Raffaella Brighi*

Informatica forense, algoritmi e garanzie processuali

ENGLISH TITLE

Digital Forensics, Algorithms and Procedural Safeguards

ABSTRACT

The rationale behind the deployment of algorithms in judicial activities and, in particular, in the investigative field is to answer to the enquiries of a judge, prosecutor or any other legal professional. Legal professionals and computer scientists must understand the manifold challenges of the problem under scrutiny to identify the best solution, on the one hand, and, on the other hand, to put into question the above findings.

This article maps out the properties of the algorithms deployed in the field of digital forensics with the aim of detecting and analysing any potential digital evidence. The overarching needs are to monitor, understand and justify algorithms' outcomes. Thus, in view of factors that may render the algorithmic logic procedure less clear, the technical activity shall preserve digital evidence's usability in trials, in order to safeguard the guarantees of due process according to national and supranational constitutional rights.

KEYWORDS

Algorithm – Digital Forensics – Fair Trial – Computational Complexity – Explicability.

1. L'informatica forense e il contesto di riferimento

L'informatica forense, in quanto area dell'informatica giuridica, si occupa della identificazione, acquisizione e analisi giudiziale del contenuto informativo di dispositivi e sistemi informatici. È dunque una scienza forense che, al pari di altre scienze (quali la medicina legale e la balistica forense), si è dappri-

* Professoressa associata in Informatica giuridica presso il Dipartimento di Giurisprudenza dell'Università di Bologna.

Ars Interpretandi, 1-2021, pp. 153-164

ISSN 1722-8352

ma proposta come scienza ausiliaria nel processo penale, per poi entrare oggi nella quasi totalità dei procedimenti giudiziari[1].

Le tecnologie informatiche possono coadiuvare polizia e autorità giudiziaria nelle indagini e contribuire, con strumenti sempre più efficaci, a una maggiore velocità, precisione e accuratezza della attività investigativa; tuttavia, nel contempo, possono comportare nuovi rischi per le persone e trasformare le indagini in "vere e proprie incursioni investigative" nel nucleo più intimo dell'individuo[2] con un ruolo spesso attivo e decisivo di attori privati. I diritti di proprietà intellettuale e le nuove forme di Intelligenza Artificiale (IA) possono inoltre rendere difficile il controllo e la verifica del *modus operandi* degli strumenti forensi che dovrebbero supportare il processo decisionale umano. È noto come si siano attribuite alla prova informatica qualità di intrinseca oggettività senza considerarne le caratteristiche di alterabilità, volatilità e intangibilità.

Le attività informatico forensi devono affrontare la complessità dei sistemi attuali: sorgenti di dati sempre più ampie ed eterogenee, architetture distribuite, nuove sofisticate forme di attacco, ubiquità degli spazi di archiviazione. Le sorgenti digitali possono contenere informazioni parziali, incomplete o ambigue rispetto all'ambiente che, solo combinate con altri dati, diventano elementi di prova in dibattimento. Nelle diverse fasi del trattamento delle potenziali prove, programmi informatici specifici (algoritmi e strutture dati) supportano l'investigatore, o più in generale l'esperto informatico forense, nelle operazioni più lunghe e laboriose e, soprattutto, nell'individuare e ricostruire, a partire da dati grezzi, informazioni rilevanti per il processo.

La prospettiva dell'attività tecnica, in questo contesto, è quella della *utilizzabilità* in dibattimento – a disposizione di tutte le parti processuali per la valutazione di ogni aspetto rilevante – a garanzia dell'esercizio del diritto di difesa e a tutela dei diritti fondamentali dei soggetti coinvolti. Ogni operazione manuale o automatizzata dovrebbe dunque essere condotta salvaguardando i requisiti tecnici di verificabilità; ripetibilità; riproducibilità e giustificabilità[3]. Tutte le parti coinvolte nel processo devono poter valutare se sono stati seguiti metodi scientifici e appropriati ed essere in grado di eseguire i processi descritti nella documentazione giungendo ai medesimi risultati; l'informatico forense dovrà essere in grado di giustificare azioni e metodi utilizzati e di aver operato le scelte migliori possibili.

