ELISABETTA GUIDO

Intelligenza artificiale e procedimento penale: ragionando di valutazione del rischio *de libertate**

L'articolo affronta il tema dell'impiego delle tecniche di intelligenza artificiale finalizzate alla valutazione della pericolosità sociale dell'accusato nell'ambito del giudizio cautelare. Dopo avere effettuato una classificazione degli algoritmi interessati, rilevante ai fini della verifica di compatibilità con i valori fondanti il giusto processo penale, l'indagine è rivolta alle problematiche specifiche che l'utilizzo di *output* computazionali solleva quando rapportato alle peculiarità dell'esercizio del potere cautelare.

Artificial intelligence and criminal proceedings: reasoning on de libertate risk assessment *

The essay addresses the issue of the use of artificial intelligence techniques aimed at assessing the social dangerousness of the accused in the context of pre-trial proceedings. After a classification of the algorithms involved, relevant to the verification of compatibility with the founding values of criminal due process, the analysis focuses on the specific problems that the use of computational output raises when related to the peculiarities of the exercise of the precautionary power.

1. *È (ancora) dell'uomo la virtù del pre-vedere?*[1] ...viene naturale chiederselo e non è agevole rispondere, se la domanda afferisce all'uomo che sostiene la responsabilità dello *ius dicere*. Compito arduo, affidato a un soggetto terzo e imparziale[2], nell'era dei computer digitali e delle macchine pensanti[3] diviene azione cognitiva che, al pari di altre, interroga sull'*an* e sul *quomodo* dell'utilizzo di un approccio automatizzato. I sistemi di intelligenza artificiale (IA) possono difatti informare l'esercizio del potere giurisdizionale. In particolare, ai fini dell'accertamento dei fatti di reato e dei responsabili, il loro impiego è destinato a interessare il processo penale in maniera trasversale:

* Il testo del presente contributo è destinato al volume *Automazione, diritto e responsabilità*, a cura di L. Picotti, edito da Edizioni Scientifiche Italiane, Napoli, in corso di stampa. Si ringraziano il curatore e l'editore per avere concesso la pubblicazione in questa Rivista.

[1] Il mito racconta che Zeus, dopo aver incaricato Epimeteo di distribuire a tutti i viventi delle qualità, appreso che l'uomo ne era rimasto sprovvisto poiché già tutte generosamente assegnate, si impietosì e affidò a Prometeo (fratello di Epimeteo) il compito di dare agli uomini la propria virtù: l'antiveggenza, il pre-vedere: lo ricorda GALIMBERTI, *I miti del nostro tempo*, Milano, 2009, 209.

[2] Principi, entrambi, scolpiti nell'art. 111, comma 2, Cost. rappresentano valori nucleari di ogni processo giusto: cfr. per tutti FERRUA, *Il giusto processo*, Bologna, 2012, 99 ss.

[3] I due fenomeni sono correlati, come spiega MITCHELL, *L'intelligenza artificiale. Una guida per essere umani pensanti*, Torino, 2022, 5 (trad. it.), posto che i primi sono «manipolatori di simboli», cosa che li accomunava al cervello umano, secondo i pionieri della computazione: Alan Turing e John von Neumann.

dall'attività investigativa a quella probatoria e decisionale. Nel raccogliere rapidamente tracce, cose, notizie destinate ad assumere rilevanza dimostrativa, quei sistemi rispondono a un'esigenza di efficienza del lavoro degli inquirenti, che si traduce in una riduzione dei tempi di indagine e così in una maggiore celerità della risposta alla domanda di giustizia[4]; nel fare luce su verità e falsità del racconto, le forme di IA interessate[5] mirano a "blindare" la credibilità della fonte dichiarativa[6]; nell'attribuire un certo peso alle singole prove e nell'incidere sul convincimento di colpevolezza o innocenza dell'imputato (*a fortiori*, quindi, sull'onere di motivazione), l'IA promette decisioni più oggettive, scevre da pregiudizi[7], e più certe[8].

---

[4] Emblematico il caso delle tecniche biometriche, in particolare quelle di riconoscimento facciale, gli *automatic facial recognition system* (AFRS), il cui vantaggio sta proprio nella velocità, come sottolineato da DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, in *Riv. it. dir. proc. pen.*, 2022, 1063. Più in generale, che la tecnologia rappresenti «una soluzione ai problemi del tempo (non ragionevole)» (così SPANGHER, *Processo penale e tempo*, in *Cass. Pen.*, 2022, 2475), è rilievo che l'occasione di analisi sistematica della vicenda processuale offerta dalla riforma Cartabia (l. 27 settembre 2021, n. 134, attuata con d. lgs. 10 ottobre 2022, n. 150, entrato in vigore il 30 dicembre 2022, in forza di un differimento disposto dal d.l. 31 ottobre 2022, n. 162) ha consentito di rinnovare.

[5] Si allude all'impiego delle moderne tecniche neuroscientifiche, si pensi alla risonanza magnetica funzionale (FMRI), allo scopo di "certificare" l'attendibilità della prova a fronte del graduale peggioramento delle capacità mnestiche della mente umana.

[6] Ambito ritenuto di esclusiva competenza giurisdizionale, con l'irrompere nel processo penale della prova scientifica diventa aspetto da sottoporre al vaglio dell'esperto: lo sottolinea LUPÁRIA, *Processo penale e scienza informatica: anatomia di una trasformazione epocale*, in Lupária-Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007, 129.

[7] Il problema delle insidie delle mente, dei *biases* cognitivi quale espressione fisiologica di ogni attività umana che implichi la formulazione di un giudizio e al tempo stesso fautori di errori giudiziari è tema legato alla decisione giudiziaria come frutto di intuizione ed emozioni oltre che di razionalità, su cui v. la bella analisi di FORZA- MENEGON- RUMIATI, *Il giudice emotivo. La decisione tra ragione ed emozione*, Bologna, 2017, in particolare, 141 ss.

