mediaLAWS

Rivista di diritto dei media
2/2022 settembre

SEDE
CONTACTS

ACCMS Studio Legale
Via Podgora 13 – 20122 Milano

Università Bocconi - Dipartimento di Studi Giuridici
Via Roentgen 1 - 20136 Milano

e-mail: submissions@medialaws.eu

ANNO 2022 - CODICE ISSN 2532-9146
Impaginazione a cura di Chiara Pavesi

MediaLaws - Rivista di diritto dei media è una rivista quadrimestrale telematica, ad accesso libero, che si propone di pubblicare saggi, note e commenti attinenti al diritto dell'informazione italiano, comparato ed europeo.

La rivista nasce per iniziativa di Oreste Pollicino, Giulio Enea Vigevani, Carlo Melzi d'Eril e Marco Bassini e raccoglie le riflessioni di studiosi, italiani e stranieri, di diritto dei media.

La rivista fa proprio il Code of Conduct and Best Practice Guidelines for Journal Editors elaborato dal COPE (Comittee on Publication Ethics).

La qualità e il rigore scientifici dei saggi della Rivista sono garantiti da una procedura di *double-blind peer review* affidata a un comitato di esperti per la valutazione individuato secondo criteri di competenza e rotazione e aggiornato ogni anno.

MediaLaws - Rivista di diritto dei media
Regolamento per la pubblicazione dei contributi

1. "MediaLaws – Rivista di diritto dei media" è una rivista telematica e ad accesso aperto che pubblica con cadenza quadrimestrale contributi attinenti al diritto dell'informazione.

2. Gli organi della rivista sono il Comitato di direzione, il Comitato scientifico e il Comitato degli esperti per la valutazione. L'elenco dei componenti del Comitato di direzione e del Comitato scientifico della rivista è pubblicato sul sito della stessa (rivista.medialaws.eu). Il Comitato degli esperti per la valutazione è sottoposto ad aggiornamento una volta l'anno.

3. La rivista si compone delle seguenti sezioni: "Saggi", "Note a sentenza" (suddivisa in "Sezione Europa", "Sezione Italia" e "Sezione comparata"), "Cronache e commenti" e "Recensioni e riletture". I singoli numeri potranno altresì ospitare, in via d'eccezione, contributi afferenti a sezioni diverse.

4. La sezione "Saggi" ospita contributi che trattano in maniera estesa e approfondita un tema di ricerca, con taglio critico e supporto bibliografico.

5. La sezione "Note a sentenza" ospita commenti alle novità giurisprudenziali provenienti dalle corti italiane, europee e straniere.

6. La sezione "Cronache e commenti" ospita commenti a questioni e novità giuridiche di attualità nella dimensione nazionale, europea e comparata.

7. La sezione "Recensioni e riletture" ospita commenti di opere rispettivamente di recente o più risalente pubblicazione.

8. La richiesta di pubblicazione di un contributo è inviata all'indirizzo di posta elettronica submissions@medialaws.eu, corredata dei dati, della qualifica e dei recapiti dell'autore, nonché della dichiarazione che il contributo sia esclusiva opera dell'autore e, nel caso in cui lo scritto sia già destinato a pubblicazione, l'indicazione della sede editoriale.

9. La direzione effettua un esame preliminare del contributo, verificando l'attinenza con i temi trattati dalla rivista e il rispetto dei requisiti minimi della pubblicazione.

10. In caso di esito positivo, la direzione procede ad assegnare il contributo alla sezione opportuna.

11. I saggi sono inviati alla valutazione, secondo il metodo del doppio cieco, di revisori scelti dall'elenco degli esperti per la valutazione della rivista secondo il criterio della competenza, della conoscenza linguistica e della rotazione. I revisori ricevono una scheda di valutazione, da consegnare compilata alla direzione entro il termine da essa indicato. Nel caso di tardiva o mancata consegna della scheda, la direzione si riserva la facoltà di scegliere un nuovo revisore. La direzione garantisce l'anonimato della valutazione.

12. La direzione comunica all'autore l'esito della valutazione.
Se entrambe sono positive, il contributo è pubblicato.
Se sono positive ma suggeriscono modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. La direzione si riserva la facoltà di sottoporre il contributo così come modificato a nuova valutazione, anche interna agli organi della rivista. Se solo una valutazione è positiva, con o senza modifiche, la direzione si riserva la facoltà di trasmettere il contributo a un terzo valutatore. Se entrambe le valutazioni sono negative, il contributo non viene pubblicato.

13. Per pubblicare il contributo, l'Autore deve inviare una versione definitiva corretta secondo le regole editoriali della rivista pubblicate sul sito della stessa, un abstract in lingua italiana e inglese e un elenco di cinque parole chiave. Il mancato rispetto dei criteri editoriali costituisce motivo di rigetto della proposta.

14. Le valutazioni vengono archiviate dalla direzione della rivista per almeno tre anni.

15. A discrezione della direzione, i saggi di autori di particolare autorevolezza o richiesti dalla direzione possono essere pubblicati senza essere sottoposti alla procedura di referaggio a doppio cieco ovvero essere sottoposti a mero referaggio anonimo, previa segnalazione in nota.

Indice
Index

Saggi

Note a sentenza

Cronache

Recensioni

Indice
Index

Essays

Case notes

Comments

Book reviews

Sono stati sottoposti a referaggio a doppio cieco i contributi di: Maria Romana Allegri, Andrea Buratti, Ylenia Maria Citino, Caterina Di Costanzo, Federica Giovanella, Angela Mendola, Daniela Messina, Cristina Evanghelia Papadimitriu, Alberto Randazzo.
Su determinazione della direzione, sono inoltre stati sottoposti a referaggio anonimo i contributi di: Filippo Donati, Simone Lonati e Vincenzo Zeno Zencovich.

Cronache

Predictive policing: dal disincanto all'urgenza di un ripensamento

Simone Lonati

Summary

1. Introduzione

In un ipotetico futuro l'umanità ha completamente eliminato gli omicidi e la maggior parte delle azioni criminali. Ciò è possibile grazie all'istituzione di un sistema chiamato *Precrimine*, che utilizza dei veggenti in grado di prevedere il futuro, i *precog* (abbreviazione di precognitivi), per sventare i crimini prima che questi possano essere commessi: è un sistema delicato, osteggiato da molti, che però sembra funzionare senza intoppi. Almeno questo è quello che pensa il capitano Anderson, responsabile della sezione *Precrime* ma soprattutto protagonista di un racconto del 1954 di Philip K. Dick[1].

È sufficiente sostituire i veggenti con algoritmi in grado di elaborare previsioni per tornare al presente. In molte città degli Stati Uniti è, infatti, ormai di uso comune l'utilizzo da parte delle forze dell'ordine di sistemi di intelligenza artificiale in grado di individuare (*crime detection*) e prevenire (*crime prevention*) attività criminali: sono i sistemi di *predictive policing* che, attraverso l'analisi di dati complessi, offrono previsioni in merito al compimento di reati e alla loro localizzazione (*place-based*) o all'elaborazione di profili criminali individuali (*predictive composite*). Il più celebre tra i sistemi predittivi di tipo *place-based* è certamente PredPol, che utilizza un algoritmo di *machine-learning* in grado di suddividere la città in griglie e di aggiornare quotidianamente le proprie previsioni. Proprio sulla base di tali analisi predittive, i Dipartimenti di polizia d'oltreoceano decidono come e dove dispiegare gli agenti nell'attività di controllo del territorio, con particolare attenzione ai luoghi ove vi è una più alta probabilità di commissione di reati (c.d. *hot spots*).

