



**INFORMATICA GIURIDICA**  
Collana diretta da Giovanni Ziccardi e Pierluigi Perri

14

Monica Palmirani - Salvatore Sapienza  
(a cura di)

# **La trasformazione digitale della giustizia nel dialogo tra discipline**

Diritto e Intelligenza Artificiale

Prefazione di Marta Cartabia

## PREFAZIONE

Gli sviluppi vorticosi della tecnologia stanno trasformando, anzi, hanno già trasformato, in profondità la trama delle nostre esistenze personali, professionali e sociali, tanto da segnare — secondo alcuni — l’inizio di una nuova era nella storia dell’umanità. L’Intelligenza Artificiale (AI) è una componente centrale di questa trasformazione, come si evince dal fiorire di dibattiti, riflessioni e ricerche, libri, seminari e convegni, che si interrogano intorno alle potenzialità e ai pericoli dell’AI.

Il giurista non può esimersi dal misurarsi con gli interrogativi suscitati dagli sviluppi dell’AI, almeno lungo due direttrici.

La prima è quella della regolazione dei sistemi di intelligenza artificiale.

La seconda è quella della possibile applicazione dei sistemi di intelligenza artificiale nel mondo del diritto e in particolare nell’amministrazione della giustizia.

Il volume *La Trasformazione Digitale della Giustizia nel Dialogo tra discipline: Diritto e Intelligenza Artificiale* — curato da Monica Palmirani e Salvatore Sapienza — offre linee di riflessione lungo entrambe le direttrici, in un momento di particolare impegno del legislatore — almeno a livello europeo — nella regolazione dell’Intelligenza Artificiale, oltre che di profonda transizione in senso digitale dell’amministrazione del sistema giustizia in Italia, resa possibile anche dal piano di interventi e di investimenti finanziati dal PNRR.

Così, ad esempio, lungo la prima direttrice, il libro analizza e discute ampiamente la proposta di Regolamento del Parlamento europeo e del Consiglio dell’aprile 2021, meglio noto come *Artificial Intelligence Act*, il progetto più compiuto di regolazione del settore attualmente disponibile, basato sulla classificazione del rischio nei vari ambiti di applicazione.

Lungo la seconda direttrice, varie parti del libro prefigurano possibili applicazioni dell’AI al settore dell’amministrazione della giustizia e ne discutono potenzialità e limiti: si esplorano le possibilità di

utilizzo dell'AI nelle attività di anonimizzazione e pseudonimizzazione delle sentenze; ci si interroga sul contributo che l'AI può dare al contrasto alla criminalità organizzata da sempre basata sul coordinamento delle informazioni; e, ancora, si esaminano i problemi specifici che può comportare l'ingresso dell'intelligenza artificiale nell'ambito della giustizia civile, amministrativa e penale — dove il dibattito è stato segnato da casi particolarmente controversi per l'esposizione dei diritti della persona a gravi compressioni, come insegna la vicenda americana sfociata nella sentenza *Loomis vs Wisconsin* del 2016.

Gli autori del libro mostrano una piena consapevolezza dei rischi che l'ingresso di strumenti tecnologici così potenti come l'AI può comportare per i diritti della persona; e, tuttavia, li esaminano con metodo scientifico, senza lasciarsi sopraffare dall'impatto emotivo che alcune specifiche vicende inevitabilmente suscitano. *Né apocalittici né integrati*, si potrebbe dire degli Autori di questo volume, parafrasando il titolo di un famoso libro di Umberto Eco del 1964.

Del resto, è innegabile il potenziale contributo che il supporto della tecnologia può offrire al lavoro del giudice — anche in vista di una migliore gestione dell'organizzazione giudiziaria, di una improcrastinabile riduzione dei tempi del processo, del contenimento del rischio di errori e di maggiore armonizzazione degli orientamenti giurisprudenziali, senza che questi e altri benefici possano far velo ai pericoli che una delega inconsapevole dell'azione alla macchina può riversare sul piano della tutela dei diritti e delle garanzie: la titolarità dell'azione resta e deve sempre restare in capo all'attore umano, al quale viene affidato il governo degli strumenti dalla progettazione all'utilizzazione finale.

Per questo la domanda che attraversa il libro non è tanto *se* l'intelligenza artificiale possa o debba trovare spazio nel mondo della giustizia. La domanda è piuttosto *quale* modello di intelligenza artificiale sia in grado di mantenere l'essere umano al centro.