[8] Dall'angolatura del principio di certezza del diritto, rileva l'applicazione dell'IA allo scopo di predizione del futuro esito della controversia sulla base dei precedenti giurisprudenziali. Per limitarci all'esempio della Corte d'appello di Venezia è stato sviluppato un algoritmo di analisi dei precedenti, raccolti e classificati in un *data-base* relativo alle pronunce di merito emesse nel distretto in ambito commerciale e del diritto del lavoro, al fine di rendere l'esito delle vertenze prevedibile e calcolabile. Richiama l'esperienza di analoghi progetti presso altri uffici giudiziari, PAJNO, *L'uso dell'intelligenza artificiale nel processo tra problemi nuovi e questioni antiche*, in *BioLab Journal – Rivista di Biodiritto*, 2022, 1, 219. Al riguardo, fermo il vantaggio in termini di ottimizzazione della strategia processuale, avverte sul pericolo che attraverso i precedenti si arrivi a una «vera e propria profilazione dello stesso giudice», GALGANI, *Considerazioni sui "precedenti" dell'imputato e del giudice al cospetto dell'IA nel processo penale*, in *Sist. Pen.*, 2020, 4, 88. Il tema dei *software* di intelligenza artificiale come ausilio al giudice nell'attività interpretativa è oggetto di riflessione anche da parte di CATERINI, *Il giudice penale robot*, in *www.lalegislazionepenale.eu*, 19 dicembre 2020, 12 ss., che lo analizza sotto il profilo delle

Fermo che il settore della giustizia rientra tra le materie che possono beneficiare dei vantaggi competitivi offerti dall'uso delle tecnologie, dal momento che l'IA garantisce un miglioramento delle previsioni, l'ottimizzazione delle operazioni e dell'assegnazione delle risorse e la personalizzazione delle soluzioni digitali per i singoli e per le organizzazioni[9], è però indiscusso che la pervasività di tali tecniche pone sul tappeto il problema (centrale) del rispetto dei diritti individuali e, in generale, della garanzia di un processo penale equo. Lo insegna l'esperienza statunitense[10], è oggetto di disciplina nelle fonti regolative coinvolte – specialmente la Carta etica europea[11] e, nel contesto dell'Unione, la proposta di Regolamento sull'intelligenza artificiale –, per il Consiglio di Stato, che si è pronunciato in materia, il ricorso a «procedure "robotizzate"» non può costituire «motivo di elusione dei princìpi che conformano il nostro ordinamento», nello specifico di imparzialità, pubblicità e trasparenza, tutti violati a ragione dell'impossibilità di comprendere il risultato generato dall'algoritmo[12].

---

interconnessioni con la sequenza del ragionamento inferenziale richiesto al giudice penale e con le regole di giudizio che presiedono la dichiarazione di colpevolezza.

[9] Cfr. Commissione europea, *Proposta di Regolamento che stabilisce regole armonizzate sull'intelligenza artificiale*, COM (2021) 206 final, oggetto di numerose proposte di emendamento sia in seno al Consiglio sia in seno al Parlamento Europeo. Al Consiglio, sotto la presidenza ceca, il dibattito orientativo tenutosi ha portato a diverse proposte di compromesso e la versione finale del testo di compromesso è stato sottoposto al Consiglio TTE in vista di un orientamento generale sulla proposta.

[10] Resta esemplare il caso *Loomis* (State v. Loomis, 881 NW 2d 749 [Wis 2016]) su cui v. *Criminal Law – Sentencing Guidelines – Wisconsin Supreme Court Requires Warnings before Use of Algorithmic Risk Assessment in Sentencing – State v. Loomis*, in *Harward LR*, 2017, 1530 ss. e, per la dottrina italiana, QUATTROCOLO, *Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi* vs *rischi e paure della giustizia digitale "predittiva"*, in *Cass. Pen.*, 2019, 1750 ss. La vicenda è nota per avere la Corte suprema del Wisconsin escluso una violazione del diritto al *due process*, lamentata dall'imputato per l'impossibilità di verificare l'attendibilità scientifica del *software*, poiché coperto da segreto industriale. Nell'occasione, la Corte stabilì sufficiente per la difesa la consultazione del manuale d'uso, con possibilità di confrontare i dati in ingresso con le stime finali. Ebbe altresì modo, su ricorso del prevenuto, di mettere a fuoco i limiti all'utilizzo (legittimo) dell'algoritmo predittivo, assurto a uno dei fattori suscettibili di essere presi in considerazione nella fase del *sentencing* (condanna): unitamente ad altri elementi di supporto – affermò la Corte – il *risk assessment tool* può aiutare il giudice, fornendogli il maggior numero di informazioni possibile per poter pronunciare una sentenza individualizzata.

[11] Documento della CEPEJ, Commissione europea per l'efficacia della giustizia, reperibile sul sito del Consiglio d'Europa, su cui v. 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, 1 ss.

[12] Cfr. Cons. St., Sez. VI, 8 aprile 2019, n. 2270, in *Guida dir.*, 2019, 19, 16, relativamente all'utilizzo dell'algoritmo nella formazione delle graduatorie per l'assegnazione delle sedi di servizio ai docenti della scuola secondaria di secondo grado. Pur mettendo in luce gli indiscussi vantaggi dell'automazione

L'evocata questione, a ben vedere, altro non è che la riproposizione di un conflitto (accertamento e repressione del crimine *vs* tutela dei diritti fondamentali) che sempre involge il processo penale, specie nel suo rapporto con la scienza[13]. Si prospetta, quindi, un'esigenza di bilanciamento tra le istanze della collettività, in termini di sicurezza e difesa sociale, come pure di certezza nell'applicazione della legge[14] – tutte potenzialmente meglio assicurate dall'uso delle macchine – e i diritti dei singoli che risultati governati da algoritmi possono ledere.

L'affermazione si specifica con riguardo ai modelli di IA predittivi, vale a dire *software* capaci di stimare la probabilità di commissione di reati o di ricaduta nel crimine: essi, noti come *risk assessment tools*, rappresentano l'applicazione di IA più comune nel campo della giustizia penale e sono funzionali tanto a prevenire attività illecite quanto ad offrire *output* che misurano la pericolosità sociale del soggetto. Si tratta di strumenti attecchiti nella prassi di taluni ordinamenti stranieri[15] e impiegati anche nel nostro Paese a determi-

---

del processo decisionale amministrativo, viene qui tracciata la cornice di legittimità dell'uso del processo informatico: *in primis*, l'algoritmo deve essere "conoscibile" e tale conoscibilità, per il principio di trasparenza, va riferita a tutti gli aspetti che lo riguardano, dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione (comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti). La sua "caratterizzazione multidisciplinare" – precisa il Collegio – «non esime dalla necessità che la "formula tecnica", che di fatto rappresenta l'algoritmo, sia corredata da spiegazioni che la traducano nella "regola giuridica" ad essa sottesa e che la rendano leggibile e comprensibile, sia per i cittadini che per il giudice» (§ 8.3.). Si tratta di principi ribaditi anche in Cons. St., Sez. VI, 4 febbraio 2020, n. 881, in *Riv. dir. proc.*, 2021, 710; Cons. St., Sez. VI, 13 dicembre 2019, n. 8478, in *DeJure*.