Prima di tornare su questi sistemi e sulle implicazioni problematiche che vi sono proprie, occorre evidenziare come la diffusione di sistemi di intelligenza artificiale, anche in campo penale, riproponga un dilemma centrale nelle riflessioni dei *policymakers* e degli studiosi delle nuove tecnologie: il *trade-off* tra i benefici, di sicuro momento, che questi sistemi promettono e l'impatto che essi presentano sui diritti umani e su alcuni

[1] P.K. Dick, *The Minority Report,* 1956.

principi costituzionali, tra cui quello di eguaglianza. Si tratta, in altri termini, di vagliare la misura entro cui l'evoluzione tecnologica possa svolgersi senza interferire indebitamente con alcuni capisaldi dell'ordinamento, ai quali è ancorata in ultima analisi la tutela della dignità dell'individuo e la sua centralità al cospetto di un mondo che si popola sempre più di macchine e algoritmi. Non è un caso che sempre più spesso i richiami al rispetto dei diritti fondamentali si accompagnino a riferimenti alla dimensione dell'etica, in grado di rafforzare e improntare ulteriormente la conformazione delle tecnologie e del loro sviluppo a un modello antropocentrico che collochi l'uomo al centro[2]. Nello stesso ambito della giustizia penale, del resto, si riscontra un riferimento centrale a questo tema nella adozione della *European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment* da parte della CEPEJ, la *European Commission for the Efficency of Justice*[3] del Consiglio d'Europa.

Questa linea di ragionamento pare coerente con le riflessioni che segnalano la necessità di preservare l'evoluzione tecnologica asservita alle ragioni del diritto, evitando "derive tecnocratiche" che diverrebbe assai difficile contrastare in modo efficace[4].

L'esigenza di ribadire questo "ordine di priorità" si respira senz'altro in settori diversi dell'ordinamento, ma pare acquisire un significato ancora più rilevante in seno al diritto penale e al diritto processuale penale, per un duplice ordine di ragioni. Da un lato, infatti, questa branca presenta una particolare idoneità a tradurre le scelte di politica criminale (anche metodologiche e "procedimentali", ossia legate alle modalità di acquisizione di elementi conoscitivi o di conduzione di attività investigative) in regole che interferiscono con i diritti umani e dunque con le norme e i principi costituzionali dettati a loro presidio (che non si esauriscono, naturalmente, nelle garanzie della libertà personale ma occupano uno spazio più ampio e articolato, che si estende – per esempio – anche al principio del giusto processo). Dall'altro lato, quello della giustizia penale rappresenta l'ambito in cui i sistemi di intelligenza artificiale si candidano a offrire un contributo più importante, soprattutto con riguardo alle attività investigative e decisionali in relazione al loro peculiare apporto predittivo[5]. Al di là dei vantaggi ge-

---

[2] Tra i più recenti, v. per esempio L. DiMatteo - C. Poncibò - M. Cannarsa (eds.), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*, Cambridge, 2022; L. Violante – A. Pajno, *Diritto e etica dell'Intelligenza Artificiale. Presentazione*, in *BioLaw Journal - Rivista di BioDiritto*, 3, 2019, 179 ss. V. anche il manifesto della Fondazione Leonardo – Civiltà delle Macchine, *Statuto etico e giuridico dell'IA,* Roma, 2019. Riferimenti si colgono già anche nel libro bianco della Commissione europea, *White paper On Artificial Intelligence - A European approach to excellence and trust*, Bruxelles, 19 febbraio 2020, COM(2020) 65 final.

[3] In tema 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 *La legislazione penale,* 2021.

[4] Cfr. anche la prospettiva di L. Floridi, T*he European Legislation on AI: a Brief Analysis of its Philosophical Approach,* in *Philosophy & Technology,* 34, 2021, 215 ss.

[5] Alcune riflessioni di ampio respiro rispetto al rapporto tra intelligenza artificiale e diritto penale si colgono in G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Diritto penale contemporaneo - Rivista trimestrale*, 4, 2020, 74 ss.; F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine,* in *Diritto penale e uomo,* 2019; S. Quattrocolo, *Per un'intelligenza penale utile al giudizio penale,* in *BioLaw Journal – Rivista di BioDiritto,* 2, 2021, 387 ss. Con specifico riguardo al processo penale, cfr. il position paper della Fondazione Leonardo – Civiltà delle Macchine, *Processo penale e Intelligenza Artificiale,* 20 ottobre 2020, con contributi di A. Pajno, G. Canzio, G. Salvi, V. Manes, G. Pignatone, F. Pinelli, S. Quattracolo e P. Severino.

nerali per l'efficientamento della giustizia che l'implementazione di nuove tecnologie ha dischiuso, il potenziale dell'intelligenza artificiale connesso agli strumenti di cui è possibile dotare giudici e organi di polizia non ha precedenti.
Proprio lo stretto legame con la dimensione valoriale tipica di ciascun ordinamento e con il quadro di principi sottostante espone però l'intelligenza artificiale e i suoi utilizzi a un quadro normativo non uniforme, che rischia di riproporre l'annoso tema della sovranità digitale in una sua nuova declinazione. Se, infatti, le peculiarità del settore del diritto e della giustizia penale sopra evidenziate fanno dell'intelligenza artificiale uno strumento critico, cui guardare con attenzione in ragione della capacità di incisione degli individui, non tutti gli ordinamenti concepiscono egualmente la portata di alcuni diritti e libertà, così come non tutti i sistemi giuridici riconoscono la medesima portata a determinati principi e valori. Per esempio, ordinamenti in ipotesi meno sensibili alla tutela del principio del giusto processo potranno regolamentare l'implementazione di sistemi di intelligenza artificiale secondo soluzioni normative maggiormente disinvolte, al contrario di sistemi più rigorosi, che offrono uno spazio più limitato all'attuazione di una disciplina di settore. Questo dato immanente nelle peculiarità degli ordinamenti giuridici deve poi essere correlato a un altro elemento strutturale ma extra-giuridico, ossia il contesto infrastrutturale e tecnologico, dipendente in larga se non totale misura dalla disponibilità a compiere ingenti investimenti pubblici ma anche di imprese private. Proprio nel prisma di questo scenario, e alla luce delle connotazioni che si sono ricordate, devono leggersi i tentativi di regolamentazione dei sistemi di intelligenza artificiale partoriti in Europa (con la proposta di regolamento ribattezzata "AI Act"[6]) ma anche oltreoceano (quantomeno come premessa di una futura regolamentazione può inquadrarsi l'AI Blueprint statunitense[7]), quantunque talvolta in forma di *soft law*. I paesi che dispongono di un quadro costituzionale e normativo più permissivo paiono però disporre anche del potenziale economico maggiore, con il rischio che mentre altri ordinamenti studiano le migliori formule regolamentari tese a disciplinare i sistemi di intelligenza artificiale, nel tentativo di coniugare tutela dei diritti e innovazione tecnologica, i primi compiano "salti in avanti" che rendano difficilmente percorribile, in seguito, un *level playing field*.