Gli autori si fanno carico della preoccupazione che, consapevolmente o inconsapevolmente, attraversa l'animo di molti — anzitutto di tutti gli operatori della giustizia — quando si ipotizza di consentire che l'intelligenza artificiale varchi le soglie dei palazzi di giustizia e penetri persino le pieghe dello svolgimento del processo. Questa preoccupazione può essere espressa con l'efficace interrogativo di T.S. Eliot: «Dov'è la conoscenza che abbiamo perduto nell'informazione? ».

L'intelligenza artificiale porta indiscutibilmente un incremento di informazione, attraverso il grande numero di dati che riesce a processare e alla sua capacità di autoapprendimento. Ma questo incremento

informativo è di per sé sintomo di una conoscenza più approfondita e accurata?

La ragione del giurista non può mai essere ridotta a mero calcolo. Tanto meno può esserlo quella del giudice. Occorre che ogni controversia possa essere valutata non solo *more geometrico*, ma con *esprit de finesse*, di cui solo la persona umana è dotata, per cogliere e valorizzare le uniche e irripetibili circostanze del singolo caso, al quale la decisione giudiziaria si applica.

Questa centralità della persona nel rapporto con la macchina — sostengono gli autori — deve essere preservata a vari livelli: sia quando l'essere umano interviene a progettare il sistema, sia quando è utente attivo del sistema, lo interroga e trae beneficio dalle sue elaborazioni, sia quando l'uomo è soggetto a decisioni che sono assunte da altri esseri umani supportati da sistemi dotati di autonomia funzionale, sia quando è parte attiva dello sviluppo dei modelli statistici tramite cui la macchina elabora la conoscenza giuridica. In conformità con questo *human centered approach*, raccomandato da tutte le fonti europee e internazionali, il volume esprime una chiara linea di pensiero che propone una metodologia informatico-giuridica — denominata *Hybrid Artificial Intelligence* — in grado di implementare, nel rispetto delle declinazioni dell'amministrazione della giustizia, uno sviluppo di sistemi di intelligenza artificiale che siano sempre sotto il controllo della persona umana, in un incessante dialogo iterativo e interattivo tra giuristi e macchine.

Un grande pensatore tedesco del secolo scorso, Romano Guardini, alla fine degli anni Venti scriveva: « Per poter renderci padroni del “nuovo”, dobbiamo in giusto modo penetrarlo. Dobbiamo dominare le forze scatenate onde farle attendere alla elaborazione di un ordine nuovo, che sia riferito all'uomo. [...] Non abbiamo bisogno di meno tecnologia, ma di più tecnologia. O meglio: ciò che ci occorre è una tecnica più forte, più ponderata, più “umana”. [...] In primo luogo, dunque: bisogna dire “sì” al nostro tempo. [...] Si avrà la soluzione soltanto andandola a cercare molto in profondità ». Perché questo accada, è dunque necessario che il cammino verso la “profondità” sia percorso con un impegno culturale corale che dica “sì” al nostro tempo, investendo prima di tutto sulla formazione delle donne e degli uomini che lo abitano, per sviluppare quel sapere critico che è il *proprium* insostituibile del “fattore umano”.

Milano, 22 dicembre 2022

Termine estratto capitolo

## CAPITOLO 1

**IL RUOLO DELL'INTELLIGENZA ARTIFICIALE  
NEL SISTEMA GIUSTIZIA:  
FUNZIONALITÀ, METODOLOGIE, PRINCIPI**di *Monica Palmirani, Salvatore Sapienza, Chantal Bompreszi*

**SOMMARIO:** 1.1. Considerazioni preliminari. — 1.2. Prospettive comparate: le esperienze extra-europee. — 1.2.1. Stati Uniti d'America. — 1.2.2. Repubblica Popolare Cinese. — 1.3. Prospettive comparate: le esperienze in Europa. — 1.4. Prospettive comparate: le esperienze in Italia. — 1.5. *L'Hybrid AI* applicata al settore giustizia: presupposti metodologici. — 1.6. (*Segue*) *L'Hybrid AI* applicata al settore giustizia: proposta metodologica.

**1.1. Considerazioni preliminari**

La progressiva diffusione dei sistemi di Intelligenza Artificiale in molti settori pubblici e privati pone la questione, tanto informatica, quanto giuridica, sulla potenziale adozione di questi sistemi nell'amministrazione della giustizia. Il dibattito sull'Intelligenza Artificiale si è a lungo concentrato sull'impatto di tale approccio computazionale sui diritti fondamentali degli individui, secondo una pluralità di prospettive giuridiche, informatiche, etiche, filosofiche, religiose. Una concordanza tra questa pluralità di vedute può essere identificata nella considerazione che la libertà personale e lo *status* giuridico degli individui possono essere oggetto di significative modifiche (o intrusioni) operate direttamente da sistemi di Intelligenza Artificiale (caso oggi invero raro), ovvero da esseri umani (giudici) che si servono di tali strumenti come ausilio del proprio processo decisionale.