[13] Sul vasto tema della prova scientifica, è proficua la lettura dei diversi contributi raccolti nell'opera di CANZIO e LUPÁRIA DONATI (a cura di), *Prova scientifica e processo penale*, Milano, 2022.

[14] Fa notare QUATTROCOLO, *Equo Processo penale e sfide della società algoritmica*, in *Biolaw Journal – Rivista di BioDiritto*, 2019, 1, 136, come la società algoritmica non si identifichi nella società che delega le decisioni alle macchine ma in quella che «perde fiducia nella discrezionalità e nell'intuito del singolo».

[15] A titolo esemplificativo, si può menzionare il *Correctional Offender Management Profiling for Alternative Sanction* (COMPAS), algoritmo impiegato negli USA a fini valutativi del rischio di recidiva, di proprietà privata e strutturato sulle risposte a un questionario di 137 domande, su precedenti giudiziari e su dati statistici. È stato utilizzato nel caso *Loomis* (v. *supra*, n. 10). Cfr. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *https://archiviodpc.dirittopenaleuomo.org*, 29 maggio 2019, 5 ss. e MALDONATO, *Algoritmi predittivi e discrezionalità del giudice: una nuova sfida per la giustizia penale*, in *Dir. pen. cont.*, 2019, 2, 403 ss.

ni scopi, in particolare nell'ambito dell'attività di prevenzione, quando del reato c'è solo il sospetto[16].

Diverso è il campo della valutazione del rischio di recidiva nell'ambito del procedimento penale, che prende avvio una volta acquisita la notizia di reato ed è assistito dalle garanzie costituzionali e sovranazionali del *fair trial*. Il giudice è chiamato ad effettuare questo tipo di apprezzamento in diverse articolazioni dell'*iter* accertativo: la prognosi – positiva – di "recidiva" (art. 274, comma 1, lett. *c* c.p.p.) legittima, sussistenti i gravi indizi di colpevolezza (art. 273 c.p.p.), l'applicazione di misure cautelari personali come pure, sul presupposto del *fumus commissi delicti*, quella provvisoria di misure di sicurezza (art. 206 c.p. e art. 312 c.p.p.); in sede di irrogazione della pena in sentenza, incide sulla relativa quantificazione (art. 133, comma 2, c.p.). Arrivati a sentenza definitiva di condanna, in fase esecutiva detto esame veicola la possibilità di beneficiare delle misure alternative al carcere[17].

L'obiettivo del presente contributo è riflettere su quanto l'utilizzo di sistemi di IA per la valutazione della pericolosità nel giudizio cautelare – che si effettua sulla base di una prognosi allo stato degli atti – possa dirsi compatibile con la presunzione di non colpevolezza (art. 27, comma 2, Cost.), presidio delle restrizioni della libertà personale durante la ricostruzione dei fatti e l'accertamento delle responsabilità individuali (art. 13, comma 2, Cost.) e canone di individualizzazione del trattamento interinale[18]. Vale la pena di preci-

[16] In tale ambito vengono utilizzati *software* sia *placed-based system*, funzionali cioè a predire i luoghi di futura commissione di reati, sia *person-based system*, volti alla profilazione del possibile autore del reato: il programma *Keycrime*, sviluppato dalla questura di Milano, serve proprio a ricostruire un determinato modello delittuoso, quindi funziona per i reati seriali e non occasionali, sulla base di dati raccolti e classificati, tanto di tipo oggettivo che soggettivo, da cui è possibile trarre previsioni su luogo e ora di eventuali ulteriori reati. Sull'argomento, v. PADUA, *Intelligenza artificiale e giudizio penale: scenari, limiti e prospettive*, in *Proc. pen. giust.*, 2021, 1491 s.

[17] Secondo la ricostruzione operata da QUATTROCOLO, *Artificial intelligence, Computazional Modelling and Criminal Proceedings. A framework for A European Legal Discussion*, Springer, 2020, 132 ss., il *risk assessment* nei procedimenti penali afferisce a due principali aree: una è quella delle misure restrittive per esigenze cautelari (*pre-trial detention*), che si colloca nella fase iniziale del procedimento, l'altra riguarda la condanna (*sentencing*), quindi il momento finale.

[18] Cfr. Corte cost., 21 luglio 2010, n. 265, in *Giur. cost.*, 2010, 3183, in cui, premesso che le restrizioni della libertà personale dell'imputato (e indagato) nel corso del procedimento sono compatibili con la presunzione d'innocenza se assumono connotati che le differenziano dalla pena (irrogabile solo dopo l'accertamento definitivo della responsabilità), la Corte ribadisce che il legislatore ordinario è tenuto, «nella tipizzazione dei casi e dei modi di privazione della libertà, ad individuare [...] esigenze diverse da quelle di anticipazione della pena», che debbano essere soddisfatte durante il corso del procedimento, «tali da giustificare, nel bilanciamento di interessi meritevoli di tutela, il temporaneo sacrificio della

sare che c'è nel sistema un problema di compatibilità laddove venga in gioco il rischio non propriamente cautelare ma di recidiva[19]. È tale fattispecie di pericolo[20] che ha posto il dubbio a fronte dell'art. 27, comma 2, Cost., perciò una volta non espunta si ammette che il giudice faccia uso di tutti i mezzi possibili per valutarne la sussistenza. Si tratta allora di capire se le metodiche di IA, di per sé non precluse, accentuino la problematica messa in evidenza, a fronte di algoritmi da cui emerga una valutazione generalizzata.

Anche la cornice definita dal diritto di difesa (art. 24, comma 2, Cost.), dal contraddittorio e dalla parità delle armi (art. 111, comma 2, Cost.) concorre a determinare le coordinate valoriali entro cui è possibile automatizzare l'apprezzamento in questione.