Grazie alla diffusione di standard tecnici e buone pratiche, alla ratifica da parte degli Stati delle iniziative internazionali di contrasto al cibercrimine e,

1. Pollit (2010) ricostruisce la storia della disciplina. Per l'inquadramento dei principi e metodi dell'informatica forense in Italia si vedano, tra tutti, Maioli (2004, 2015).

2. Orlandi, 2018.

3. Requisiti fissati dalle norme tecniche di riferimento e in particolare dalla ISO 27037.

non da ultimo, alla definizione della cornice epistemologica per le scienze forensi di riferimento, si è raggiunta una maggior attenzione al tema della prova informatica nelle aule di giustizia[4]. Nel contesto europeo, soprattutto in ambito penale, importanti basi normative per la disciplina della prova scientifica nei momenti della ammissione, dell'assunzione e dell'utilizzazione dell'elemento di prova contribuiscono a definire il ruolo della scienza nel processo; inoltre, diverse sentenze fissano criteri per la validazione del sapere scientifico non consolidato. Il consulente informatico forense non si sostituisce al giudice, ma deve fornirgli tutti gli strumenti affinché possa formulare un giudizio analitico e rigoroso su quanto prodotto. In particolare, l'obbligo di motivazione della decisione appare determinante, in quanto garantisce la funzione autonoma del giudice rispetto all'esperto, sostenendo l'esigenza di un "controllo razionale"[5].

L'informatica forense è dunque un interessante terreno di intersezione tra diritto e informatica, dove la centralità dell'algoritmo nei processi di individuazione e analisi delle potenziali prove informatiche si coniuga con la necessità di controllare, comprendere e giustificarne gli esiti.

2. Algoritmi e risoluzione dei problemi

La finalità degli algoritmi nell'attività giudiziaria è quella di rispondere a una precisa esigenza investigativa espressa attraverso il quesito di un giudice, di un pubblico ministero o di altri professionisti del diritto. La comprensione da parte di entrambi i gruppi, giuristi e informatici, dello scenario di riferimento, del linguaggio, della logica di funzionamento e dei termini del problema è imprescindibile per trovare la soluzione migliore e per poterne mettere in discussione gli esiti.

A seconda del problema che si vuole risolvere possono essere definiti, di norma, algoritmi diversi. Più in generale si osserva che l'algoritmo – il testo contenente una sequenza ordinata e finita di passi, ripetibili, che se eseguita con determinati dati in ingresso produce in uscita la soluzione di una classe di problemi – non presenta elementi di ambiguità e aleatorietà ed è perfettamente leggibile come pure lo è, conoscendo il linguaggio di programmazione, la conseguente codifica dell'algoritmo nella sua veste formale, il programma.

I problemi, che si cerca di risolvere in modo automatico, sono riconducibili a tre categorie[6]: problemi per i quali sono al momento noti un certo numero

4. Brighi, Maioli, 2015.

5. Cass. pen., sez. II, 9 dicembre 2010, n. 43789. Prima di questa sentenza, che accoglie i "Criteri Daubert" in merito alla prova scientifica, in Italia non erano forniti al giudice criteri espressi per valutare l'ammissibilità di questo tipo di prove.

6. Harel, 1987.

di algoritmi risolutivi; problemi per i quali è noto che non esistono algoritmi risolutivi; problemi per i quali non si sa se esistano o meno algoritmi risolutivi. Ad ogni algoritmo è associata la *classe di complessità* che attiene al tempo e alla memoria occorrente perché il programma che lo esegue pervenga alla risoluzione del problema[7]. Dal punto di vista della risolubilità pratica sono considerati: buoni, i problemi il cui limite superiore di tempo di esecuzione è una funzione polinomiale (P); cattivi, i problemi il cui limite superiore di tempo di esecuzione è una funzione non polinomiale; indecidibili, i problemi su cui non si sanno fornire soluzioni.