2. I sistemi predittivi e il dibattito in materia

Tenendo in considerazione le osservazioni appena formulate in relazione ai tentativi regolatori che si appuntano sull'uso di sistemi di intelligenza artificiale, può essere utile ora ritornare sui sistemi di *predictive policing* cui si è fatto cenno in introduzione.
Sin dall'adozione di questi sistemi, negli Stati Uniti è sorto un dibattito che ne ha evidenziato le grandi opportunità, soprattutto in termini di controllo e prevenzione

[6] Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale – Legge sull'intelligenza artificiale – e modifica alcuni atti legislativi dell'Unione,* Bruxelles, 21 aprile 2021, COM(2021) 206 final.

[7] Cfr. The White House, *Blueprint for an AI Bill of Rights. Making Automated Systems Work for the American People,* October 2022.

della criminalità, ma allo stesso tempo le grandi problematicità, legate soprattutto alla natura anti-egualitaria di alcuni di questi modelli e all'assenza di trasparenza in merito al loro funzionamento.

La preoccupazione principale nei confronti del loro utilizzo risiede nella consapevolezza che i sistemi di intelligenza artificiale, pur impiegando algoritmi e strumenti di *machine learning* come sostituti della mente umana, in realtà sono prodotti creati dall'uomo e per questo intrinsecamente caratterizzati dalle umane imperfezioni. Infatti, molti autorevoli studiosi, nell'evidenziare come la qualità e l'equità dei sistemi di *predictive policing* dipenda strettamente dal livello qualitativo dei dati che vi vengono inseriti, hanno denunciato il rischio che all'interno dei *software* predittivi utilizzati dalle forze dell'ordine vengano inseriti i c.d. *dirty data*, ovvero dati ufficiali presenti all'interno dei *databases* dei Dipartimenti di Polizia derivanti (o comunque influenzati) da pregiudizi, pratiche corrotte o attività illegali (ad es. report ufficiali falsificati, prove falsificate, arresti motivati da pregiudizi razziali ecc.) perpetrate nel corso degli anni da parte delle forze dell'ordine, spesso nei confronti di minoranze[8]. Inoltre, a condurre verso pratiche discriminatorie non è solo la scarsa qualità dei dati inseriti nell'algoritmo, ma anche il modo in cui queste informazioni sono raccolte. Le tecnologie utilizzate per la raccolta dei dati sono molto eterogenee: dall'analisi dei *social network* al riconoscimento facciale, le quali, com'è noto, suscitano forti perplessità in tema di *privacy* dei cittadini e sul fronte della loro potenzialità discriminatoria. Ma non è soltanto la qualità dei dati a costituire un primo fronte problematico dal quale deriva l'"educazione" degli algoritmi sottesi al funzionamento di sistemi di intelligenza artificiale. Vi è anche un problema talvolta trascurato, legato a una dimensione quantitativa: la parzialità delle basi di dati esaminate e assimilate dai sistemi di intelligenza artificiale, dai quali non possono che scaturire ulteriori forme e manifestazioni di *bias* che pure non presuppongono un immanente pregiudizio.

Il dibattito in merito all'impatto dei sistemi di *predictive policy* ha anche coinvolto la giurisprudenza che si è trovata a doversi confrontare con le sfide poste dall'innovazione tecnologica nel campo della giustizia penale e con gli aspetti positivi e negativi dei modelli predittivi.

Il primo momento di confronto tra le corti e l'avvento di sistemi di intelligenza artificiale si è avuto con il celeberrimo precedente nel caso *State v. Loomis*[9], con il quale le elaborazioni dottrinali in tema si devono oggi giocoforza confrontare. Il caso ha trovato definizione con una pronuncia della Corte Suprema del Wisconsin, in considerazione del rigetto della richiesta di *certiorari* da parte della Corte Suprema degli Stati Uniti[10]. All'origine della controversia si poneva la contestazione in ordine all'utilizzo

[8] In generale, v. anche per ulteriori riferimenti bibliografici F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information,* Cambridge (MA), 2016. Sul tema specifico, v. poi R. Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, in *University of California, Davis, Law Review,* 51, 2017, 399 ss. V. anche F.Z. Borgesius, *Discrimination, Arttificial Intelligence, and Algorithmic Decision-Making*, Council of Europe, 2018.

[9] 2016 WI 68, 371 Wis. 2d 235, 881 N.W.2d 749. A commento v. Criminal law - *State v. Loomis Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing*, in *Harvard Law Review,* 130, 2017, 1530 ss.

[10] *Loomis v. Wisconsin*, 881 N.W.2d 749, cert. denied, 137 S.Ct. 2290.

del software COMPAS, in grado di pronosticare la probabilità di recidiva correlata all'imputato e così aiutare il giudice nell'individuazione della condanna. Questo sistema si fonda sulla generazione di *risk assessment* (*Presentence Investigation Report*) che forniscono un apprezzamento del livello di rischio in relazione ad alcuni dati assunti come input, acquisiti sia nel corso di colloqui con l'imputato sia attraverso l'analisi delle informazioni relative al suo storico criminale. Riportata la condanna, il sig. Loomis contestava la violazione delle sue garanzie difensive, appellandosi in particolar modo al principio del *due process,* che non avrebbe tollerato l'utilizzo di un sistema sviluppato da privati e quindi coperto da privativa industriale, come tale non controllabile nell'esplicazione delle sue inferenze e deduzioni.

Il tema del controllo su *software* coperti da segreto industriale, che si innesta "formalmente" sul rispetto delle garanzie difensive del giusto processo, si inserisce così quale ulteriore nodo critico "sostanziale" nella già complessa trama di motivi oggetto di dibattito. A ben vedere, non pare che l'apporto fornito da strumenti di matrice proprietaria e riconducibili a privati possa costituire una novità anche nell'esercizio di funzioni di rilievo pubblico come quelle giurisdizionali: si pensi alle banche dati, ai massimari giurisprudenziali e a tutte le risorse di cui ogni giurista (e non solo un giudice) può avvalersi, e che inevitabilmente "condizionano" – orientandolo – il suo percorso per fare intelligenza di fenomeni giuridici. Dove si colloca, allora, la differenza con l'utilizzo di sistemi predittivi? Ciò che desta maggiore preoccupazione rispetto all'avvento di questi sistemi e alla loro diffusione crescente è la capacità di restituire indicazioni apparentemente vincolanti per il giudice, quale frutto di un percorso logicamente non controllabile da un agente umano. In realtà, proprio la consapevolezza dell'esistenza di limiti intrinseci che connotano questi sistemi, derivanti anche dalla già ricordata parzialità dei dati e dalle criticità connesse alla loro incerta qualità e attendibilità segna un punto importante a favore della loro corretta implementazione nell'ambito della giustizia penale; questi limiti, infatti, per un verso segnalano la precarietà intrinseca dei sistemi predittivi, mettendo fine a ogni velleità (invero nemmeno teorizzata in dottrina) di equiparazione, se non addirittura di sostituzione, del giudice con un agente *software*; per altro verso, e in modo correlato, questi limiti rendono palese l'unica utilità ricavabile dai sistemi predittivi nel rispetto dei principi che governano il giusto processo, quale supporto conoscitivo soggetto alla libera valutazione del giudice[11].

La "decisione algoritmica", così, non è una determinazione che si sovrappone a quella del giudice, ma semmai un apporto conoscitivo di matrice statistica rimesso all'apprezzamento delle corti. Questo sostanziale ridimensionamento non elimina, naturalmente, le criticità proprie dei sistemi di intelligenza artificiale: il giudice non potrà, forse, esaminare come un sistema predittivo sia giunto a formulare un dato *output*, dovendo giocoforza appagarsi di una risposta che questi non può controllare né sindacare; ma il giudice resta indiscutibilmente al centro del processo decisionale che precede l'emanazione della sentenza.