Il settore delle misure cautelari, infatti, è certamente coinvolto nel discorso sulla "giustizia predittiva"[21], dato che si tratta di precauzioni adottate dal giudice sulla base di una valutazione prognostica allo stato degli atti che si vorrebbe rendere performante proprio grazie all'utilizzo di *automated evidence*[22]. L'analisi terrà conto, in particolare e come già intuibile, della complessa prognosi di recidivanza[23] contemplata nella norma processuale di riferimento (art. 274, comma 1, lett. *c* c.p.p.).

---

libertà personale di chi non è stato ancora giudicato colpevole in via definitiva». Tale pronuncia è richiamata da GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, cit., 21.

[19] «L'intervento cautelare diventa misura di sicurezza», scriveva CORDERO, *Procedura penale*, Milano, 1998, 467, che aggiungeva «Metamorfosi poco felice: la tutela degli interessi collettivi esige rimedi ad hoc; gli ibridi costano più di quanto rendano».

[20] Che, secondo GREVI, *Libertà personale dell'imputato e Costituzione*, Milano, 1976, 48, finiva per rendere l'intero sistema delle misure restrittive della libertà personale dell'imputato una reazione «in funzione di autotutela proiettata verso il futuro».

[21] Al suo interno rientrano, come è emerso nel testo e per sintetizzare, sia *software* di *predictive policing*, che servono a preconizzare il luogo di commissione di reati sia applicativi, ad uso del procedimento penale, che hanno il fine di effettuare predizioni su futuri comportamenti del prevenuto. Ma l'espressione vale a comprendere anche l'impiego dell'algoritmo per predire il futuro esito della causa, futuribile preoccupante se non finalizzato a orientare la scelta dell'interessato o a fornire un suggerimento al giudice ma al «preconfezionamento» della pronuncia: v. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Dir. pen. cont.*, 2020, 4, 83.

[22] In ordine allo specifico tema del dato conoscitivo generato attraverso l'algoritmo e delle problematiche derivanti dal relativo impiego nel processo penale, cfr., tra gli altri, QUATTROCOLO, *Equità del processo penale e* automated evidence *alla luce della Convenzione europea dei diritti dell'uomo*, in *Rev. Italo-Española Derecho Procesal*, 2019, 1, 107 ss.; CANZIO, *Intelligenza artificiale e processo penale*, in *Prova scientifica e processo penale*, cit., 903 ss.

[23] Simile rischio – lo si vuole qui ricordare – è l'unico preso in considerazione nel procedimento penale a carico dell'ente incolpato dell'illecito amministrativo dipendente da reato. L'applicazione alla *societas*

2. Questione di algoritmo. Prima di esaminare le problematiche sottese al tema dell'accertamento algoritmico della pericolosità dell'accusato, occorre partire dall'assunto in base al quale, se è l'algoritmo a conferire «l'"anima" all'A.I.»[24], non tutti gli algoritmi sono uguali[25]. La definizione di intelligenza artificiale adottata nella proposta di Regolamento europeo in materia prova tale asserzione. È difatti formulata in senso ampio e inclusivo: comprende l'uso di algoritmi deterministici, non deterministici o di apprendimento automatico[26]. Questa classificazione si correla con una differenziazione che attinge il versante della *prevedibilità* del risultato (per il quale l'algoritmo è stato programmato), della *comprensibilità* del sistema (intesa quale peculiarità del medesimo di essere compreso nel suo funzionamento da un essere umano), della *spiegabilità* della decisione (cioè, della capacità del sistema di giustificare il processo decisionale che ha prodotto un determinato *output*)[27]. Al confron-

---

di misure cautelari – speculari per tipologia alle sanzioni interdittive irrogabili in sede di condanna – oltre al presupposto tipico dei gravi indizi richiede infatti il pericolo specifico che apicali o dipendenti commettano, nell'interesse o a vantaggio dell'ente medesimo, ulteriori reati della stessa indole di quelli per cui si procede (art. 45 d. lgs. 8 giugno 2001, n. 231). Lo stato dell'organizzazione aziendale riveste un ruolo centrale nella valutazione cautelare (cfr. Cass., Sez. VI, 25 gennaio 2010, n. 20560, in *Guida dir.*, 2010, 28, 86), posto che il giudice della cautela dovrà valutare l'efficacia preventiva del modello di organizzazione e di gestione che l'ente abbia adottato *ante factum* o *ex post*, cioè a misura applicata e in prospettiva della sospensione o della revoca. Tale delibazione implica un giudizio di idoneità e di efficace attuazione del modello, indicatori questi su cui già impattano i *software* di IA. Sul tema, che cade sotto l'etichetta di *digital criminal compliance*, senz'altro meritevole di un'analisi più compiuta, v. MOZZARELLI, *Digital Compliance: The Case for Algorithmic Transparency*, in Manacorda-Centonze, *Corporate Compliance on a Global Scale*, Springer, 2022, 259 ss.

[24] RUFFOLO, *Le responsabilità da* artificial intelligence, *algoritmo e* smart product*: per i fondamenti di un diritto dell'intelligenza artificiale self-learning*, in Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, 97.

[25] Cfr., al riguardo, la chiara analisi di PERUZZI, *Intelligenza artificiale e tecniche di tutela*, in *Dir. e lav.*, 2022, 3, 542 ss., i cui sviluppi sono presi a riferimento nell'analisi qui portata avanti.

[26] Cfr. la *Proposta di Regolamento del parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale)*, Orientamento generale, *considerando* 6, 6-*bis*, 6-*ter*, in *https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/it/pdf*.