I problemi algoritmici indecidibili si dicono anche *non computabili*; gli altri, indipendentemente dalla complessità, si dicono *computabili*. I problemi per cui esiste una soluzione algoritmica buona si dicono *trattabili*; sono detti *intrattabili* i problemi indecidibili e quelli le cui uniche soluzioni ammissibili sono di tipo cattivo. Una volta che si è dimostrato che un problema è indecidibile non può esistere un linguaggio di programmazione recente o una architettura di elaborazione con prestazioni potenti per potere trovare soluzioni; analogamente è molto bene definito l'insieme dei problemi algoritmici computabili, siano essi effettivamente risolubili o decidibili[8]. Come è noto, le limitazioni alla computazione paradossalmente sono state alla base della implementazione di strumenti per dare garanzie agli utilizzatori, come la crittografia a chiave pubblica o la *dimostrazione a conoscenza zero*[9].

Nel rispondere a un quesito specifico deve essere individuata una soluzione cui corrisponda un algoritmo trattabile. La supposizione che la forza bruta di un computer possa risolvere qualunque problema opportunamente codificato in programma e la mancata comprensione dei meccanismi algoritmici può portare alla sopravalutazione delle capacità delle macchine.

Un ruolo importante nella classificazione degli algoritmi ha il concetto della *riducibilità*, intesa come possibilità di collegare la ipotetica soluzione di un problema indecidibile a problemi *equivalenti* della stessa classe. Nel caso di quesiti che non siano risolubili in tempi compatibili con l'applicazione, se non per piccole istanze dei dati input, al fine di produrre risultati utili in giudizio può essere valutata l'ipotesi di ridurre il problema ricorrendo ad algoritmi

7. Si valuta l'ordine di grandezza della lunghezza (in termini di numero di operazioni) del processo di esecuzione al crescere dell'ampiezza dell'input, ossia degli N dati inseriti. Se il tempo di esecuzione rimane costante all'aumentare di N la complessità si definisce *costante*; se cresce in modo proporzionale a N la complessità è *lineare*; se aumenta di un fattore, o una combinazione di fattori, che sono esponenti di N (N^k) la complessità è *polinomiale* (P); se aumenta "di molto", in quanto N è all'esponente si definisce che la complessità è *esponenziale* 2^N, N^N o anche fattoriale di N (N!).

8. È la nota tesi di Church-Turing, individuata quasi contemporaneamente da più studiosi, tra il 1930 e 1940, che adottarono formalismi diversi per indagare la computabilità-calcolabilità effettiva degli algoritmi (Trakhtenbrot, 1964).

9. Utilizzate di recente nei sistemi *blockchain* (Li *et al*., 2020).

approssimati. Si introduce un arbitrio, un "oracolo", che rompe il determinismo della soluzione esaustiva e di conseguenza la complessità dell'algoritmo acquisita un limite inferiore polinomiale, una sorta di approssimazione della soluzione che riduce la quantità di calcoli da eseguire. Quei problemi che si adattano alla nuova classe di complessità, divenendo trattabili, si dicono NP-completi (Non-deterministico Polinomiale)[10].

Nella attività forense, non sono infrequenti casi giudiziari in cui il quesito è mal posto dal giudice o si debbano affrontare problemi con complessità alte, a fronte dei quali si ricorre a soluzioni approssimate che dovranno essere giustificate, pesate e valutate. Tali scenari mostrano quanto siano strategici formazione e dialogo tra le discipline, perché ciascuno dei due gruppi, scienziati forensi e operatori del diritto, possa avere una comprensione delle necessità e dei limiti dell'altro.

Numerosi algoritmi verificabili, ripetibili e riproducibili vengono impiegati a supporto delle attività investigative come: il calcolo dell'*hash* di un *file*[11], preliminare a molte operazioni forensi; l'individuazione in una rete *Peer to Peer* di *file* – da confrontare con una lista di *hash* di *file* noti come illeciti alla Autorità Giudiziaria – estraendo indirizzi IP, date e orari di caricamento e scaricamento[12]; il rilevamento di tutte le occorrenze di uno o più specifici *pattern* in un testo (problemi di *pattern matching*)[13], fino a problemi più complicati quali l'associazione del nome e tipo originario a *file* recuperati *da hard disk* danneggiati[14].

In tutti questi casi l'istanza del problema è perfettamente nota, il problema è trattabile e risolubile.