Questi stessi fattori paiono aver guidato la decisione della Corte Suprema del Wiscon-

[11] Riflessioni a proposito del caso *Loomis* da una prospettiva europea si trovano in S. Carrer, *Se l'amicus curiae è un algoritmo: il chiacchierato caso Loomis alla Corte Suprema del Wisconsin*, in *Giurisprudenza Penale Web*, 2019, 4.

sin in *Loomis*, incentrata su una visione "strumentale" del *software* COMPAS rispetto all'attività decisionale del giudice. Proprio nella sua sentenza, la Corte ha escluso che l'utilizzo di COMPAS integrasse una violazione del diritto di Loomis al giusto processo, rilevando che non vi fosse alcuna prova del fatto che la sentenza oggetto di gravame si fosse fondata precipuamente su fattori personali (quali il genere) che connotavano la persona dell'imputato.

Per giungere alla conclusione che il tribunale distrettuale non avesse errato nella sua sentenza, la Corte Suprema ha dovuto sviscerare alcuni aspetti peculiari di COMPAS. La sentenza è cristallina nell'affermare che una decisione giudiziale non può trovare fondamento esclusivo nei *risk assessment* prodotti dal *software* in questione, che non possono costituire dunque un fattore dirimente. Questi sistemi invece racchiudono un potenziale utile per migliorare la ponderazione e la valutazione degli elementi di prova a disposizione del giudice, ma continuano a qualificarsi come serventi rispetto all'apprezzamento da condursi da parte del giudice. Questo implica un potere dispositivo rispetto alla considerazione attribuita ai report generati da COMPAS. La Corte ha ricordato, tra l'altro, che i punteggi di rischio non dovrebbero determinare la severità della condanna né l'applicazione di circostanze aggravanti o attenuanti, o ancora della pena detentiva: si tratta, semmai, di elementi che devono essere utilizzati per la riduzione e la gestione del rischio (e pertanto in una funzione "accessoria" rispetto al contenuto decisorio tipico). Di qui, anche la necessità di formulare alcuni avvertimenti agli utilizzatori di questo sistema, in modo da costringerne gli utilizzi entro modalità precise e consentite dall'ordinamento: nel caso di Loomis, l'uso (legittimo) di COMPAS è funzionale al controllo dell'individuo all'interno della comunità proprio in relazione al livello di rischio correlato. Su queste premesse, ed escluse le effrazioni ai principi costituzionali temute da Loomis, la Corte Suprema ha ritenuto che la corte distrettuale avesse correttamente soppesato le informazioni acquisite tramite COMPAS, conformandosi peraltro alla necessità di adoperare una generale cautela relativa al *fair use* algoritmico.

Nella stessa occasione, la Corte Suprema ha poi respinto le doglianze inerenti alla natura proprietaria di COMPAS, riscontrando come – benché il codice sorgente del *software* fosse tutelato dal Trade Secret Act – il manuale fornito per l'utilizzo del *software* recasse un insieme di istruzioni sufficienti a spiegare le modalità di calcolo del punteggio, così come a illustrare – tra l'altro – le variabili rilevanti di un sistema ritenuto dalla Corte sufficientemente affidabile.

Ma un punto a sua volta assai importante sul quale si sono concentrati i giudici è quello inerente al rischio di generalizzazioni tali da "spersonalizzare" la valutazione della condotta penalmente rilevante, attribuendo rilievo a fattori circostanziali in modo peraltro discriminatorio (come l'origine etnica o il genere). In questo passaggio è racchiuso, forse, il nucleo problematico che tuttora condiziona l'attuazione di sistemi algoritmici in ambito penale. Il timore rappresentato alla Corte Suprema del Wisconsin riguardava il rischio che, per effetto della intrinseca parzialità dei dati processati e delle possibili discriminazioni insite nei set di dati utilizzati per educare il *software*, quest'ultimo fosse incline a suggerire l'applicazione di un regime sanzionatorio più severo in considerazione dell'appartenenza dell'imputato ad alcune categorie oggetto di *bias*. Si

tratta forse dell'aspetto più critico sul fronte della giustizia penale, che insinua il pericolo di un depotenziamento del principio di personalità della responsabilità criminale. Ed è proprio su questo crinale così delicato che la pronuncia è parsa maggiormente evasiva, limitandosi a esigere dai produttori del *software* un aggiornamento costante che tenga in considerazione le continue evoluzioni che si registrano anche sul piano sociale; spetterà invece alle corti contestare, se del caso, l'eventuale cattivo esercizio di discrezionalità da parte dei giudici che abbiano fatto impiego dei report generati da COMPAS. Un'occasione forse persa per ribadire con vigore e fermezza la rilevanza del quadro costituzionale, che la Corte Suprema ha superato osservando che in realtà nel caso di specie non vi fosse stata prova che la condanna del sig. Loomis era dipesa esclusivamente e in modo determinante dalla considerazione del *gender*, a dispetto della corretta (a giudizio dei giudici supremi) ponderazione che invece la sentenza gravata aveva effettuato di altri fattori rilevanti nella vicenda in questione.
Al di là dell'impostazione a tratti formalistica e di una prospettiva forse eccessivamente superficiale sul piano della tutela dei diritti costituzionali, la sentenza ha avuto il merito di non avversare completamente e in via aprioristica l'implementazione di sistemi di intelligenza artificiale nell'ambito del processo penale, mostrando semmai lo sforzo di immaginarne una collocazione al riparo quantomeno da criticità "frontali". Forse proprio la limitata, non rigoristica attenzione al piano della tutela sostanziale dell'individuo ha permesso alla Corte Suprema del Wisconsin di leggere nel sistema COMPAS i tratti di un *software* compatibile con l'ordinamento e con il principio del giusto processo; lasciando però scoperto un fianco rispetto al tema più delicato, su cui non a caso si sono inserite pronunce successive di segno parzialmente diverso.

3. Il caso *United States v. Curry*

Nel luglio del 2020 sul tema della discriminazione condotta attraverso sistemi predittivi si è pronunciata anche la Corte d'Appello del Fourth Circuit in composizione *en banc* (United States Court of Appeals for the Fourth Circuit, *United States of America v. Billy Curry, Jr.*[12]). Nel caso *United States v. Curry* i giudici erano chiamati a decidere se il fermo e la perquisizione dell'imputato fossero giustificati alla luce della dottrina delle c.d. *exigent circumstances* e hanno offerto un'interessante disamina proprio in tema di *predictive policing*[13].
Come noto, la dottrina delle *exigent circumstances* consente di derogare al requisito costituzionale prescritto dal Quarto Emendamento di ottenere un *warrant* per condurre *searches* e *seizures*. La sua elaborazione risale alla sentenza della Corte Suprema statunitense nel caso *Missouri v. McNeely*[14], ove i giudici avevano rilevato come: «*A variety of circumstances may give rise to an exigency sufficient to justify a warrantless search, including law enforcement's need to provide emergency assistance to an occupant of a home* […] *engage in "hot pur-*

[12] No. 18-4233, 15 luglio 2020.

[13] A commento specifico di questa vicenda v. anche l'intervento di V. Manes nel *position paper* di Fondazione Leonardo – Civiltà delle Macchine, *Processo penale e Intelligenza Artificiale,* cit., 11 ss., spec. 12.

