49 ss.

B. Panattoni, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio*

dall'automazione tecnologica all'autonomia artificiale, in *Il diritto dell'informazione e dell'informatica,* 2021, n. 2, pp. 317 ss.

C. Parodi, V. Sellaroli, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Diritto penale contemporaneo – Archivio web*, 29 maggio 2019.

D. Petrini, *Il trattamento del delinquente sessuale, tra esigenze securitarie e controllo della recidiva*, in *Rivista italiana di medicina legale*, 2013, pp. 1823 ss.

M. Pifferi, *L'individualizzazione della pena: difesa sociale e crisi della legalità penale tra Otto e Novecento*, Milano, 2013.

K. Popper, *Postscript to the Logic of Scientific Discovery,* London, 1982, trad. it. *Poscritto alla logica della conoscenza scientifica*, I, Milano, 1984.

S. Quattrocolo, *Sui rapporti tra pena, prevenzione del reato e prova nell'era dei modelli computazionali psico-criminologici,* in *Teoria e critica della regolazione sociale*, 2021, n. 1, pp. 257 ss.

S. Quattrocolo, *Artificial intelligence*, *Computational Modelling and Criminal Proceedings*. *A Framework for a European Legal Discussion*, Cham, 2020.

S. Quattrocolo, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *La legislazione penale – Rivista web*, 18 dicembre 2018.

M. Romano, G. Grasso, *Commentario sistematico del codice penale*, II, IV ed., Milano, 2012.

R. Rumiati, C. Bona, *Dalla testimonianza alla sentenza. Il giudizio tra mente e cervello,* Bologna, 2018.

P. Severino, *Intelligenza artificiale e diritto penale*, in U. Ruffolo, *Intelligenza artificiale*. *Il diritto, i diritti, l'etica*, Milano, 2020, pp. 531 ss.

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. process.*, 2021, n. 1, pp. 101 ss.

R. Simmons, *Quantifying criminal procedure: how to unlock the potential of Big Data in our criminal justice system*, in *Michigan State Law Review*, 2016, n. 4, pp. 947 ss.

J.P. Singh, D.G. Kroner, J.S. Wormith, S.L. Dermarais, Z. Hamilton (a cura di), *Handbook of recidivism Risk/Needs Assessment*, 2018.

F. Stella, *Giustizia e modernità. La protezione dell'innocente e la tutela delle vittime*, Milano, 2003.

A. Tversky, D. Kanheman, *Judgement under uncertainty: Heuristics and biases*, Cambridge, 1982.

G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2020, n. 4, pp.

75 ss. (ora anche in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, pp. 9 ss.)

G. Ubertis, *Sistema di procedura penale*, I, *Principi generali*, Milano, 2017.

C. Valerio, *Predicting recidivism using the Offender Screening Tool*, The University of Arizona, 2020.

M. Venturoli, *Modelli di individualizzazione della pena. L'esperienza italiana e francese nella cornice Europea*, Torino, 2020.

G. Zara, D.P. Harrington, *Criminal Recidivism: explanation, prediction and prevention*, Londra, 2016.

BIBLIOGRAFIA ESSENZIALE

AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Atti del XXXIII Convegno di studio online "Enrico De Nicola" (Milano, 15 ottobre 2020), Milano, 2021, pp. 134.

W. Barfield, U. Pagallo (eds.), *Research Handbook on the Law of Artificial Intelligence*, Cheltenham-Northampton, 2018, pp. XXVIII-702.

E. Calzolaio (a cura di), *La decisione nel prisma dell'intelligenza artificiale*, Milano, 2020, pp. 202.

A. Carleo (a cura di), *Decisione robotica*, Bologna, 2019, pp. 342.

S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020, pp. 408.

R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, Milano, 2022, pp. XXXI-1072.

J. Nieva-Fenoll, *Intelligenza artificiale e processo* (2018), Traduzione e Prefazione di Paolo Comoglio, Torino, 2019, pp. XVI-158.

S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Cham, 2020, pp. X-230.