3. (segue) opacità dell'algoritmo

Il programma informatico è la formulazione per l'elaboratore della soluzione al problema mediante regole decisionali descritte dal programmatore associate ad algoritmi noti e validati dalla comunità scientifica; ciascun criterio di scelta che contribuisca alla soluzione, ciascuna approssimazione o riduzione del problema è operata da chi lo definisce e progetta; il suo contenuto e le strutture dati su cui opera sono la rappresentazione del mondo attraverso le categorie ontologiche del programmatore, compresi i suoi pregiudizi e le sue aspettative.

10. Alla classe NP appartengono molti algoritmi di riconoscimento, decisione e ottimizzazione.

11. Maioli, 2015.

12. Ferrazzano, 2018.

13. Brighi *et al.*, 2008.

14. In Costantini *et al.* (2019) si propone una soluzione in cui il problema è ricondotto a quello dei "matrimoni stabili" o degli abbinamenti stabili.

Che i programmi informatici non siano neutrali, in quanto espressione di un pensiero umano, è un orientamento consolidato[15]. Essi sono soggetti ad errori e vulnerabilità ma, negli esempi fin qui illustrati, esistono solide procedure e metodologie di sviluppo per controllare e anche correggere le azioni compiute da un software. La documentazione tecnica e la disponibilità del codice sorgente sono prerequisiti fondamentali per la verificabilità e la salvaguardia di quei criteri di trasparenza e controllo ribaditi anche da recenti sentenze rese su casi in cui la decisione finale era stata affidata ad un algoritmo[16].

Se da un lato si incoraggia l'utilizzo di una procedura informatica che conduca direttamente alla decisione finale, evidenziandone numerosi vantaggi quali la notevole riduzione della tempistica procedimentale, l'esclusione di interferenze del funzionario (essere umano) e la conseguente maggior garanzia di imparzialità della decisione automatizzata, d'altro lato si ribadisce la 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[17].

Al di là delle osservazioni giurisprudenziali, va ricordato che il diritto alla conoscibilità del processo decisionale automatizzato è un tema centrale nel Regolamento Generale sulla Protezione dei Dati (UE/2016/679), soprattutto quando gli esiti prodotti dagli algoritmi hanno il compito di decidere in maniera completamente autonoma producendo effetti giuridici sull'interessato o incidendo significativamente sulla sua persona[18].

Quando vi è l'impossibilità di comprendere il processo logico-algoritmico si dice che il sistema è opaco. L'opacità di un sistema può essere più o meno intenzionale e dovuta a diversi fattori. In primis un'opacità tecnica, legata alla complessità congenita di sistemi che richiedono un alto grado di specializza-

15. Già nel 1976 Weizenbaum rilevava come: (*i*) il computer segua la logica che gli abbiamo dato e "tale logica può portare a conseguenze molto diverse rispetto ai processi mentali contaminati dal desiderio di raggiungere determinati risultati"; (*ii*) molte persone abbiano difetti nel formalizzare procedure di cui hanno piena conoscenza e "il nostro potere predittivo, per quanto grande e affidabile, talora si basa su intuizioni che semplicemente non siamo in grado di spiegare adeguatamente" (Weizenbaum, 1976, p. 65). Sul punto, tra gli altri, Romeo (2020).

16. In Italia la questione dell'opacità degli algoritmi di *Decision Making* è stata affrontata per la prima volta nel 2017 dal TAR Lazio nel c.d. caso buona scuola. Tar Lazio, sez. III bis, n. 3769 del 2017; e TAR Lazio, sez. III bis, n. 9224-9230 del 2018. Sul punto anche la sezione Lavoro del Tribunale di Bologna in una sentenza del 31 dicembre 2020 rivolta ai criteri discriminatori definiti (dall'azienda) nell'algoritmo di *ranking* reputazionale della piattaforma *Deliveroo*.