[14] 569 US 141 (2013).

suit" of a fleeing suspect . . . or enter a burning building to put out a fire and investigate its cause»[15].
Il caso aveva tratto origine dal fermo del sig. Curry, giustificato dall'esplosione di alcuni colpi d'arma da fuoco nelle vicinanze di un complesso residenziale distante pochi minuti dal luogo dove egli si trovava al momento della perquisizione che aveva condotto al suo fermo.
Le circostanze fattuali, nel caso di specie, hanno permesso ai giudici di soffermarsi sulle implicazioni derivanti dall'utilizzo da parte delle forze dell'ordine della città di Richmond di un modello di *predictive policing*[16] declinato in forma di attuazione di *hot-spot policing*. Questo sistema presuppone una previa identificazione di aree connotata da pericolo elevato, in modo da governare l'allocazione delle forze di polizia concentrandola nelle zone più rischiose in modo non solo da perseguire la commissione di crimini ma anche da prevenirla. Questa modalità operativa, come si legge nella sentenza, si è progressivamente evoluta alimentandosi dell'elaborazione di *big data* e del supporto fornito da sistemi di *machine learning*.
In questo caso non siamo dunque di fronte a un intervento dei sistemi di intelligenza artificiale in sede di condanna, come nella vicenda *Loomis*, bensì all'impiego di sistemi innovativi con capacità predittive nell'organizzazione delle attività di polizia. Nonostante le differenze con il caso *Loomis*, gli spunti rispetto alla capacità di interferenza di questi ultimi sistemi non mancano e offrono l'occasione per riprendere alcuni dei fronti critici che quella decisione non aveva forse del tutto sopito.
Le argomentazioni proposte a difesa dei sistemi predittivi sono state criticate all'interno di tre separate *concurring opinions*, affidate ai giudici Gregory, Wynn e Thacker. Quest'ultima, in particolare, ha proposto una delle argomentazioni più forti avverso l'utilizzo dei modelli predittivi, ovvero la già ricordata natura anti-egualitaria degli stessi, paragonati dalla giudice a veri e propri strumenti di profilazione razziale. L'utilizzo di algoritmi informatici in grado di localizzare il probabile compimento di attività criminali non rappresenta più lo strumento innovativo e promettente di un tempo avendo rivelato tutti i pregiudizi razziali con cui i modelli di *predictive policing* sono costruiti, come dimostrato dalla recente decisione della città di Los Angeles, una delle prime ad adottare un *software* di questo tipo, di porre fine al loro utilizzo. Nella sua *opinion*, la giudice Thacker, nell'evidenziare come la tecnologia non possa annullare i difetti dell'essere umano, ha rimarcato che la bontà degli algoritmi dipende dalla qualità dei dati che vi vengono inseriti (secondo la logica del c.d. GIGO, "*garbage in, garbage out*"): anni e anni di condotte discriminatorie da parte delle forze dell'ordine hanno prodotto dati sulle attività criminali inficiati da pregiudizi razziali e particolarmente affliggenti nei confronti delle minoranze e, in particolare, delle comunità di colore.
Il grido d'allarme lanciato dalla giudice statunitense è d'altronde corroborato da alcune autorevoli ricerche empiriche, tra cui quella portata avanti nel 2019 dal centro studi AI Now, condotta in 13 giurisdizioni statunitensi che utilizzavano algoritmi di *predictive policing*, da cui è emerso come ben in 9 di esse i sistemi predittivi erano stati programmati con l'utilizzo dei c.d. *dirty data*. Uno dei rischi principali che si celano dietro ad un

[15] *Opinion* della Corte, 5.

[16] Descritto peraltro in J. Bachner, *Predictive Policing: Preventing Crime with Data and Analytics,* IBM Center for the Business of Government, 2013, 29-30.

sistema così costruito è proprio quello di alimentare, attraverso l'utilizzo dei modelli predittivi, il c.d. *confirmation feedback loop*: i sistemi di *predictive policing* composti da dati alterati porteranno a previsioni viziate che rischiano di perpetrare ulteriori forme di ingiustizia nei confronti delle comunità più emarginate e già afflitte da anni di violenze subite, con gravissime conseguenze sul sistema della giustizia penale e, più in generale, sul tessuto sociale di una comunità. La stessa giudice non ha lesinato un importante richiamo allo *Statement of Concern about Predictive Policing by ACLU and 16 Civil Rights Privacy, Racial Justice, and Technology Organizations*[17] emesso già nell'agosto 2016. Secondo questo documento, redatto da associazioni impegnate a promuovere la tutela dei diritti umani: «*Predictive policing systems threaten to undermine the constitutional rights of individuals. The Fourth Amendment forbids police from stopping someone without reasonable suspicion -- a specific, individualized determination that is more than just a hunch. Computer-driven hunches are no exception to this rule, and a computer's judgment is never a further reason (beyond the articulable facts that intelligibly caused that judgment) for a stop, search, or arrest. Similarly, predictive policing must not be allowed to erode rights of due process and equal protection. Systems that manufacture unexplained "threat" assessments have no valid place in constitutional policing*».

La pronuncia del Fourth Circuit, pur non potendo certamente essere confinata esclusivamente all'interno del dibattito sui modelli di *predictive policing*, è rappresentativa della discussione in atto oltreoceano (ma ormai, come si vedrà, anche in Europa) in merito alle sfide e prospettive che l'innovazione tecnologica pone nel campo della giustizia penale. Se è, infatti, innegabile che gli strumenti predittivi costituiscano un importante strumento in mano alle Autorità nel campo della sicurezza pubblica e della prevenzione dei reati, è allo stesso tempo necessario rilevare come sia già in atto una forma di disincanto nei confronti di questi modelli per gli effetti potenzialmente discriminatori che essi sono in grado di produrre. Effetti, questi, che possono essere evitati solo qualora gli algoritmi e i *software* utilizzati per l'analisi dei Big Data siano resi più trasparenti, in modo che sia possibile per un'autorità indipendente valutarne i processi sottostanti e gli standard utilizzati[18].

4. E in Italia?

Se gli Stati Uniti rappresentano il termine di paragone al quale occorre giocoforza rifarsi per comprendere quale sensibilità si sia formata rispetto all'implementazione dei sistemi più avanzati e alla loro conformità ai diritti costituzionali, occorre volgere lo sguardo anche in Europa per comprendere quale sia lo stato dell'arte rispetto alle prospettive future, su cui andranno a intervenire in prima battuta il prossimo AI Act, pur regolamento di contenuto generalista, e a seguire un'altra serie di atti normativi.

Occorre anzitutto premettere che il quadro assiologico europeo confezionato dalla Convenzione europea dei diritti dell'uomo, dalla Carta dei diritti fondamentali dell'UE

[17] Reperibile online in *aclu.org*.

[18] Per alcuni spunti generali cfr. anche A. Pajno - M. Bassini - G. De Gregorio - M. Macchia - F.P. Patti - O. Pollicino - S. Quattrocolo - D. Simeoli - P. Sirena, *AI: profili giuridici Intelligenza Artificiale: criticità emergenti e sfide per il giurista,* in *BioLaw Journal - Rivista di BioDiritto*, 3, 2019, 205 ss.

nonché dalle tradizioni costituzionali che accomunano molti degli Stati che aderiscono all'Unione e/o al Consiglio d'Europa pare improntato a una maggiore prudenza rispetto all'implementazione di sistemi predittivi. A differenza del sistema statunitense, tendenzialmente proteso sulla preservazione della regolarità procedurale ancorata al *due process* quale unica "barriera" rispetto all'attuazione di meccanismi come quelli in indagine, le "difese immunitarie" dell'ordinamento europeo si offrono in una dimensione prevalentemente sostanziale, qual è quella della tutela di alcuni diritti assurti ormai a cifra del costituzionalismo del vecchio continente, tra cui la *privacy*.