Molti ambiti dell'amministrazione della giustizia possono utilizzare diverse tecniche della vasta costellazione della complessa ed interdisciplinare area dell'intelligenza artificiale. Per semplicità divideremo gli strumenti in simbolici, non-simbolici, sub-simbolici <sup>(1)</sup> e cercheremo di

---

<sup>(1)</sup> Per una panoramica, v. S. J. RUSSELL, P. NORVIG (2005), *Intelligenza artificiale. Un approccio moderno* (Vol. 1), Person Education Italia, Milano; F. COREA "AI

commentarne i possibili rischi e limiti per arrivare a identificare alcune soluzioni atte a mitigare le possibili lacune di ogni metodo.

• *Intelligenza Artificiale simbolica*. Nata negli anni '70, l'Intelligenza Artificiale simbolica si basa sulla formalizzazione del diritto mediante costrutti logico-matematici (e.g., ragionamento logico mediante la logica proposizionale, la *first order logic*, la logica *defeasible*, etc.) oppure mediante regole di ricorrenza (e.g., *regular expression* del linguaggio giuridico) oppure ancora mediante formalizzazione della conoscenza in formati deduttivi (e.g., ontologie formali). Queste tecniche sono molto dispendiose in termini di tempo ed energie che gli esperti del diritto devono impiegare per ottenere un buon prodotto finale. Inoltre, gli strumenti informatici (e.g., *engine reasoner*) hanno spesso problemi di scalabilità computazionale. Ciò significa, in pratica, che possono avere problemi nel fornire una risposta in tempi accettabili per l'utente quando applicati a grandi mole di regole (*knowledge base*). L'attendibilità di questa famiglia di strumenti, tuttavia, è piuttosto elevata perché sviluppata con processi cognitivi controllati da esperti e utilizzando modelli formali. Questi strumenti sono anche spiegabili nel loro comportamento potendo rispondere alle domande "perché si ottiene questo risultato" e "come si è ottenuto", onorando così la trasparenza e la conoscibilità del procedimento di ragionamento automatico e del conseguente risultato.

• *Intelligenza Artificiale non-simbolica*. Questa grande famiglia comprende moltissime tecniche, tutte fondate su modelli matematici statistico-probabilistici <sup>(2)</sup>. La loro accuratezza può essere anche molto elevata, ma la loro spiegabilità di processo e di risultato non sempre è raggiungibile proprio perché si tratta di correlazioni frequenziali o possibili senza un evidente nesso di causalità definito *ex ante*. Si tratta, infatti, di applicare un processo di interpretazione dei risultati *ex post* e di trovare una spiegazione semantica o fenomenologica rispetto ad un *goal* atteso. Solitamente il *goal* è trovare un modello matematico che correli dati di input e risultati di output per poi replicare tale modello a nuovi dati e quindi predire il risultato atteso. Si possono distinguere

---

Knowledge Map: how to classify AI technologies", in F. COREA, *An Introduction to Data 2019*, Springer, Cham, pp. 25-29. Per una ricostruzione storica, v. G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione: Corso di informatica giuridica*. Vol. 2, 2016, Giappichelli Editore, Milano, al cap. 6.2. Sui profili di regolamentazione, inclusa la definizione normativa di Intelligenza Artificiale, v. il Capitolo 3 di questo volume.

(2) V. *ex multis* M. I. JORDAN e T. M. MITCHELL, *Machine learning: Trends, perspectives, and prospects*. In *Science*, 2015, 349.6245: 255-260.

tecniche di apprendimento, come quelle supervisionate dagli esperti, i quali forniscono dati annotati agli algoritmi che imparano il modello sottostante, o quelle non supervisionate, secondo cui si chiede all'algoritmo di ricavare per induzione parametri qualificativi della realtà immessa tramite i dati. Vi sono anche tecniche intermedie, dette semi-supervisionate, per ridurre i tempi di annotazione da parte degli esperti, vale a dire la fase che crea maggior impegno di risorse umane e di dati. Un'ulteriore categoria è definita come *reinforcement learning* (apprendimento per rinforzo), in cui l'immissione di dati annotati avviene in una prima fase di modellazione, ma persiste anche durante l'utilizzo (e.g., *self-driving car systems*, assistenti vocali).