17. Così il Consiglio di Stato, sentenza n. 2270 del 2019.

18. Palmirani, 2020. In particolare, l'art. 22, par. 3 del GDPR prevede che siano attuate misure appropriate a garantire all'interessato il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

zione e la capacità di rendere comprensibile (non solo conoscibile) la logica utilizzata dal programma. Il grado di opacità dell'algoritmo, come si chiarirà in seguito, può aumentare quando si entra nel perimetro delle intelligenze artificiali: dai *Rule-based System*, dove la conoscenza del problema è codificata in regole logiche dal programmatore, che presentano un bassissimo grado di opacità fino alle *Neural Network*, caratterizzate da un approccio *data-driven*, che, soprattutto nella versione *Deep Neural Network* (DNN), sono estremamente opache. Opacità possono essere legate anche ad impedimenti di natura giuridica, quali la natura dei dati coinvolti, la tutela di segreti industriali e della proprietà intellettuale, tra cui i diritti d'autore sul software[19], o ancora a ragioni di sicurezza. Infine, intenti manipolatori o di elusione di norme vigenti possano contribuire a opacità intenzionali.

Il principio di trasparenza, invocato spesso come soluzione, non sempre è di facile applicazione. Nel contesto dell'informatica forense, in cui i sistemi informatici sono coinvolti nella formulazione di decisioni giudiziarie, l'assenza di trasparenza può condurre alla lesione del diritto di ricevere la motivazione della decisione, o della possibilità generale di controllo sulla sentenza[20]. La trasparenza, inoltre, è un valore per gli stessi programmatori e ricercatori, qualora intendano comprendere e migliorare il loro sistema.

4. Intelligenza artificiale per l'informatica forense

Negli ultimi anni, come è noto, lo sviluppo dei sistemi di IA ha avuto un forte impulso, grazie in particolare all'approccio data-driven favorito da hardware sempre più potente, algoritmi sofisticati e da fattori quali *Big Data*, l'*Internet of Things* (IoT) o il *Cloud Computing*[21]. Numerose iniziative e, soprattutto, i molteplici interventi dell'UE[22] sono il segnale che non manca la consapevolezza dei rischi legati all'uso dell'IA in ogni ambito della società, non da ultimo nei sistemi giudiziari[23].

Le direttrici per l'applicazione di tecniche di IA all'informatica forense, tracciate dalle ricerche più recenti, sono sostanzialmente due. La prima linea riguarda l'automazione delle diverse fasi di trattamento delle potenziali prove informatiche, dall'individuazione all'analisi dei dati, tra cui: algoritmi per

19. Di fronte a diritti costituzionalmente sanciti, quali il diritto di difesa, il diritto di proprietà intellettuale appare tuttavia destinato a cedere il passo.

20. In tal senso, il caso Loomis, relativo all'uso del sistema COMPAS per il calcolo della probabilità di recidiva, è un caso che ha fatto scuola (Contissa *et al*., 2019).

21. Marmo, 2020.

22. Zanichelli, 2021.

23. Consiglio d'Europa, (CEPEJ), European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment (2018).

estrarre informazioni da set di dati complessi, identificazione e individuazione di elementi (persone, oggetti, volti) in immagini e video, estrazione di segnali da tracce audio, analisi del linguaggio naturale e classificazione dei contenuti crittografati[24]. La seconda linea ha l'obiettivo di guidare l'esperto nelle fasi di valutazione dei potenziali elementi di prova attraverso l'interpretazione di fatti noti integrando e correlando le diverse tracce trovate, riguarda quindi sistemi di supporto alle decisioni per formare ipotesi o confrontare ipotesi alternative e sistemi per la condivisione delle informazioni sulle prove e sulle operazioni svolte (*chain of custody*).

L'informatica forense deve affrontare sfide sempre maggiori per esaminare frammenti di conoscenza da cui arrivare a trarre conclusioni sul caso mediante correlazione logico-deduttive, ma si è visto che i modelli teorici, da soli, sono inefficaci, perché difficilmente riescono a risolvere tutti i casi concreti e richiedono grandi sforzi di formalizzazione. Seguendo le classificazioni maggiormente condivise[25] nell'ambito della IA ricadono: sistemi di rappresentazione della conoscenza; sistemi per la descrizione e modellazione del ragionamento con diversi formalismi logici; sistemi di ragionamento basato sui casi (CBR); algoritmi di *pattern recognition*; sistemi di *knowledge discovery* e, infine, sistemi di apprendimento automatico (*machine learning*).