[27] Mentre gli algoritmi deterministici si fondano sulla logica e approdano a una certa conclusione in forza di una sequenza inferenziale per cui, accettato in *input* un numero di informazioni, l'*output* fornito è uno solo – il processo decisionale da essi regolato può quindi dirsi prevedibile *ex ante*, comprensibile e spiegabile –, gli algoritmi non deterministici seguono un approccio statistico/probabilistico per cui il processo decisionale non è a priori prevedibile: tuttavia, poiché i passaggi di cui si compone il processo in questione sono tracciabili e ricostruibili *ex post*, anche detti sistemi godono di un certo grado di *transparency by design*.

to di questi parametri, sono gli algoritmi di apprendimento automatico a sollevare le questioni più spinose.
Il modello che governa il processo decisionale non è qui definito da regole predeterminate in fase di programmazione dell'algoritmo ma è il prodotto di un metodo di apprendimento consegnato alla macchina dall'algoritmo addestratore. Questo approccio di IA, che prende il nome di *machine learning*, è basato su reti neurali artificiali che apprendono tramite esposizione a grandissime quantità di dati e durante tale fase di addestramento – così è chiamata l'esposizione alle informazioni da cui si deve apprendere (*training data*) – il sistema algoritmico impara la regola che andrà poi a guidare la procedura di determinazione dell'*output*[28]. Più profondo è l'apprendimento, vale a dire più strati di reti neurali artificiali ci sono, maggiore è l'opacità algoritmica, il cosiddetto effetto *black-box*, ritenuto cozzare contro il principio di trasparenza del funzionamento dell'algoritmo predittivo[29], presupposto fondamentale perché l'imputato possa esercitare il proprio diritto di difesa sottoponendo a sindacato l'*an* e il *quomodo* della previsione generata come risposta dal sistema di apprendimento. La delicatezza di tale approccio, all'evidenza, sta nel fatto di trovarsi al di fuori della dimensione di mera automazione, dove il sistema opera nella cornice di regole codificate e predefinite, e più vicini al concetto di autonomia: cognitiva e valutativa.
Sarebbe, tuttavia, un errore ignorare che l'apprendimento automatico costituisce un sottocampo dell'IA che presenta varie articolazioni. Esistono diversi tipi di apprendimento: supervisionato, non supervisionato e per rinforzo[30] e,

[28] L'apprendimento rappresenta il passo successivo rispetto alla memoria e alla capacità di calcolo, principali punti di forza dei computer digitali: cfr., sul tema, TEGMARK, *Vita 3.0. Esseri umani nell'era dell'intelligenza artificiale*, Milano, 2018, 101-112.
[29] Un principio che non è garantito dal solo accesso al codice sorgente (cfr. LUPÀRIA DONATI- FIORELLI, *Diritto probatorio e giudizi criminali ai tempi dell'Intelligenza Artificiale*, in *Dir. pen. cont.*, 2022, 2, 43). Nei sistemi di apprendimento automatico, l'uomo non fornisce alla macchina tutta la conoscenza ma un metodo di apprendimento in base al quale è la macchina a estrarre dai dati di cui è in possesso le indicazioni per svolgere un determinato compito. Quest'ultimo – può trattasi di una previsione, classificazione o azione – è svolto dall'«algoritmo addestrato», mentre è l'«algoritmo addestratore» a essere scritto in linguaggio di programmazione intellegibile.
[30] Cfr. sul tema SARTOR e LAGIOIA, *Le decisioni algoritmiche tra etica e diritto*, in Ruffolo (a cura di), *Intelligenza artificiale*, cit., 69 ss. Sull'addestramento delle reti neurali, secondo una procedura così scansionata – «insieme di addestramento», formato da una serie di dati (es. immagini di un oggetto), cartella o file di etichettatura, impostazione dei pesi della rete, introduzione dell'immagine come *input*, calcolo strato per strato e invio della «percentuale di confidenza» – v. MITCHELL, *L'intelligenza artificiale*, cit., 71.

sotto il profilo dell'opacità, l'approccio più critico è il *deep learning*. L'espressione indica l'addestramento delle *deep neural networks*, cioè reti neurali con più di uno strato nascosto compreso tra l'*input* e l'*output*. Più alto è il numero di strati nascosti più profonda sarà la rete neurale. Se per questa tecnica si può rilevare un difetto di spiegabilità delle decisioni prodotte dal sistema e, per riflesso, di contestabilità delle medesime[31], rispetto al modello di apprendimento con supervisione – il più utilizzato – un certo grado di trasparenza è possibile, almeno per il soggetto esperto[32].
Un tanto ci permette di osservare che il rapporto tra IA e giustizia penale deve misurarsi con la regolazione e l'architettura delle reti neurali, poiché aspetti che caratterizzano l'addestramento e influiscono sulla prestazione finale. Ed è evidente che solo conoscendo il funzionamento di un determinato algoritmo sarà possibile, per le parti, controllare il risultato prodotto e contestarne la validità; per il giudice, valutare la sua idoneità all'accertamento del fatto di reato e riuscire, *ex post*, a motivare la decisione presa sulla base dell'IA[33].

3. IA e rischio di recidiva. La sintetica rassegna sui diversi sistemi di IA ci permette di rilevare, a proposito dei *tools* di valutazione della pericolosità sociale, come per essi possano valere le medesime problematiche note ad altre applicazioni di IA. In quanto strumenti a matrice statistico-probabilistica non sono immuni da fallibilità: possono infatti fornire risultati poco efficaci, anche a motivo di *biases* cognitivi causati da dati immessi in *input* nella macchina di

[31] Carenza per la verità superabile attraverso le tecniche *Explainable* AI (XAI) che rispondono alla necessità di spiegare le decisioni del modello al di là delle prestazioni di predizione: cfr., sul tema, ARRAS-OSMAN- SAMEK, *CLEVR-XAI: A benchmark dataset for the ground truth evaluation of neural network explanations*, in *Information fusion*, 2022, 81, 14-40; ARRIETA- DÍAZ-RODRÍGUEZ- DEL SER-BENNETOT- TABIK- BARBADO- GARCIA- GIL LOPEZ- MOLINA- BENJAMINS- CHATILA- HERRERA, *Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI*, in *Information fusion*, 2020, 58, 82-115.
[32] Lo segnala PERUZZI, *Intelligenza artificiale e tecniche di tutela*, cit., 545.
[33] In letteratura si è utilizzata l'espressione *algorithmic due process* (ISRANI-CHANG, *Algorithmic due process: Mistaken Accountability and Attribution in* State v. Loomis, in *www.jolt.law.harvard.eu*, 31 agosto 2017) quasi a significare la sfida della futura procedura penale, chiamata a costruire garanzie tarate sul funzionamento dell'IA, che attengono alla formazione dei *database*, alla qualità dei dati, alla trasparenza dei *software* utilizzati e alle tecniche di addestramento sì da evitare la creazione di effetti discriminatori, alla necessità di un effettivo controllo umano sui risultati della macchina. Per tali considerazioni, rispetto ai riconoscimenti facciali, DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., 1092.

scarsa qualità, e, considerato l'approccio del *deep learning*, risultare oscuri nel loro funzionamento.