Le linee di continuità tra la tutela del diritto alla *privacy* e alla protezione dei dati e la tutela dell'individuo al cospetto di sistemi predittivi si coglie in almeno due livelli.

Nell'ordinamento dell'Unione europea, anzitutto, i tentativi di regolamentazione dei sistemi di intelligenza artificiale rivelano l'adozione di un approccio regolatorio analogo a quello della disciplina della protezione dati affidata al GDPR (Regolamento Generale sulla Protezione dei Dati, regolamento (UE) 2016/679)[19]. Il cosiddetto "approccio basato sul rischio" tende a modulare gli obblighi applicabili a seconda del livello di rischio intrinseco a ciascun sistema di intelligenza artificiale, così da imporre, per un verso, una preliminare valutazione del rischio da tradursi in una analisi di impatto sui diritti e sulle libertà individuali e da escludere, per altro verso, la commerciabilità di sistemi che presentino un rischio non tollerabile. Questa modulazione non esclude la possibilità di implementare, anche nell'ambito della giustizia penale, sistemi ad alto rischio, ponendo tuttavia dei requisiti stringenti che circoscrivono le condizioni di fruibilità di nuove tecniche.

Prima ancora, dunque, di interrogarsi sulla possibilità di integrazione tra sistemi predittivi e norme processuali[20] vi è da considerare la "barriera" della tutela dei diritti umani contro la quale si sono peraltro infranti già alcuni tentativi di implementare analoghi sistemi nell'ambito dell'attività amministrativa. Del resto, difficilmente tecniche che presentassero criticità sotto il versante della loro compatibilità con principi costituzionali (quale quello di non discriminazione) o con diritti fondamentali (quale quello alla *privacy* e protezione dei dati) potrebbero utilmente offrirsi nell'ambito del giudizio penale quale strumento di supporto o di ausilio del giudice. Proprio il terreno di sperimentazione di sistemi algoritmici nell'ambito dell'attività della pubblica amministrazione individua il secondo livello da cui emerge la connessione poc'anzi denunciata con la tutela dei dati personali quale "cifra" della compatibilità tra sistemi di intelligenza artificiale e ordinamento giuridico.

A livello nazionale, infatti, le indicazioni rilevanti si possono cogliere solamente in alcune prese di posizione della giurisprudenza amministrativa, in cui i giudici (Tar del Lazio e Consiglio di Stato) hanno adoperato il "filtro" della normativa europea sulla

[19] Su questi profili, v. G. De Gregorio - P. Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *Common Market Law Review*, 59(2), 2022, 473 ss. Sul rapporto tra intelligenza artificiale protezione dei dati personali v. anche A. Pajno – F. Donati – A. Perrucci (a cura di), *Intelligenza Artificiale e diritto: una rivoluzione?,* Bologna, 2022, vol. 1, parte III, nella sezione a cura di M. Bassini e O. Pollicino.

[20] Su cui più in dettaglio si esprimono G. Canzio, *Intelligenza Artificiale, algoritmi e giustizia penale,* in *Sistema penale,* 8 gennaio 2022 e S. Quattrocolo, *Equo processo penale e sfide della società algoritmica*, in *BioLaw Journal - Rivista di BioDiritto*, 3, 2019, 135 ss.

protezione dei dati personali come metodo di vaglio della legittimità dei *software* di cui era stato contestato l'utilizzo da parte della pubblica amministrazione[21]. Le vicende giurisprudenziali di cui si discorre sono note, ma vale la pena evidenziare la capacità delle corti di offrire una lettura "trasversale" della compatibilità di queste tecniche. Le quali, se per un verso sono destinate all'adozione nel campo dell'attività amministrativa, assoggettata – così come quella giurisdizionale – ad alcuni principi costituzionali, per altro sono egualmente condizionate nella loro pratica implementazione dal rispetto di alcuni diritti.

In questo frangente è emersa la centrale connessione con alcuni capisaldi che la disciplina racchiusa nel GDPR presenta in relazione ad alcune garanzie di sistema legate al trattamento di dati. Il nodo centrale non riguarda tanto le modalità di trattamento di dati personali disciplinate nelle regole del GDPR, quanto il rispetto di una serie di principi e garanzie che il regolamento ha posto rispetto alla loro idoneità a incidere sui diritti e libertà degli individui i cui dati siano oggetto di trattamento. In questo senso si coglie come il GDPR sia andato invero "oltre" la mera definizione di regole di *data governance*, prendendo atto della sua capacità prescrittiva al di fuori delle regole sul trattamento di dati *tout court*. Non a caso la dottrina ha evidenziato come le implementazioni algoritmiche di cui si è effettuato uno scrutinio di legittimità in ambito amministrativo costituissero una sorta di "stress test" della capacità della normativa in materia di trattamento di dati di "reggere" e preservare la centralità dei diritti e delle libertà individuali al cospetto di evoluzioni non calcolabili all'atto del *drafting* legislativo[22]. La chiave di lettura offerta del GDPR e di alcune sue importanti previsioni non ha poi impedito ai giudici amministrativi di cogliere anche alcuni aspetti ulteriori che rivelano la capacità delle emergenti tecnologie predittive di impattare garanzie tipicamente processuali.

Andando però per ordine, il "filtro" del GDPR pare costituire una prima barriera fondamentale sul cui crinale si gioca la concreta fattibilità di implementazioni di sistemi predittivi. Con la sentenza n. 8472 del 13 dicembre 2019, infatti, la sesta sezione del Consiglio di Stato ha potuto mettere a fuoco un tema a ben vedere assai prossimo a quello affrontato dalla Corte Suprema del Wisconsin nel caso *Loomis*, ossia le conseguenze della natura proprietaria del software[23]. I giudici di Palazzo Spada hanno richiamato i precedenti del Tar Lazio per soffermarsi sulla necessità che gli algoritmi sottostanti soddisfino condizioni di conoscibilità e comprensibilità, requisiti che non indicano solamente l'esigenza di rendere pubblico il metodo di funzionamento delle tecniche adoperate ma anche quella di presentare queste informazioni secondo un

[21] Su queste vicende, si v. i commenti dettagliati, tra gli altri, di S. Vernile*, Intelligenza artificiale e diritto: una rivoluzione?,* in questa *Rivista,* 2, 2020, 136 ss.; L. Musselli, *La decisione amministrativa nell'età degli algoritmi: primi spunti,* ivi, 1, 2020, 18 ss.; G. Fasano, *Le decisioni automatizzate nella pubblica amministrazione: tra esigenze di semplificazione e trasparenza algoritmica,* ivi, 3, 2019, 234 ss. In generale, v. anche D. Galetta - J.G. Corvalàn, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *Federalismi.it,* 3, 2019,

[22] Si v. M. Bassini – O. Pollicino, *La Cassazione sul "consenso algoritmico". Ancora un tassello nella costruzione di uno statuto giuridico composito,* in *Giustizia Insieme*, 21 giugno 2021.