U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, pp. XXIV-648.

A. Santosuosso, *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Milano, 2020, pp. XVI-328.

UNIVERSITÀ DI TRENTO
Facoltà di Giurisprudenza

Ciclo di Incontri
"I nuovi orizzonti del processo penale"
nell'ambito delle attività del Dipartimento d'Eccellenza

INTELLIGENZA ARTIFICIALE & PROCESSO PENALE

INDAGINI, PROVE, GIUDIZIO

Venerdì, 12 novembre 2021
Webinar (Zoom) - Ore 15.00-18.00

Presiede e introduce:

Prof.ssa Gabriella Di Paolo
Ordinario di Diritto processuale penale (Università di Trento)

Ne discutono:

Jacopo Della Torre – Ricercatore di Diritto processuale penale (Università di Trieste)
Giulia Lasagni – Ricercatrice di Diritto processuale penale (Università di Bologna)
Lucia Maldonato – Assegnista di ricerca in Diritto penale (Università Cattolica – Milano)
Luca Pressacco – Assegnista di ricerca in Diritto processuale penale (Università di Trento)

Conclusioni:

Prof.ssa Serena Quattrocolo
Ordinario di Diritto processuale penale (Università del Piemonte Orientale)

Coordinamento scientifico: Prof.ssa Gabriella Di Paolo; Dott. Luca Pressacco

Per ulteriori informazioni sul contenuto dell'evento e la registrazione, si rinvia alla pagina web:
https://webmagazine.unitn.it/evento/giurisprudenza/98113/intelligenza-artificiale-e-processo-penale

COLLANA
'QUADERNI DELLA FACOLTÀ DI GIURISPRUDENZA'

UNIVERSITÀ DEGLI STUDI DI TRENTO

1. *L'applicazione delle regole di concorrenza in Italia e nell'Unione europea. Atti del IV Convegno Antitrust tenutosi presso la Facoltà di Giurisprudenza dell'Università di Trento* - (a cura di) GIAN ANTONIO BENACCHIO, MICHELE CARPAGNANO (2014)

2. *Dallo status di cittadino ai diritti di cittadinanza* - (a cura di) FULVIO CORTESE, GIANNI SANTUCCI, ANNA SIMONATI (2014)

3. *Il riconoscimento dei diritti storici negli ordinamenti costituzionali* - (a cura di) MATTEO COSULICH, GIANCARLO ROLLA (2014)

4. *Il diritto del lavoro tra decentramento e ricentralizzazione. Il modello trentino nello spazio giuridico europeo* - (a cura di) ALBERTO MATTEI (2014)

5. *European Criminal Justice in the Post-Lisbon Area of Freedom, Security and Justice* - JOHN A.E. VERVAELE, with a prologue by Gabriele Fornasari and Daria Sartori (Eds.) (2014)

6. *I beni comuni digitali. Valorizzazione delle informazioni pubbliche in Trentino* - (a cura di) ANDREA PRADI, ANDREA ROSSATO (2014)

7. *Diplomatici in azione. Aspetti giuridici e politici della prassi diplomatica nel mondo contemporaneo* - (a cura di) STEFANO BALDI, GIUSEPPE NESI (2015)

8. *Il coordinamento dei meccanismi di stabilità finanziaria nelle Regioni a Statuto speciale* - (a cura di) ROBERTO TONIATTI, FLAVIO GUELLA (2014)

9. *Reti di libertà. Wireless Community Networks: un'analisi interdisciplinare* - (a cura di) ROBERTO CASO, FEDERICA GIOVANELLA (2015)

10. *Studies on Argumentation and Legal Philosophy. Further Steps Towards a Pluralistic Approach* - (Ed. by) MAURIZIO MANZIN, FEDERICO PUPPO, SERENA TOMASI (2015)

11. *L'eccezione nel diritto. Atti della giornata di studio (Trento, 31 ottobre 2013)* - (a cura di) SERGIO BONINI, LUCIA BUSATTA, ILARIA MARCHI (2015)