Il paradigma del *machine learning* (ML) in ambito giuridico – quindi anche in informatica forense dove l'esperto deve essere in grado di giustificare e spiegare ogni operazione – apre, tuttavia, alcuni scenari di criticità perché introduce modelli approssimati, non deterministici e basati su correlazioni statistiche che spesso non hanno una spiegazione causale. Nelle sue diverse declinazioni (supervisionato, non supervisionato e rinforzato) il ML comprende una serie di tecniche, tra cui le reti neurali, cui corrispondono diversi livelli di trasparenza e controllo, fino alle DNN in cui i parametri in gioco diventano talmente tanti per cui la spiegazione non è più intuitiva. D'altra parte, per alcuni contesti applicativi le DNN sono molto utili e più efficienti dell'umano.

Opinione generalmente riconosciuta tra gli studiosi di intelligenza artificiale per il diritto[26] è che, per avere soluzioni efficaci nel dominio giuridico, si debbano combinare tecniche per la modellazione logica esplicita della conoscenza e del ragionamento con tecniche di apprendimento automatico, orientandosi verso uno standard debole di IA che consenta all'essere umano di mantenere il controllo della macchina[27].

24. Diversi prodotti professionali propongono per tali operazioni, già oggi, soluzioni basate su IA.

25. Russell, Norvig, 2009.

26. Sartor, 2016.

27. Canzio, 2021.

La *spiegabilità*[28] resta un elemento importante, in particolare in ambito legale-giudiziario: la spiegazione consente di comprendere, anticipare, valutare e contestare; preserva la capacità di decidere e impedisce che si deleghi la decisione all'algoritmo. La mancanza di controllo e trasparenza dei sistemi impiegati si scontra con i requisiti che devono essere garantiti nel trattamento della prova informatica e precludono la possibilità di verificare se ci siano state alterazioni nei dati. I sistemi di IA possono commettere errori, essere attaccati dall'esterno, o incorporare pregiudizi. Un esempio tra tutti è l'automazione del processo di identificazione e di attribuzione dell'età della vittima nei casi di pedopornografia, di grande utilità per l'informatica forense, dove le difficoltà tecniche si scontrano con la necessità di ricostruire il percorso logico in modo da rendere conto dei risultati dello strumento[29].

A fronte della pervasività dei sistemi odierni, si ravvisa inoltre la tendenza delle indagini informatiche ad assumere un carattere di proattività volto, più che alla repressione, all'esplorazione dei dati per la ricerca di notizie di reato.

Occorre dunque riflettere su quali debbano essere le modalità di ingresso nel processo di elementi di prova ricostruiti con le nuove tecniche di IA e quale sia la loro utilizzabilità dibattimentale; fondamentale, naturalmente, è elaborare un forte sistema di garanzie in un'ottica di bilanciamento delle opposte esigenze.

5. CONCLUSIONI

Nel settore giudiziario, in cui la penetrazione delle tecnologie dell'informazione e della comunicazione è iniziata in ritardo rispetto ad altri settori, le aree del diritto penale e della procedura penale e della informatica forense, dove sono consolidate le prove scientifiche, sono quelle più in contatto con algoritmi e sistemi informatici.

La definizione di standard tecnici e buone pratiche ha portato nell'ultima decade a un maggior rigore scientifico nel ricorso all'informatica, stante il ruolo del giudice-*gatekeeper* cui si chiede di comprendere i presupposti di validità del metodo presentato e, su queste basi, di formulare la propria decisione autonoma. Tuttavia, gli aspetti della verificabilità *ex post* e del controllo tecnico del *software*, per accertare che il funzionamento corrisponda a quanto dichiarato, non rientrano nell'attuale assetto normativo che non prevede fasi di approvazione dei programmi informatici impiegati dagli organi competenti. La *certificazione* e la convalida potrebbero invece contribuire a rafforzare la fiducia nell'uso di tali tecnologie, sulla traccia di quanto avviene in materia di

28. Floridi *et al*., 2018.
29. Brighi *et al*., 2020.

sicurezza informatica dove il legislatore europeo[30] ha avviato la definizione di processi di certificazione del *software* da enti indipendenti per garantirne specifiche caratteristiche.