- *Intelligenza Artificiale sub-simbolica*. Nell'ambito della giustizia è bene ricordare che diversi diritti spesso devono essere bilanciati caso per caso. L'idea di utilizzare *multi-agent systems*, in cui più agenti intelligenti negoziano fra loro usando la teoria dell'argomentazione, è sicuramente un ambito in cui la ricerca sta investigando. Queste tecniche sono usate anche per mitigare rischi, *bias*, o per fornire una spiegabilità all'elaborazione non-simbolica. In questo ultimo caso, agenti intelligenti monitorano la parte non-simbolica e provano a fornire un'argomentazione.

- *Hybrid AI*: la c.d. Intelligenza Artificiale ibrida è quell'approccio che utilizza un mix delle tecniche sopra definite al fine di mitigare eventuali debolezze dell'uno e dell'altro metodo. In questo paradigma si sostanzia l'approccio metodologico proposto in chiusura di questo capitolo <sup>(3)</sup>.

Il presupposto dell'esistenza di una "giustizia automatizzata" è che ogni — o, più cautamente, qualche — componente dei processi decisionali che comunemente caratterizzano l'attività giudicante possa essere delegata agli algoritmi appena descritti. Tale *delegazione* implica che gli algoritmi siano dotati di un certo livello di autonomia funzionale <sup>(4)</sup>: maggiore è la capacità di un algoritmo di operare senza interazione con l'essere umana, maggiore sarà la complessità del com-

---

<sup>(3)</sup> V. *infra* § 1.5. e § 1.6.

<sup>(4)</sup> In generale, l'autonomia funzionale di una macchina può definirsi come quella condizione per cui non venga richiesta una costante supervisione da parte di un essere umano. In questo senso, un algoritmo dotato di autonomia funzionale può svolgere funzioni complesse in assenza di controllo. Per una prospettiva generale sulla delega agli algoritmi e sul tema dell'autonomia funzionale v. F. FOSSA, *Etica funzionale*,

pito che ad esso viene delegato. Viceversa, all’algoritmo non verrà delegato un processo decisionale, ma esso offrirà il suo *supporto* ad un operatore umano. Idealmente, l’intero processo decisionale del giudicante potrebbe essere delegato all’algoritmo. Ciononostante, questa possibilità sembra remota per la complessità del compito in questione, che richiede algoritmi ad alta autonomia funzionale. Più plausibili appaiono minori forme di delegazione o, più correttamente, di supporto all’operato dei giudicanti tramite frazioni del più complesso procedimento decisionario. In questi “frammenti di decisione”, algoritmi soggetti al controllo umano cooperano con il giudicante nello svolgimento di alcuni compiti.

Per illustrare queste possibilità, una breve ricostruzione dell’Intelligenza Artificiale applicata alla giustizia illustra il proliferare di nuove applicazioni, schematizzabili secondo le seguenti categorie tassonomiche <sup>(5)</sup>:

- Supporto al controllo di gestione: strumenti di supporto per la pianificazione e gestione utilizzando classici *tool* di ottimizzazione già utilizzati con successo in ambito aziendale. Un esempio è la gestione dei calendari di udienza nelle singole sedi giudiziarie mediante strumenti di ottimizzazione di spazi, risorse (staff) e gestione del tempo;

- Supporto alla pianificazione del *workflow* delle cause: mediante strumenti di Intelligenza Artificiale si possono soppesare i “pesi” delle cause partendo dai dati contenuti nei fascicoli di parte alla luce anche delle strategie che ogni presidente di ufficio giudiziario intende adottare e anche in relazione ai diversi riti (e.g., rito del lavoro), alle diverse norme di procedura civile e penale (e.g., improcedibilità nella Riforma Cartabia del 2018), alle priorità che ciascun territorio esprime (e.g., il c.d. “codice rosso”, frodi, fallimenti). Strumenti di simulazione, già impiegati con successo nel settore privato, possono trovare applicazione anche nel sistema giustizia per prospettare diverse opzioni orga-

---

in *Filosofia*, 2020, 65: 91-106. Tuttavia, va sottolineata anche l’esigenza di un “controllo umano significativo” avvertita dalla dottrina etica e giuridica (v. sul punto, § 3.3.2).