Queste criticità di fondo sembrano amplificarsi quando rapportate alle peculiarità dell'esercizio del potere cautelare, i cui pilastri, com'è noto, sono rappresentati dalla valutazione di gravità indiziaria (art. 273 c.p.p.) e del *periculum* da arginare nel caso concreto (art. 274, comma 1, c.p.p.): di inquinamento probatorio (lett. *a*), di fuga (lett. *b*) e di reiterazione del reato (lett. *c*). Una valutazione che, in ogni caso, deve essere improntata ad accuratezza e responsabilità, invito che discende dal rafforzamento del ruolo di garante del giudice cui è richiesta una «autonoma valutazione» dei presupposti applicativi (art. 292, comma 2, lett. *c* c.p.p.), come pure dei «motivi per i quali sono stati ritenuti non rilevanti gli elementi forniti dalla difesa» e altresì «delle concrete e specifiche ragioni» ostative per l'applicazione di misure restrittive diverse dalla custodia cautelare in carcere (art. 292, comma 2, lett. *c-bis* c.p.p.). Così prefigurato il ragionamento probatorio interinale, riflesso della finalità di contenimento che si è voluta affidare alla valutazione delle esigenze cautelari[34], è rispetto a tale archetipo motivazionale che sarà necessario verificare il risultato di probabilità che un determinato pericolo si verifichi offerto dalla computazione.

La pericolosità sociale dell'imputato certamente rappresenta, dei tre contemplati nel sistema cautelare codicistico (sopra richiamati), il pericolo da evitare divenuto egemonico nella prassi. Ma è anche l'area su cui si può immaginare che i sistemi di IA avranno il maggiore impatto: lo scopo di prevenzione speciale che identifica il finalismo cautelare in questione accosta la cautela alla sanzione e, su tale ultimo versante, è già stato sperimentato l'impiego di processi computazionali per la prognosi di futuri comportamenti delittuosi da parte dell'imputato[35]. Inoltre, l'accennato parallelismo – fermo il divieto di assimilazione della coercizione processuale alla coercizione propria del diritto penale ai sensi dell'art. 27, comma 2, Cost. – costituisce un dato di realtà normativa. L'art. 133, comma 2, c.p. elenca tra i criteri di commisurazione della pena, sintomatici della capacità a delinquere, elementi che l'art. 274,

[34] Circa l'aspetto della funzionalità del vaglio sul *periculum* alla riduzione dell'applicabilità delle restrizioni provvisorie, cfr. PRESUTTI, *Le cautele nel processo penale come forma di anticipazione della pena*, in *Riv. dir. proc.*, 2014, 45.

[35] Si allude, guardando all'ordinamento statunitense, al rilievo sempre maggiore che la valutazione algoritmica del rischio ha assunto nella fase del *sentencing*. V., in argomento, D'AGOSTINO, *Gli algoritmi predittivi per la commisurazione della pena*, in *Dir. pen. cont.*, 2019, 2, 360 ss.

comma 1, lett. *c* c.p.p. replica, *in nuce*, per la valutazione di sussistenza del pericolo di commissione di altri reati: modalità e circostanze del fatto e personalità del reo[36].

Ciò per dire che i *risk assessment tools*, una volta ammessi nel procedimento penale, sarebbero spendibili in sede di condanna come pure per l'applicazione di misure restrittive della libertà personale ad accertamento in corso dei fatti. La peculiarità del settore cautelare, tuttavia, fa affiorare due problematiche. L'una, più generale, attiene alla individuazione della categoria giuridica atta a qualificare l'*output* generato dal processo algoritmico. La discussione in dottrina è aperta, con la certezza che se si trattasse di perizia psicologica e criminologica, il discorso sull'ammissibilità dei *software* di *risk assessment* finirebbe sul nascere, stante il divieto stabilito nell'art. 220, comma 2, c.p.p. di suo utilizzo nel giudizio di cognizione[37]. Si preferisce, quindi, propendere per l'opzione interpretativa secondo cui il dato generato dall'IA debba essere trattato alla stregua di un mero indizio[38]: una sorta di indicazione che considerata nell'insieme degli elementi apprezzabili dal giudice – oltre alle specifiche modalità e circostanze del fatto, «comportamenti o atti concreti» del soggetto imputato o indagato oppure i «suoi precedenti penali» – consenta di trarre conclusioni più sicure sul futuro comportamento dell'accusato.

L'altra, connessa, questione riguarda il rapporto tra il dato algoritmico (indizio) e la motivazione dell'ordinanza cautelare. Assodato che la stima di pericolosità cui approda il processo computazionale sia uno degli elementi probatori alla base del *decision making*, di per sé quindi priva di valore determinante per la positiva prognosi di recidiva, la domanda è la seguente: sotto quale profilo il risultato automatizzato può essere impiegato? Su quale "tema di prova" può incidere? Il giudice – lo stabilisce la lett. *c* dell'art. 274 c.p.p. nella

[36] Per tale rilievo, v. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., 19.

[37] Per M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., 20, i *risk assessment tools* «non [sono] finalizzati specificamente a scandagliare il foro interiore dell'interessato»: ad escludere l'applicabilità dell'art. 220, comma 2, c.p.p. l'inconferenza del risultato digitale ad accertare il carattere e la personalità dell'imputato e, in genere, le sue qualità psichiche indipendenti da cause patologiche. Diversamente, secondo QUATTROCOLO, *Quesiti nuovi e soluzioni antiche?*, cit., 1762, «pare assodato che sia i sistemi attuariali, sia, a maggior ragione, quelli strutturati professionali, rappresentino una valutazione tecnico-scientifica assimilabile alla perizia, trasfondendo in un procedimento algoritmico e/o digitale, i principi, gli assiomi, le teorie della scienza psicologica, purché validate dal sostegno della comunità scientifica».

[38] Cfr. MAUGERI, *L'uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra* evidence based practices *e tutela dei diritti fondamentali*, in *questa Rivista*, 2021, 1, 32.

versione riformata nel 2015 – applica una misura cautelare se il pericolo di reiterazione del reato, oltre che «concreto», è «attuale»[39]. Non è agevole seguire la giurisprudenza nel suo ruolo di interprete di tali caratterizzazioni. All'opzione secondo cui, in forza del requisito dell'attualità, la prognosi di recidiva dovrà avvenire sulla base del seguente schema logico: dato per certo o per altamente probabile che l'occasione del delitto si presenterà, con altrettanta certezza o elevato grado di probabilità l'imputato ricadrà nel reato[40], si contrappone quella che sgrava il giudice della verifica di specifiche occasioni di recidivanza[41].