La comunità scientifica, peraltro, mostra grande attenzione al tema della *spiegabilità* delle IA, percepito anche dai tecnici come essenziale; diversi progetti di ricerca affrontano il problema della progettazione di sistemi di IA secondo un paradigma di *explanation by design*[31]. Un'adeguata *spiegabilità*, *ex ante* ed *ex post,* è garantita dalla conoscibilità, non solo dei modelli matematici e informatici e dell'implementazione tecnica, ma anche dei dati di *training*, di sviluppo, di *testing* e di contesto su cui è basata la decisione automatica[32]. Per scenari complessi, dove si individuano più livelli di *spiegabilità*, si stanno studiando strumenti capaci di dare accesso a algoritmi e strutture dati in forma comprensibile e dinamica, con l'aiuto per esempio di grafi della conoscenza e moduli di *question answering*.

Tre punti ulteriori emergono dalle riflessioni sull'impiego di sistemi automatizzati in supporto alle decisioni nel campo penale[33]. Il primo punto riguarda il ruolo dell'argomentazione giuridica a fronte della "purificazione dell'approssimato linguaggio naturale"[34] utilizzato nel mondo del diritto a opera del linguaggio algoritmico, chiaro e inequivocabile. Il secondo punto, la constatazione di una "fattualizzazione"[35] del diritto informatico, ossia un appiattimento del diritto tra tanti fatti e precedenti giurisprudenziali, per la maggior reattività dei sistemi di IA al fenomeno piuttosto che al ragionamento giuridico. Il terzo punto, infine, come l'impiego dei sistemi automatici possano piegare l'orientamento della scelta nel dubbio interpretativo, se *pro reo* o *pro repubblica*.

L'interpretazione giuridica quasi sempre ammette una pluralità di risultati alternativi plausibili, razionalmente fondati, tra i quali è necessario individuarne uno esplicitando le ragioni di questa scelta. In linea con gli studi sugli algoritmi *equitativi*, che guardano al futuro piuttosto che riproporre l'orientamento del passato[36], il sistema automatico potrebbe essere impostato per scegliere non l'interpretazione "più probabile che non" ma quella più favorevole all'imputato, ottimizzando il sistema anche in termini valoriali[37].

30. Regolamento (EU) 2019/881 (Cybersecurity Act).

31. XAI – Science and technology for the eXplanation of AI decision making (https://xai-project.eu).

32. Palmirani, 2020, p. 87.

33. Sul punto Caterini, 2020.

34. Ivi, p. 7.

35. Ivi, p. 13.

36. Algoritmi che possono proporre alle parti risultati che meglio soddisfino le istanze di cui sono portatrici secondo un equo bilanciamento piuttosto che scegliere in base a criteri probabilistici (Romeo, 2020, p. 120).

37. Sartor, 2020.

Non si intende con ciò escludere il giudice dal processo decisorio: le garanzie processuali, connaturate anche alla motivazione della sentenza, impongono all'essere umano di mantenere un "controllo significativo"[38] del sistema informativo.

Per assicurare la opportuna flessibilità del sistema processuale, con l'apporto della scienza nella ricerca della verità, i criteri della sentenza di Dubert del 1993, rafforzati dalla succitata Cassazione del 2010, l'art. 189 c.p.p. che porta a vagliare criticamente gli elementi di prova per "assicurare l'accertamento dei fatti" e, importante, senza che venga pregiudicata "la libertà morale delle persone", stabiliscono come il giudice debba esaminare l'affidabilità di un metodo o di periti e consulente tecnici.

Usando le parole di Canzio: "la professionalità, l'etica e l'implementazione del grado di expertise accumulata dal giudice nell'utilizzo delle tecniche inferenziali del ragionamento e nella verifica degli schemi statistico-probabilistici, acquisiti con l'ausilio della tecnologia digitale, di software informatici e algoritmi predittivi o con l'apporto della informatica e della logica dell'IA, potrebbero certamente contribuire a restituire al funzionamento della giustizia penale una più adeguata immagine di efficacia e qualità".

RIFERIMENTI BIBLIOGRAFICI

Brighi, R., Ferrazzano, M., Summa, L. (2020). Legal Issues in AI Forensics: Understanding the Importance of Humanware. *I-Lex. Scienze Giuridiche, Scienze Cognitive e Intelligenza Artificiale*, 13(I).