<sup>(5)</sup> V. *ex multis*, C. CASONATO, *Intelligenza artificiale e giustizia: potenzialità e rischi*. DPCE Online, 2020, 44(3); K.D. ASHLEY, *Artificial intelligence and legal analytics: new tools for law practice in the digital age*, Cambridge University Press, Cambridge, Regno Unito, 2020; si veda anche lo special issue “Artificial Intelligence for Justice” della rivista *Artificial Intelligence and Law* a cura di F. BEX, H. PRAKKEN, T. van ENGERS, B. VERHEIJ, E. TAVATTA, *Il processo di regolamento algoritmico e le applicazioni nel sistema giudiziario*. *Annali di Diritto dell’Intelligenza*

Termine estratto capitolo



## CAPITOLO 2

**ANONIMIZZAZIONE E PSEUDONIMIZZAZIONE  
DI SENTENZE GIUDIZIARIE**di *Monica Palmirani, Emanuela Podda*

**SOMMARIO:** 2.1. Il bilanciamento del diritto all'informazione giuridica e il diritto alla *privacy* nella pubblicazione delle sentenze giudiziarie. — 2.2. Dato giudiziario, dato personale e asimmetria del rischio identificativo. — 2.3. Il trattamento del dato giudiziario come dato personale relativo a sentenze giudiziarie. — 2.4. Modelli tipici di anonimizzazione per le sentenze giudiziarie: dati strutturati, semi-strutturati e non strutturati. — 2.5. La pseudonimizzazione: una questione aperta. — 2.6. Anonimizzazione e Pseudonimizzazione: Stati Membri a confronto. — 2.7. Conclusione.

**2.1. Il bilanciamento del diritto all'informazione giuridica e il diritto alla *privacy* nella pubblicazione delle sentenze giudiziarie**

Nei moderni ordinamenti giuridici la pubblicazione delle sentenze giudiziarie ha da sempre rappresentato uno strumento volto a garantire lo scrutinio pubblico dell'attività giudiziaria, nonché la conoscenza pubblica del diritto <sup>(1)</sup>. L'informatica giuridica assolve tale compito, elaborando automaticamente l'informazione giuridica, diffondendo il diritto e rendendolo conoscibile <sup>(2)</sup>.

L'incremento e lo sviluppo di tecnologie sempre più avanzate garantiscono non solo una superba organizzazione dell'informazione

---

<sup>(1)</sup> Commissione Europea, "Digitalisation of Justice", 2022, reperibile qui: [https://ec.europa.eu/info/policies/justice-and-fundamental-rights/digitalisation-justice\\_en](https://ec.europa.eu/info/policies/justice-and-fundamental-rights/digitalisation-justice_en). (ult. visita 05 Ottobre 2022). In tal senso, si vedano anche precedenti studi commissionati dal legislatore europeo in tal senso: M.V. OPIJNEN, G. PERUGINELLI, E. KEFALI, M. PALMIRANI, *On-line Publication of Court Decisions in the EU Report of the Policy Group of the Project. Building on the European Case Law Identifier*. Febbraio 2017, reperibile qui: <https://bo-ecli.eu/uploads/deliverables/Deliverable%20WS0-D1.pdf> ult. visita 05 Ottobre 2022).

<sup>(2)</sup> G. SARTOR, *L'Informatica giuridica e le tecnologie dell'informazione*, Torino, Giappichelli, 2016, p. 26-34.

stessa, ma anche l'estrazione di conoscenza a servizio e supporto delle più disparate attività, perfino nell'espletamento delle funzioni pubbliche.

Tuttavia, l'avvento di Internet, dei *big data* e delle moderne tecnologie dell'informazione ha messo in luce come la massiva diffusione dell'informazione possa spesso interferire con la vita delle persone, la loro riservatezza e *privacy*, imponendo un bilanciamento tra i principi coinvolti <sup>(3)</sup>.

Le sentenze giudiziarie sono, di fatto, foriere di dettagli sulla vita delle persone, nonché sul loro contesto di appartenenza.