[23] La pronuncia ha trovato peraltro pedissequa conferma in Cons. Stato, sez. VI, 4 febbraio 2020, n. 881.

registro accessibile a qualsiasi individuo, così da garantire che possa spiegarsi il suo potere di controllo. Di fronte a queste fondamentali salvaguardie, secondo il Consiglio di Stato non ha ragione di reclamarsi utilmente un'aspettativa di riservatezza industriale da parte delle imprese produttrici. Questo argomento, difatti, viene privato di pregio in conseguenza della messa a disposizione e a servizio del potere autoritativo di tali strumenti. Con questa affermazione non pare invero che il Consiglio di Stato abbia inteso ridimensionare l'importanza dei requisiti menzionati così da circoscriverla soltanto ai sistemi destinati a un impiego in ambito pubblico; semmai, la pronuncia tende a evidenziare la centralità che la conformità a determinati principi guadagna al cospetto della loro fruizione da parte di autorità (giurisdizionali o di altro tipo) per l'assolvimento di finalità pubblicistiche. Proprio questa funzionalizzazione comporta l'assoggettamento a un canone di trasparenza che altrimenti potrebbe dirsi non altrettanto rilevante, a fronte del quale nessuna obiezione può essere utilmente avanzata, secondo il Consiglio di Stato, rispetto alla pretesa di segretezza delle privative industriali. Nel merito della questione, i giudici hanno rilevato come le esigenze predette trovino corrispondenza nelle previsioni stabilite dal GDPR. Infatti, il regolamento costituisce un diritto *ex* art. 15 per garantire all'interessato (la persona fisica cui appartengono le informazioni) l'accesso ai dati personali che lo riguardano; l'interessato può così venire a conoscenza se un dato soggetto, in qualità di titolare, tratti i suoi dati, e in caso affermativo avrà diritto a conoscere le caratteristiche di tali trattamenti. In questo modo il regolamento appaga i requisiti conoscitivi poc'anzi ricordati. Allo stesso tempo, però, il GDPR pone un limite esplicito ai processi decisionali integralmente automatizzati con la previsione di cui all'art. 22, cui è peraltro collegata, nell'elaborazione dottrinale, la discussa sussistenza di un "diritto alla spiegazione" che possa rendere edotte all'interessato le modalità operative sottostanti il processo decisionale. Da questa disposizione, la cui portata è oggetto di dibattito, sembrerebbe evincersi, nelle parole del Consiglio di Stato, la necessità di individuare un centro di imputazione e di responsabilità, onde poter accertare la legittimità e la logicità della decisione algoritmica e poterla imputare a un organo competente. Quella del GDPR, allora, non è un'incidenza che si spiega soltanto sul piano dei trattamenti di dati ma che si estende anche oltre, inerendo intimamente al collegamento tra persona e automazione.

Secondo il Consiglio di Stato, infatti, dal diritto dell'Unione si possono individuare tre principi rilevanti in questo ambito: dapprima il principio di conoscibilità, che si "potenzia" e diviene principio di comprensibilità di fronte all'attuazione di decisioni automatizzate da parte di soggetti pubblici; in secondo luogo, il principio di non esclusività della decisione algoritmica (c.d. *human in the loop*), che garantisce un intervento umano che potrà in ogni caso controllare, validare o smentire la decisione automatizzata; infine, il principio di non discriminazione algoritmica, che richiede al titolare del trattamento ad attuare misure adeguate anche per rettificare quei fattori che comportano inesattezze, minimizzare gli errori e impedire possibili effetti discriminatori connaturati anche alla parzialità delle informazioni processate nella fase di *training* (c.d. *garbage in, garbage out*).

Così, leggendo anche queste righe alla luce del considerando 71 del GDPR[24], si co-

[24] «L'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa

glie come un algoritmo, per poter effettivamente dirsi compatibile con l'ordinamento, deve non solo essere conoscibile e comprensibile, ma anche rappresentare una tra le varie (e non l'unica) motivazioni della decisione e – da ultimo – non presentare carattere discriminatorio.

La pronuncia del Consiglio di Stato ha ritenuto che gli algoritmi sottostanti al *software* utilizzato dalla pubblica amministrazione (e in particolare dal Ministero dell'Istruzione, dell'Università e della Ricerca) per le assegnazioni di docenti di scuola superiore secondaria non rispettassero queste prescrizioni. In particolare, il sistema adoperato non consentiva di discernere le ragioni per le quali il *software* fosse pervenuto a una determinata decisione, frustrando le aspettative di soggetti collocati in graduatorie senza una precisa spiegazione. Il Consiglio di Stato ha riconosciuto che la conformità a questi principi non implica una meccanica e rigida applicazione delle regole procedimentali all'attività amministrativa in forma algoritmica, così offrendo un importante margine rispetto alla sperimentazione anche di sistemi predittivi che potrebbero essere attuati altrove (come nel processo penale); tuttavia, la presa di posizione si segnala per collocare in assoluta primazia il rispetto del canone di trasparenza, funzionale ad assicurare il rispetto requisiti strutturali, ontologici della decisione pubblica, ossia la motivazione e giustificazione. In questa pronuncia, i giudici hanno così escluso che si possa presumere una corrispondenza tra il canone di legalità, inteso in senso ampio, e le operazioni algoritmiche, tutt'altro che "perfette". L'eventuale corrispondenza deve

includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani. Tale trattamento comprende la «profilazione», che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona. Tuttavia, è opportuno che sia consentito adottare decisioni sulla base di tale trattamento, compresa la profilazione, se ciò è espressamente previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento, o se è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, o se l'interessato ha espresso il proprio consenso esplicito. In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura non dovrebbe riguardare un minore.

Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti. Il processo decisionale automatizzato e la profilazione basati su categorie particolari di dati personali dovrebbero essere consentiti solo a determinate condizioni».

infatti essere dimostrata, in particolare grazie a una scrupolosa verifica delle condizioni impartite quali input e dell'iter seguito dalla tecnologia per giungere a una determinazione.
Prima del Consiglio di Stato, numerose pronunce del Tribunale amministrativo del Lazio si erano appuntate sulla medesima vicenda, dalla quale è derivata la proposizione di diversi ricorsi. In precedenza, in linea con i giudici di primo grado, il Consiglio di Stato si era già espresso con la sentenza n. 2270 dell'8 aprile 2019, in cui la sesta sezione aveva più timidamente osservato come l'impiego del *software* per le assegnazioni del personale docente da parte del MIUR avesse determinato la violazione dei principi di imparzialità, pubblicità e trasparenza, ma sempre in relazione all'impossibilità di venire a conoscenza dell'iter logico sottostante la decisione algoritmica. Proprio in questa pronuncia, i giudici di Palazzo Spada avevano evidenziato come l'automazione favorita dall'impiego di un software dovesse in linea di principio salutarsi con favore, quale virtuosa declinazione del principio di buon andamento (e di efficienza) della pubblica amministrazione di cui all'art. 97 Cost. Al contempo, però, i giudici avevano rilevato come un'attività siffatta non potesse, per tale ragione, sfuggire ai requisiti che si impongono nell'ordinamento per l'attività amministrativa. In questa occasione, il Consiglio di Stato ha affermato che la regola tecnica rimane pur sempre, in questo contesto, una regola amministrativa generale, che deve essere in quanto tale costruita dall'uomo e non già elaborata da una macchina, che semmai potrà occuparsi della sua applicazione. Proprio per questo, il supremo tribunale amministrativo aveva enunciato il rispetto di quattro condizioni quale requisito per ogni regola algoritmica: la conformità a canoni di pubblicità e trasparenza, ragionevolezza e proporzionalità, conseguente alla piena efficacia giuridica della regola così costruita; l'assenza di un margine di discrezionalità affidato al *software*, che sarebbe incompatibile con la necessità che la regola amministrativa assecondi con precisione e certezza ogni determinazione; l'assolvimento da parte della pubblica amministrazione del compito di composizione degli interessi in gioco, con conseguente "educazione" dell'algoritmo; la sindacabilità della regola algoritmica da parte del giudice, che deve essere in grado di appurare la correttezza di ogni processo automatizzato in ogni fase. In altri termini, la precedente pronuncia dei giudici amministrativi aveva rivendicato una sovranità giuridica e amministrativa sullo sviluppo di regole tecniche.