12. José Luis Guzmán D'Albora, *Elementi di filosofia giuridico-penale* - (a cura di) GABRIELE FORNASARI, ALESSANDRA MACILLO (2015)

13. *Verso nuovi rimedi amministrativi? Modelli giustiziali a confronto* - (a cura di) GIANDOMENICO FALCON, BARBARA MARCHETTI (2015)

14. *Convergences and Divergences between the Italian and the Brazilian Legal Systems* - (Ed. by) GIUSEPPE BELLANTUONO, FEDERICO PUPPO (2015) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl.handle.net/11572/116513)

15. *La persecuzione dei crimini internazionali. Una riflessione sui diversi meccanismi di risposta. Atti del XLII Seminario internazionale di studi italo-tedeschi, Merano 14-15 novembre 2014 - Die Verfolgung der internationalen Verbrechen. Eine Überlegung zu den verschiedenen Reaktionsmechanismen. Akten des XLII. Internationalen Seminars deutsch-italienischer Studien, Meran 14.-15. November 2014* - (a cura di / herausgegeben von) ROBERTO WENIN, GABRIELE FORNASARI, EMANUELA FRONZA (2015)

16. *Luigi Ferrari Bravo. Il diritto internazionale come professione* - (a cura di) GIUSEPPE NESI, PIETRO GARGIULO (2015)

17. *Pensare il diritto pubblico. Liber Amicorum per Giandomenico Falcon* - (a cura di) MAURIZIO MALO, BARBARA MARCHETTI, DARIA DE PRETIS (2015)

18. *L'applicazione delle regole di concorrenza in Italia e nell'Unione europea. Atti del V Convegno biennale Antitrust. Trento, 16-18 aprile 2015* - (a cura di) GIAN ANTONIO BENACCHIO, MICHELE CARPAGNANO (2015)

19. *From Contract to Registration. An Overview of the Transfer of Immoveable Property in Europe* - (Ed. by) ANDREA PRADI (2015) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl.handle.net/11572/140085)

20. *Diplomatici in azione. Aspetti giuridici e politici della prassi diplomatica nel mondo contemporaneo. Volume II* - (a cura di) STEFANO BALDI, GIUSEPPE NESI (2016) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl.handle.net/11572/143369)

21. *Democrazie e religioni: libertà religiosa, diversità e convivenza nell'Europa del XXI secolo. Atti del convegno nazionale Adec Trento, 22 e 23 ottobre 2015* - (a cura di) ERMINIA CAMASSA (2016)

22. *Modelli di disciplina dell'accoglienza nell'"emergenza immigrazione". La situazione dei richiedenti asilo dal diritto internazionale a quello regionale* - (a cura di) JENS WOELK, FLAVIO GUELLA, GRACY PELACANI (2016)

23. *Prendersi cura dei beni comuni per uscire dalla crisi. Nuove risorse e nuovi modelli di amministrazione* - (a cura di) MARCO BOMBARDELLI (2016)

24. *Il declino della distinzione tra diritto pubblico e diritto privato. Atti del IV Congresso nazionale SIRD. Trento, 24-26 settembre 2015* - (a cura di) GIAN ANTONIO BENACCHIO, MICHELE GRAZIADEI (2016)

25. Fiat Intabulatio*. Studi in materia di diritto tavolare con una raccolta di normativa* - (a cura di) ANDREA NICOLUSSI, GIANNI SANTUCCI (2016)

26. *Le definizioni nel diritto. Atti delle giornate di studio, 30-31 ottobre 2015* - (a cura di) FULVIO CORTESE, MARTA TOMASI (2016)

27. *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali. Atti del convegno. Trento, 2 e 3 ottobre 2015* - (a cura di) ROBERTO WENIN, GABRIELE FORNASARI (2017)

28. *Studies on Argumentation & Legal Philosophy / 2. Multimodality and Reasonableness in Judicial Rhetoric* - (Ed. by) MAURIZIO MANZIN, FEDERICO PUPPO, SERENA TOMASI (2017) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl.handle.net/11572/106571)