L'embrionale definizione di *privacy* <sup>(4)</sup> sottolineava l'importanza di tale contesto nella valutazione e nel riconoscimento di questo diritto, fortemente legato agli sviluppi sociologici. Il tempo ne ha dimostrato la sua dipendenza anche da quelli economici e tecnologici. Tale contestualizzazione, difatti, ha inciso sul fulcro di riferimento del diritto stesso: dalla formula originaria del "diritto ad essere lasciato solo", si è passati all'autodeterminazione informativa <sup>(5)</sup> intesa come la libertà di mantenere il controllo sul flusso delle proprie informazioni. Da ultimo, a prendere gradualmente consapevolezza che tale libertà individuale subisce sempre più la fagocitante attitudine delle — sempre più — moderne tecnologie dell'informazione. Tale libertà risulta quindi fortemente impattata dalle attitudini e dalle *capacità tecnologiche* di ciascuno. *In primis*, perché il contesto attuale è caratterizzato dall'ipertrofia dell'informazione: mentre, in passato, il processo conoscitivo si fondava sulla ricerca delle informazioni, attualmente la tecnologia ha capovolto la prospettiva. Oggi è diventato determinante filtrarle; risulta sempre più semplice trovare informazioni personali nella c.d. *infosfera* <sup>(6)</sup>, diventando particolarmente difficile appurarne veridicità e attendibilità, con grande ripercussione sulla *privacy*, riservatezza e reputazione delle persone.

---

<sup>(3)</sup> M.V. OPIJNEN, *Court Decisions on the Internet; Development of a Legal Framework in Europe*, in *Journal of Law, Information & Science*, 2016, 2: 26-48.

<sup>(4)</sup> S.D. WARREN, L.D. BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, 1890, 4(5): p. 193-220.

<sup>(5)</sup> G. FINOCCHIARO, *Identità personale (diritto alla)*, in AA.VV. (a cura di), *Digesto delle Discipline Privatistiche*, Torino, Utet, 2010, p. 721-738. Il diritto alla protezione dei dati personali si estrinseca nella libertà positiva di esercitare un controllo sul flusso delle proprie informazioni.

<sup>(6)</sup> L. FLORIDI, *La Quarta Rivoluzione. Come L'infosfera Sta Trasformando Il Mondo*, Raffaello Cortina, Milano, 2017.

Indubbiamente, l'unico elemento incontrovertito, in dottrina quanto in giurisprudenza, è il dinamismo legato al diritto alla *privacy* e alla riservatezza. Questo sembra, infatti, non essere destinato a consolidarsi in un modello solido e univoco, quanto, piuttosto, in un concetto costantemente in evoluzione (7). Un contesto tecnologicamente meno sviluppato, sebbene meno innovativo e decisamente utopico, risulterebbe essere più garantista dal punto di vista della *privacy*. Tuttavia, la velocità e la *voracità* del mondo moderno pare non concedere benefici e/o deroghe in tal senso.

La prima relazione annuale del Presidente dell'Autorità Garante per la Protezione dei Dati Personali in Italia (8), dava conto proprio di questo dinamismo. Sottolineava il carattere trasversale del diritto alla *privacy*, attesa la necessità di garantire tutela in ogni settore della vita sociale, pubblica o privata, e in qualunque attività basata sul trattamento di dati personali.

Fin da allora emergeva che tale trasversalità, da una parte aumentava il grado di tutela della persona e dall'altra, si innestava con varie discipline di settore, in modo spesso problematico o addirittura conflittuale. È difatti indubbio che *privacy* e riservatezza possano subire deroghe e limitazioni — sebbene ispirate ai principi di proporzionalità, pertinenza e minimizzazione dei dati — in favore di altri principi costituzionali. Tra questi, *in primis*, i principi di pubblicità e trasparenza a corollario del principio democratico *ex art. 1 Cost.*, estesi a tutti gli aspetti rilevanti della vita pubblica e istituzionale. Anche ai sensi dell'art. 97 Cost. teso a garantire il buon funzionamento dell'amministrazione e dei dati che essa raccoglie e tratta. Non da ultimo, la piena conoscibilità del contenuto delle decisioni giudiziarie che non riguarda solo il diritto all'informazione nelle sue diverse componenti, *ex art. 21 Cost.*, ma come uno dei cardini del sistema costituzionale su cui si basa l'esercizio delle funzioni giudiziarie. Solo attraverso la motivazione (*P.Q.M.*) quale elemento necessario di ogni provvedimento giurisdizionale *ex art. 111 Cost.*, è possibile verificare la corretta amministrazione della giustizia, esercitata non solo nell'interesse delle parti processuali, ma anche nell'interesse di tutti cittadini.

---

(7) S. RODOTÀ, *Privacy in rete*, in *Parolechiave*, 2005, 34: 23-32.

(8) S. RODOTÀ, *Prefazione alla Relazione per l'anno 1997 del Garante per la protezione dei dati personali*, Roma, 1997, reperibile qui: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/3528995> (ult. visita 05 Ottobre 2022).