Vero è che, al di là degli sforzi esegetici volti a significare il concetto di pericolo attuale, esiste un perno attorno a cui ruota il vaglio necessario a ravvisare la sussistenza dell'esigenza cautelare *de quo*, e cioè la fattispecie concreta. È la condotta, per come si è manifestata, a farsi rivelatrice anche della personalità dell'accusato; non basta la proclività a delinquere per giudicare positivo il rischio di ricaduta nel reato. Ma se così è, se il fulcro della valutazione restano principalmente le modalità e le circostanze del fatto[42], la funzione di ausilio che il tasso di probabilità risultato dal calcolo algoritmico potrebbe ricoprire rispetto al caso di specie non può che tradursi in una conferma, per il giudice, di effettività del pericolo. La *vis* criminale dell'imputato, già ritenuta dimostrata dall'apprezzamento umano generale del fatto di reato, finirebbe per essere elemento irrobustito perché "validato" dallo strumento informatico "intelligente", che così corrobora la previsione umana. È difficile ipotizzare che il giudice abbia motivo di discostarsi da tale prova, peraltro in assenza di ele-

[39] Questa duplice caratterizzazione è da riferire alla l. 16 aprile 2015, n. 47, che ha appunto aggiunto il requisito della attualità, da tenere distinto da quello della concretezza, rotante attorno alla capacità a delinquere dell'imputato, al dichiarato fine di «rafforzare l'esigenza di una valutazione più stringente dell'effettiva pericolosità del prevenuto» (così, la *Relazione di presentazione*, in *Atti Camera – XVII Legislatura – Documenti, C. 631*).

[40] È l'interpretazione accolta da Cass., Sez. un., 28 aprile 2016, n. 20769, Lovisi, in *Guida dir.*, 2016, 24, 51, per cui il concetto di attualità implica per il giudice un accertamento circa la sussistenza di occasioni prossime al reato. Tra le sezioni semplici cfr., *ex multis*, Cass., Sez. VI, 27 ottobre 2016, n. 10516, in *Cass. Pen.*, 2019, 1934, con nota critica di GIULIANI, *Sull'attualità del pericolo di reiterazione del reato.*

[41] Cfr. Cass., Sez. IV, 7 luglio 2022, n. 38044; Cass., Sez. I, 11 febbraio 2022, n. 22753; Cass., Sez. II, 24 novembre 2020, n. 5054; Cass., Sez. IV, 19 giugno 2020, n. 19881.

[42] Cfr. CESARIS, sub *art. 274*, in ILLUMINATI- GIULIANI (a cura di), *Commentario breve al codice di procedura penale*, Milano, 2020, 1187.

menti concreti addotti dalla difesa che, com'è noto, non partecipa nella fase applicativa della misura[43].

Sono conosciute le critiche circa l'utilizzo dell'*output* del processo computazionale nei provvedimenti giudiziari, dovute essenzialmente al difetto di trasparenza dell'algoritmo, e di qui a cascata il *vulnus* per i diritti della difesa, che non sarebbe nelle condizioni di contestare la dosimetria effettuata dal *tool* digitale. Ma è come esso impatta sul diritto alla libertà personale a interrogare sull'opportunità di queste tecnologie nella fase interinale. Il provvedimento cautelare deve contenere una motivazione che attesti l'effettività del pericolo da evitare e quindi anche la spiegazione del perché la macchina abbia sortito una determinata stima di rischio. Ciò discende dallo stringente accertamento che la disciplina codicistica esige per attivare lo strumento coercitivo: al giudice è richiesto un giudizio provvisorio ancorato al caso concreto. La disponibilità di valutazioni algoritmiche fondate su generalizzazioni[44], al di là della preoccupazione circa una possibile deviazione del sistema penale che passerebbe dal diritto penale del fatto al diritto penale del profilo d'autore[45], in opposizione al principio di legalità (art. 25, comma 2, Cost.), potrebbe dare la stura ad uno svuotamento dell'obbligo di motivazione sul *periculum* che rischia di tradursi in una trappola per l'interessato, privato del bene costituzionale della libertà fisica e con armi difensive spuntate non potendo contare su un effettivo diritto di impugnazione (artt. 309 e 311 c.p.p.) né sull'attivazione degli istituti di revoca o sostituzione della misura (art. 299 c.p.p.).

---

[43] Si è soliti parlare, proprio per l'assenza del contraddittorio che caratterizza il momento genetico della misura restrittiva, di dimensione probatoria unidimensionale: v. GIOSTRA, *Il giudice per le indagini preliminari e le garanzie della libertà personale*, in *Riv. it. dir. proc. pen.*, 1994, 1261.

[44] Premesso che l'insieme di addestramento della rete neurale consiste di dati personali, per quel che attiene la previsione della *vis* criminale «presuppone informazioni sul reo, ma anche sui comportamenti di altre persone condannate in passato». Così SARTOR e LAGIOIA, *Le decisioni algoritmiche tra etica e diritto*, cit., 73. V. anche D'AGOSTINO, *Gli algoritmi predittivi per la commisurazione della pena*, cit., 367, per il quale il punteggio di rischio «calcolato incrociando i dati relativi a situazioni simili o vicende analoghe» fa cadere il giudizio sulla recidiva «in un labirinto di inevitabili generalizzazioni empiriche». Cfr. in relazione alla configurazione dell'algoritmo Compas, strutturato, tra l'altro, su precedenti giudiziari, dati statistici e risposte a un questionario, SIGNORATO, *Giustizia penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo*, in *Riv. dir. proc.*, 2020, 611 ss.

[45] Cfr. MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in Ruffolo (a cura di), *Intelligenza artificiale*, cit., 559; GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., 21.

4. Osservazioni conclusive. Ai rischi, che contornano il discusso settore dell'IA predittiva, si accompagnano i vantaggi connessi a queste tecnologie digitali. Che si riassumono in un interrogativo di fondo. Posta la domanda su quali siano le prime associazioni mentali rispetto al sistema di amministrazione della giustizia nel proprio paese, Max Tegmark rilancia, chiedendosi se non sarebbe meraviglioso che anziché i lunghi ritardi, i costi elevati e le condanne ingiuste, «i primi pensieri fossero "efficienza" ed "equità"»[46].