29. *Il Giudice di pace e la riforma della magistratura onoraria. Atti del Convegno. Trento, 3-4 dicembre 2015* - (a cura di) GABRIELE FORNASARI, ELENA MATTEVI (2017) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl. handle.net/11572/178978)

30. *Il diritto in migrazione. Studi sull'integrazione giuridica degli stranieri* - (a cura di) FULVIO CORTESE, GRACY PELACANI (2017)

31. *Diplomatici in azione. Aspetti giuridici e politici della prassi diplomatica nel mondo contemporaneo. Volume III* - (a cura di) STEFANO BALDI, GIUSEPPE NESI (2017) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl.handle.net/11572/184772)

32. *Carlo Beduschi. Scritti scelti* - (a cura di) LUCA NOGLER, GIANNI SANTUCCI (2017)

33. *Diplomatici. 33 saggi su aspetti giuridici e politici della diplomazia contemporanea* - (a cura di) STEFANO BALDI, GIUSEPPE NESI (2018)

34. *Sport e fisco* - (a cura di) ALESSANDRA MAGLIARO (2018)

35. *Legal Conversations Between Italy and Brazil* - (a cura di) GIUSEPPE BELLANTUONO, FABIANO LARA (2018)

36. *Studies on Argumentation & Legal Philosophy / 3. Multimodal Argumentation, Pluralism and Images in Law* - (Ed. by) MAURIZIO MANZIN, FEDERICO PUPPO, SERENA TOMASI (2018) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl.handle.net/11572/218719)

37. *Assetti istituzionali e prospettive applicative del* private antitrust enforcement *nell'Unione europea. Atti del VI convegno biennale antitrust. Facoltà di Giurisprudenza. Trento, 6-8 aprile 2017* - (a cura di) GIAN ANTONIO BENACCHIO, MICHELE CARPAGNANO (2018)

38. *La Direttiva quadro sulle acque (2000/60/CE) e la Direttiva alluvioni (2007/60/CE) dell'Unione europea. Attuazione e interazioni con particolare riferimento all'Italia* - (a cura di) MARIACHIARA ALBERTON, MARCO PERTILE, PAOLO TURRINI (2018)

39. *Saggi di diritto economico e commerciale cinese* - (a cura di) IGNAZIO CASTELLUCCI (2019)

40. *Giustizia riparativa. Responsabilità, partecipazione, riparazione* - (a cura di) GABRIELE FORNASARI, ELENA MATTEVI (2019) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl.handle.net/11572/234755)

41. *Prevenzione dei sinistri in area valanghiva. Attività sportive, aspetti normativo-regolamentari e gestione del rischio* - (a cura di) ALESSANDRO MELCHIONDA, STEFANIA ROSSI (2019)

42. *Pubblica amministrazione e terzo settore. Confini e potenzialità dei nuovi strumenti di collaborazione e sostegno pubblico* - (a cura di) SILVIA PELLIZZARI, ANDREA MAGLIARI (2019)

43. *Il private antitrust enforcement in Italia e nell'Unione europea: scenari applicativi e le prospettive del mercato. Atti del VII Convegno Antitrust di Trento, 11-13 aprile 2019* - (a cura di) GIAN ANTONIO BENACCHIO, MICHELE CARPAGNANO (2019)

44. *Conciliazione, mediazione e deflazione nel procedimento davanti al giudice di pace. Esperienze euroregionali. Atti del Convegno. Trento, 10 maggio 2019* - (a cura di) SILVANA DALLA BONTÀ, ELENA MATTEVI (2020) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl.handle.net/11572/259285)

45. *Diritto e genere. Temi e questioni* - (a cura di) STEFANIA SCARPONI (2020)

46. *Le parti in mediazione: strumenti e tecniche. Dall'esperienza pratica alla costruzione di un metodo* - (a cura di) SILVANA DALLA BONTÀ (2020) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl.handle.net/11572/269082)