A tale scopo, nel definire il bilanciamento dei principi coinvolti nella pubblicazione delle sentenze giudiziarie, appare doveroso precisare che, in questo ambito, la tecnica legislativa utilizzata per circoscrivere le limitazioni del trattamento dei dati personali risulta discontinua <sup>(9)</sup>, complessa e frammentaria.

Sul quadro europeo rilevano diverse fonti. Anzitutto, la Direttiva (UE) 680/2016 contenente le norme generali per la protezione delle persone fisiche in relazione al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati. Inoltre, il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 Aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR).

La Direttiva è da intendersi *lex specialis* rispetto al Regolamento, in quanto normativa relativa al settore penalistico. Entrambe le fonti hanno poi dispiegato i loro effetti sul contesto giuridico italiano. Il recepimento della Direttiva ha portato all'emanazione del D.Lgs. 51/2018 che ha inciso, anch'esso, sul Codice della *Privacy*. Con l'entrata in vigore del Regolamento 2016/679 il legislatore italiano ha riscritto, attraverso il D.Lgs. 101/2018 (senza abrogare, se non in alcune disposizioni considerate incompatibili), il D.Lgs. 196/2003, *Codice in materia di protezione dei dati personali* (Codice della *Privacy*). In ultima battuta, sebbene aventi natura non vincolante, rilevano i pareri del Garante per la Protezione dei dati Personali. Tra questi, il Parere del 22 Febbraio 2018 finalizzato al recepimento della Direttiva e all'armonizzazione del quadro normativo che, tuttavia, non ha trovato alcun riscontro da parte del legislatore <sup>(10)</sup>.

---

<sup>(9)</sup> M. CARTABIA, *Le Norme sulla Privacy come Osservatorio sulle Tendenze Attuali delle Fonti del Diritto*, in M. G. LOSANO (a cura di), *La legge italiana sulla privacy: un bilancio dei primi cinque anni*, Roma, GLF editori Laterza, 2001.

<sup>(10)</sup> Si veda al riguardo il Parere 22 febbraio 2018 sullo schema di decreto legislativo recante *Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio*, finalizzato a consentire una collocazione sistematica delle norme in esame, nonché l'opportunità di un loro inserimento all'interno del Codice, reperibile qui: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/8005333> (ult. visita 05 Ottobre 2022). Si sottolineava, «l'esigenza della contestuale sostituzione degli articoli da 47 a 49 del Codice con i dispositivi di cui al presente decreto, nonché con altre relative disposizioni del Codice, in modo da assicurare l'unitarietà del sistema in

## CAPITOLO 3

**ALGORITHMIC JUSTICE E CLASSIFICAZIONE  
DI RISCHIO NELLA PROPOSTA AI ACT**di *Chantal Bomprezzi, Salvatore Sapienza* (\*)

**SOMMARIO:** 3.1. Considerazioni preliminari. — 3.2. Proposta *AI Act* e amministrazione della giustizia. — 3.2.1. Le attività di assistenza dei sistemi di IA all'autorità giudiziaria. — 3.2.2. I rischi derivanti dall'uso di sistemi di IA da parte dell'autorità giudiziaria. — 3.2.3. Una panoramica dei requisiti dei sistemi di IA di ausilio al giudice nella Proposta *AI Act*. — 3.3. Prime indicazioni sui requisiti di *compliance: data governance, human oversight, explainability*. — 3.3.1. La *Data Governance* e la gestione dei dati in ambito giudiziario. — 3.3.2. Il controllo umano (*human oversight*) nella decisione *AI-supported*. — 3.3.3. *Explicability, explainability* e obbligo di motivazione. — 3.4. Certificazione, standardizzazione, mercato e diritti. — 3.4.1. Standard tecnici e mercato. — 3.4.2. Il risultato algoritmico approssimato e la sua rilevanza in giudizio. — 3.4.3. I soggetti coinvolti nell'allocazione del rischio. — 3.5. *AI in e-Justice* e responsabilità. — 3.5.1. Responsabilità e Intelligenza Artificiale. — 3.5.2. La responsabilità civile del magistrato. — 3.5.3. Responsabilità contrattuale ed extra-contrattuale. — 3.6. Considerazioni finali.