Si tratta della sfida che lo stato attuale dell'evoluzione tecnologica consegna alla fruttuosa collaborazione uomo-macchina, considerata come un argine agli errori umani di cui i sistemi giudiziari sono costellati[47]. Le sentenze possono difatti essere influenzate da pregiudizi di varia natura, dalle inclinazioni umane[48], dalla carenza di conoscenze tecniche aggiornate: difetti tutti che verrebbero azzerati grazie ai robogiudici. Prospettiva, quest'ultima, avvertita come preoccupante in dottrina, a ragione se si pensa che il processo penale ha peculiarità tali, sul versante dell'accertamento e della valutazione, che occorre «uno scavo ermeneutico e ricostruttivo» che solo un giudice in persona può operare[49].

L'errore, peraltro, non riguarda solamente il giudicato, come la sua accezione tecnica vorrebbe. Può colpire anche la fase della restrizione cautelare, con effetti gravi, tanto per la lesione immediata della libertà personale che l'accusato subisce quanto per l'eventuale riverbero sulla fase di merito[50].

Ecco che, non senza timore di riprendere rilievi già sollevati in letteratura, l'ammissibilità dei *risk assessment tools* nel nostro processo penale, che pure non incontra ostacoli dovuti alla presunzione di non colpevolezza (perché

[46] TEGMARK, *Vita 3.0. Esseri umani nell'era dell'intelligenza artificiale*, cit., 143.

[47] Sulle cause, per un inquadramento generale, v. CANZIO, *Alle radici dell'errore giudiziario: "heuristics and biases"*, in Lupária Donati (a cura di), *L'errore giudiziario*, Milano, 2021, 81 ss.

[48] Le neuroscienze hanno dimostrato che le emozioni, gli impulsi, i pregiudizi incidono sulla decisione che, quindi, può risultare affetta da errore non tanto per una inesatta applicazione della legge ma per un ragionamento distorto da paraocchi della mente. Cfr. FORZA- MENEGON- RUMIATI, *Il giudice emotivo. La decisione tra ragione ed emozione*, cit., *passim*.

[49] Così GALGANI, *Giudizio penale*, habeas data *e garanzie fondamentali*, in *questa Rivista*, 2019, 1, 23.

[50] Il fatto che le medesime circostanze storiche siano fatte oggetto di un doppio apprezzamento, ai fini della gravità indiziaria e della valutazione del *periculum*, comporta il rischio che l'errore sul primo presupposto si rifletta sul secondo creando una sorta di circolarità nell'errore. Certamente, poi, l'ordinanza applicativa della misura cautelare può influire sulla motivazione della sentenza col rischio che l'errore commesso nell'incidente cautelare si traduca in un errore giudiziario: cfr. CENTORAME, *L'errore giudiziario in fase cautelare*, in Lupária Donati (a cura di), *L'errore giudiziario*, cit., in particolare, 389 e 395 ss.

non è l'uso in sé dell'IA a far emergere un contrasto con tale principio ma l'uso collegato alla fattispecie di pericolosità, là dove il metodo utilizzato impedisce al giudice di addivenire a una valutazione individualizzata), deve ritenersi vincolata: non solo dal rispetto dei canoni di legalità ed equità che connotano l'andamento generale del processo penale (art. 111, commi 1 e 3, Cost.) ma dall'idoneità di quei *software* a non pregiudicare oltremodo i diritti fondamentali dell'individuo, l'inviolabilità della libertà personale (art. 13 Cost.) nel caso che ci occupa.

Sul versante generale dell'equità processuale, nella declinazione della parità delle armi, è evidente che le decisioni frutto di un processo computazionale debbano poter essere permeabili a un controllo *ex post*. L'algoritmo potrà anche essere utilizzato a supporto della decisione giudiziale ma non renderà quella decisione necessariamente più solida e più affidabile. Perché si arrivi a questo obiettivo, ed è il senso della struttura dialettica del *fair trial*, occorrono materiali probatori decifrabili per le parti e spiegabili per il giudice. Su tale versante, in caso di apprendimento automatico, operano tecniche informatiche specifiche[51] ma è tutta da stabilire la sostenibilità economica di un simile rimedio[52].

Sotto il profilo particolare della libertà personale, sono ammesse sue compressioni nel corso del procedimento penale ma solo a fronte di determinati pericoli, che la legge processuale descrive in maniera tassativa, data la salvaguardia della presunzione di non colpevolezza dell'imputato. Ciò significa che allorquando il nostro ordinamento decidesse di dotarsi di sistemi di IA per la valutazione della pericolosità dovrebbe anzitutto porsi un problema di proporzionalità e precisare casi e modi di utilizzo dei *tools* predittivi per ossequio al disposto dell'art. 13, comma 2, Cost.

L'ingresso di "prove algoritmiche" quando si tratti di decidere se limitare o meno la libertà personale dell'accusato deve tradursi in un vantaggio per l'intera collettività, quindi per la sicurezza dei cittadini, senza che ciò provochi compressioni ingiustificate del bene individuale costituzionalmente garantito. In questa prospettiva, il punteggio di pericolo che la macchina effettua e di cui

[51] Si allude alle tecniche XAI, v. *supra*, n. 31.

[52] Torna utile riprendere le riflessioni di QUATTROCOLO, *Equità del processo penale e* automated evidence *alla luce della Convenzione europea dei diritti dell'uomo*, cit., 118, a proposito dello squilibrio conoscitivo che il sapere scientifico ha introdotto nel processo penale, a danno della parte privata i cui mezzi sono limitati rispetto a quella pubblica e, con la prova algoritmica, tale asimmetria viene portata a conseguenze più estreme.

l'autorità giudiziaria viene a disporre potrebbe avere un impiego, su base normativa, nell'ambito della scelta della cautela personale da applicare nel caso concreto, più che sul piano della valutazione di sussistenza del pericolo cautelare.

Occorre tenere a mente che più si rafforza una fase – quella cautelare nel tempo è stata fortemente avvicinata a quella di merito, sui versanti sia probatorio che decisionale, e l'avanzata dell'IA non potrà che incrementare tale tendenza – più gli equilibri processuali si alterano. Così, l'insidia di misure cautelari applicate come pena anticipata è sempre dietro l'angolo.