5. Spunti conclusivi

Come si è osservato, l'ordinamento italiano non offre materiale utile a comprendere, sul piano empirico, la concreta "fattibilità" di soluzioni tecniche tese, grazie al supporto degli algoritmi, a efficientare il processo decisionale del giudice penale o a offrirvi comunque supporto. Il secondo livello di verifica, già compiuto negli Stati Uniti nel caso *Loomis*, legato all'integrazione tra tecnologie algoritmiche di natura predittiva con le garanzie processuali, non si è potuto ancora compiutamente dischiudere nel nostro ordinamento, né è detto che giungerà a maturazione in un futuro prossimo. Le attenzioni della giurisprudenza sono state rivolte prevalentemente, se non esclusivamente,

al piano della conformità dell'attività amministrativa algoritmica con alcuni capisaldi che sono dettati *in primis* dalla legislazione europea in tema di dati personali, ancorché facilmente rinsaldabili con alcuni principi costituzionali. Ma queste indicazioni offrono già uno spaccato sufficiente a comprendere le difficoltà che i sistemi predittivi potrebbero incontrare rispetto a una loro diffusione nel giudizio penale. La via dell'automazione è certamente una direzione già tracciata anche nell'ambito dei disegni di riforma della giustizia penale, ma l'integrazione tra algoritmi, intelligenza artificiale e processo pare ancora lontana, in Italia, dal trovare un momento di saldatura, quantomeno se ci si attende che i predetti sistemi possano rappresentare qualcosa in più di semplici strumenti conoscitivi apprezzabili dal giudice, il che costituisce – allo stato – l'unico inquadramento possibile e ipotizzabile di strumenti predittivi nel contesto della giustizia[25].

[25] Per riflessioni ulteriori, si rinvia alle diffuse e analitiche trattazioni, tra gli altri, di E. Negri, *Artificial Intelligence, l'innovativo rapporto di (in)compatibilità fra machina sapiens e processo penale,* in *Sistema penale,* 7, 2021, 5 ss.; S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Cham, 2020.

Elenco autori

Maria Romana Allegri
professoressa associata di istituzioni di diritto pubblico, Sapienza - Università di Roma
Andrea Buratti
professore ordinario di diritto pubblico comparato, Università degli Studi di Roma "Tor Vergata"
Liliana Ciliberti
esperta di copyright e di regolamentazione dei media e delle comunicazioni elettroniche
Ylenia Maria Citino
assegnista di ricerca di istituzioni di diritto pubblico, LUISS Guido Carli
Caterina Di Costanzo
assegnista di ricerca di diritto costituzionale, Università degli Studi di Firenze
Filippo Donati
professore ordinario di diritto costituzionale, Università degli Studi di Firenze
Andrea Fedi
avvocato in Roma
Filippo Luigi Giambrone
ricercatore di diritto tributario, Università degli Studi del Sannio
Federica Giovanella
professoressa associata di diritto privato comparato, Università degli Studi di Udine
Carloalberto Giusti
professore ordinario di diritto privato comparato, Link University
Ottavio Grandinetti
avvocato in Roma
Simone Lonati
professore associato di diritto processuale penale, Università Bocconi
Valerio Lubello
avvocato in Milano
Angela Mendola
docente a contratto di diritto privato, Università degli studi di Salerno
Daniela Messina
docente a contratto di diritto dell'informazione e dell'informatica, Università degli Studi di Napoli "Parthenope"
Matteo Monti
assegnista di ricerca di diritto pubblico comparato, LUISS Guido Carli
Cristina Evanghelia Papadimitriu
ricercatrice di diritto dell'economia, Università degli Studi di Messina
Maria Pia Peluso
dottoranda di ricerca, Università degli Studi di Roma "Tor Vergata"
Ludovica Paseri
assegnista di ricerca di diritto amministrativo, Università degli Studi di Torino
Cesare Pinelli
professore ordinario di istituzioni di diritto pubblico, Sapienza - Università di Roma
Alberto Randazzo
professore associato di istituzioni di diritto pubblico, Università degli Studi di Messina
Marco Ventoruzzo
professore ordinario di diritto commerciale, Università Bocconi
Vincenzo Zeno Zencovich
professore ordinario di diritto privato comparato, Università degli Studi Roma Tre

CODICE ETICO

La **Rivista di diritto dei media** intende garantire la qualità dei contributi scientifici ivi pubblicati. A questo scopo, la direzione, il Comitato degli esperti per la valutazione e gli autori devono agire nel rispetto degli standard internazionali editoriali di carattere etico.

Autori: in sede di invio di un contributo, gli autori sono tenuti a fornire ogni informazione richiesta in base alla policy relativa alle submissions. Fornire informazioni fraudolente o dolosamente false o inesatte costituisce un comportamento contrario a etica. Gli autori garantiscono che i contributi costituiscono interamente opere originali, dando adeguatamente conto dei casi in cui il lavoro o i lavori di terzi sia/siano stati utilizzati. Qualsiasi forma di plagio deve ritenersi inaccettabile. Costituisce parimenti una condotta contraria a etica, oltre che una violazione della policy relativa alle submission, l'invio concomitante dello stesso manoscritto ad altre riviste. Eventuali co-autori devono essere al corrente della submission e approvare la versione finale del contributo prima della sua pubblicazione. Le rassegne di dottrina e giurisprudenza devono dare esaustivamente e accuratamente conto dello stato dell'arte.

Direzione: la direzione (ivi compresi direttori e vice-direttori) si impegna a effettuare la selezione dei contributi esclusivamente in base al relativo valore scientifico. I membri della direzione (ivi compresi direttori e vice-direttori) non potranno fare uso di alcuna delle informazioni acquisite per effetto del loro ruolo in assenza di un'esplicita autorizzazione da parte dell'autore o degli autori. La direzione è tenuta ad attivarsi prontamente nel caso qualsiasi questione etica sia portata alla sua attenzione o emerga in relazione a un contributo inviato per la valutazione ovvero pubblicato.

Comitato degli esperti della valutazione: i contributi sottoposti a valutazione costituiscono documentazione a carattere confidenziale per l'intera durata del processo. Le informazioni o idee acquisite confidenzialmente dai valutatori per effetto del processo di revisione non possono pertanto essere utilizzate per conseguire un vantaggio personale. Le valutazioni devono essere effettuate con profondità di analisi, fornendo commenti e suggerimenti che consentano agli autori di migliorare la qualità delle loro ricerche e dei rispettivi contributi. I revisori dovranno astenersi dal prendere in carico la valutazione di contributi relativi ad argomenti o questioni con i quali sono privi di familiarità e dovranno rispettare la tempistica del processo di valutazione. I revisori dovranno informare la direzione ed evitare di procedere alla valutazione nel caso di conflitto di interessi, derivante per esempio dall'esistenza di perduranti rapporti professionali con l'autore o la relativa istituzione accademica di affiliazione.

mediaLAWS

ANNO 2022 - CODICE ISSN 2532-9146