Brighi, R., Lesmo, L., Mazzei, A., Palmirani, M., Radicioni, D. (2008). Towards Semantic Interpretation of Legal Modifications through Deep Syntactic Analysis. In *Legal Knowledge and Information Systems* (pp. 202-206). IOS Press.

Brighi, R., Maioli, C. (2015). Un cambio di paradigma nelle scienze forensi. Dall'armonizzazione tecnico-giuridica a una nuova cornice epistemologica. *Informatica e diritto*, XXIV(1-2), 217-234.

Canzio, G. (2021). Intelligenza artificiale, algoritmi e giustizia penale. *Sistema Penale*, https://www.sistemapenale.it.

Caterini, E. (2020). Il giudice penale robot. *La legislazione penale*, https://www.lalegislazionepenale.eu.

Contissa, G., Lasagni, G., Sartor, G. (2019). Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo. *Diritto di Internet*, 4, 619-634.

Costantini, S., De Gasperis, G., Olivieri, R. (2019). Digital Forensics and Investigations Meet Artificial Intelligence. *Annals of Mathematics and Artificial Intelligence*, 86,193-229.

38. Ubertis, 2020.

Di Giovine, O. (2020). Il "judge-bot" e le sequenze giuridiche in materia penale. *Cassazione Penale*, 952-953.

Ferrazzano, M. (2018). *Aspetti metodologici, giuridici e tecnici nel trattamento di reperti informatici nei casi di pedopornografia*. Aracne.

Floridi, L. *et al.* (2018). An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*, 28(4), 689-707.

Harel, D. (1987). *Algorithmics: The Spirit of Computing*. Addison-Wesley.

Li, W. *et al.* (2020). *Privacy-Preserving Traffic Management: A Blockchain and Zero-Knowledge Proof Inspired Approach*. IEEE Access, DOI: 10.1109/access.2020.3028189.

Maioli, C. (2004). Introduzione all'informatica forense. In P. Pozzi (cur.), *La sicurezza preventiva dell'informazione e della comunicazione. Sicurezza delle informazioni*. Franco Angeli.

Maioli, C., cur. (2015). *Questioni di informatica forense*. Aracne.

Marmo, R. (2020). *Algoritmi per l'intelligenza artificiale. Progettazione dell'algoritmo, dati e machine learning, neural network, deep learning*. Hoepli.

Orlandi, R. (2018). Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma. *Riv. it. dir. proc. pen*., 2, 538-556.

Palmirani, M. (2020). Big Data e conoscenza. *Rivista Italiana di Filosofia del diritto*, IX(1),73-92.

Pollitt, M. (2010). A History of Digital Forensics. In *Advances in Digital Forensics* (6th ed., pp. 3-15). Springer.

Romeo, F. (2020). Giustizia e predittività. Un percorso dal machine learning al concetto di diritto. *Rivista italiana di Filosofia del diritto*, IX(1), pp. 195-124.

Russell, S., Norvig, P. (2009). *Artificial Intelligence: A Modern Approach*. Prentice Hall Press.

Sartor, G. (2016). *L'informatica giuridica e le tecnologie dell'informazione*. Giappichelli.

Sartor, G. (2020). Artificial Intelligence and Human Rights: Between Law and Ethics. *Maastricht Journal of European and Comparative Law*, 27, 705-719.

Trakhtenbrot, A. (1964). *Algoritmi e macchine calcolatrici automatiche*. Progresso Tecnico Editoriale.

Ubertis, G. (2020). Intelligenza artificiale, giustizia penale, controllo umano significativo. *Sistema penale*, https://sistemapenale.it.

Weizenbaum, J. (1976). *Computer Power and Human Reason: From Judgment to Calculation*. W.H. Freeman and Company.

Zanichelli, M. (2021). Ecosistemi, opacità, autonomia: le sfide dell'intelligenza artificiale in alcune proposte recenti della Commissione europea. In A. D'Aloia (cur.), *Intelligenza artificiale e diritto. Come regolare un 'mondo nuovo'* (pp. 9-29). Franco Angeli.