47. *Effettività delle tutele e diritto europeo. Un percorso di ricerca per e con la formazione giudiziaria* - (a cura di) PAOLA IAMICELI (2020)

48. *Infermità mentale, imputabilità e disagio psichico in carcere. Definizioni, accertamento e risposte del sistema penale* - (a cura di) ANTONIA MENGHINI, ELENA MATTEVI (2020)

49. *Le (in)certezze del diritto. Atti delle giornate di studio. 17-18 gennaio 2019* - (a cura di) CINZIA PICIOCCHI, MARTA FASAN, CARLA MARIA REALE (2021)

50. *Studies on Argumentation & Legal Philosophy / 4. Ragioni ed emozioni nella decisione giudiziale* - (Ed. by) MAURIZIO MANZIN, FEDERICO PUPPO, SERENA TOMASI (2021) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl.handle.net/11572/296052)

51. *Comunicare, negoziare e mediare in rete. Atti del Convegno. Trento, 25 settembre 2020* - (a cura di) SILVANA DALLA BONTÀ (2021) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl.handle.net/11572/306972)

52. *La giurisdizione penale del giudice di pace: un bilancio sui primi vent'anni* - (a cura di) MARCELLO BUSETTO, GABRIELLA DI PAOLO, GABRIELE FORNASARI, ELENA MATTEVI (2021)

53. *State and Religion: Agreements, Conventions and Statutes* - (Ed. by) CINZIA PICIOCCHI, DAVIDE STRAZZARI, ROBERTO TONIATTI (2021)

54. *Pandemia e gestione responsabile del conflitto. Le alternative alla giurisdizione. Atti del Convegno. Trento, 10 giugno 2021* - (a cura di) ANTONIO CASSATELLA, SILVANA DALLA BONTÀ, ELENA MATTEVI (2021)

55. *Il rapporto tra diritto, economia e altri saperi: la rivincita del diritto. Atti della* Lectio Magistralis *di Guido Calabresi in occasione della chiusura dell'anno accademico del Dottorato in Studi Giuridici Comparati ed Europei. Facoltà di Giurisprudenza. Trento, 24 ottobre 2019* - (a cura di) GIUSEPPE BELLANTUONO, UMBERTO IZZO (2022)

56. *Il contributo di Pietro Trimarchi all'analisi economica del diritto. Atti del Convegno. Trento, 16-18 dicembre 2020* - (a cura di) GIUSEPPE BELLANTUONO, UMBERTO IZZO (2022)

57. *Le relazioni fra Autonomie speciali e Regioni ordinarie in un contesto di centralismo asimmetrico: le complessità di una dialettica (1970-2020)* - (a cura di) ROBERTO TONIATTI (2022)

58. *Giustizia e mediazione. Dati e riflessioni a margine di un progetto pilota* - (a cura di) SILVANA DALLA BONTÀ, ELENA MATTEVI (2022)

59. ANTONIO ARMELLINI - *L'Italia e la carta di Parigi della CSCE per una nuova Europa. Storia di un negoziato (luglio-novembre 1990)*. Introduzione di GIUSEPPE NESI. Postfazione di ETTORE GRECO. Con contributi di STEFANO BALDI, FABIO CRISTIANI, PIER BENEDETTO FRANCESE, NATALINO RONZITTI, PAOLO TRICHILO (2022)

60. *La rieducazione oggi. Dal dettato costituzionale alla realtà del sistema penale. Atti del Convegno. Trento, 21-22 gennaio 2022* - (a cura di) ANTONIA MENGHINI, ELENA MATTEVI (2022)

61. *La specialità nella specialità* - (a cura di) ROBERTO TONIATTI (2022)

62. *L'amministrazione condivisa* - (a cura di) GREGORIO ARENA, MARCO BOMBARDELLI (2022)

63. *Intelligenza artificiale e processo penale. Indagini, prove, giudizio* - (a cura di) GABRIELLA DI PAOLO, LUCA PRESSACCO (2022)