**3.1. Considerazioni preliminari**

L'introduzione di sistemi di Intelligenza Artificiale (IA o AI) nel settore della giustizia è accompagnata da un rilevante novero di questioni etico-giuridiche causate da una molteplicità di fattori di rischio <sup>(1)</sup>. Se lasciate aperte, tali criticità possono rivelarsi determinanti nel prevenire l'adozione di sistemi di IA in grado di rendere più

---

(\*) Senza tradire l'unitarietà del lavoro, a C. Bomprezzi vanno attribuite le sezioni 3.2. (eccetto il par. 3.2.2., da attribuire anche a S. Sapienza), 3.5. e 3.6. (da attribuire anche a S. Sapienza) e a S. Sapienza le sezioni 3.1., 3.3. e 3.4. (eccetto il par. 3.4.3., da attribuire a C. Bomprezzi).

<sup>(1)</sup> Si veda, *ex multis*, A. PAJNO, M. BASSINI, G. De GREGORIO, M. MACCHIA, F. P. PATTI, O. POLLICINO, S. QUATTROCOLO, D. SIMEOLI, P. SIRENA, *AI: profili giuridici*.

efficiente il settore in questione. Risolvere questi dubbi si rende necessario al fine di raggiungere quella “AI Trustworthiness” <sup>(2)</sup> che caratterizza in maniera decisa l’operato normativo del legislatore europeo sul tema dell’IA.

Illustri studiosi e studiose hanno ampiamente dibattuto le modalità con cui l’adozione di sistemi AI nella giustizia possa dar luogo a rischi per i diritti e le libertà fondamentali degli individui. La discussione ha spesso preso spunto da casi pratici, come *Loomis* <sup>(3)</sup>, in cui un calcolo automatico della probabilità di recidiva di un individuo appartenente ad una minoranza etnica ha fatto emergere la possibile sussistenza di *bias* algoritmici sfavorevoli al suo rilascio in ragione della sua etnia <sup>(4)</sup>. Occorre tuttavia, a nostro avviso, andare al di là di un mero approccio episodico e concentrare le nostre riflessioni su una prospettiva olistica non solo capace di descrivere le criticità dell’impiego di sistemi di IA nella giustizia, ma anche di indagarne le cause tecniche e vagliare possibili soluzioni in chiave informatico-giuridica.

Nell’adottare questo metodo, la riflessione dovrà necessariamente tenere conto delle recenti proposte legislative sul tema e dei prossimi interventi normativi. In particolare, la Proposta per un *AI Act* formulata dalla Commissione Europea nell’Aprile 2021 <sup>(5)</sup> è un crocevia legislativo fondamentale nella regolamentazione dei sistemi AI in settori critici, compreso quello della giustizia.

La Proposta intende regolare sistemi di IA, definiti come quei software che, per un insieme di obiettivi definiti dagli esseri umani, generano output quali contenuti, predizioni, raccomandazioni o decisioni in grado di influenzare l’ambiente con cui interagiscono. Per restringere il campo di applicazione della Proposta, i sistemi soggetti alla normazione devono anche adottare una o più delle tecniche e degli approcci descritti nell’Allegato I, il quale ricomprende un ampio

---

*Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in *BioLaw Journal-Rivista di BioDiritto*, 2019, 3: 205-235.

<sup>(2)</sup> High-Level Independent Group on Artificial Intelligence (AI HLEG) (2019).

<sup>(3)</sup> *State vs. Loomis*, case n. 2015AP157-CR. V. anche § 1.2.1. in questo volume.

<sup>(4)</sup> G. DE MINICO, *Towards an ‘Algorithm Constitutional by Design’*, in *BioLaw Journal-Rivista Di BioDiritto*, 2021, 1: 381-403.

<sup>(5)</sup> Proposal For a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. COM/2021/206 FINAL, di seguito “Proposta”.

novero di tecniche computazionali, inclusi tutti gli approcci di *machine learning* (supervisionato, non supervisionato, con rinforzo), approcci *logic-based* e *knowledge-based* — inclusi i sistemi esperti, i *reasoner* e i motori inferenziali — e altri approcci (statistici, stimatori di Bayes, metodi di ottimizzazione e ricerca) <sup>(6)</sup>.

Va naturalmente sottolineata l'avvertenza che qualsiasi risultato raggiunto da questo studio sarà soggetto alla volontà del legislatore europeo. A corredo dell'analisi legislativa, sarà dunque opportuno inquadrare tale proposta nel quadro normativo di riferimento esistente, compensando la relativa aleatorietà ermeneutica che contraddistingue una proposta di discussione con alcune riflessioni ormai consolidate in dottrina.

Questo breve saggio intende illustrare il contenuto del proposto intervento normativo, suggerendo alcuni spunti ermeneutici (Sezione 2) e discutendo di alcune specifiche disposizioni peculiari dei sistemi di IA applicati alla giustizia (Sezione 3), anche nel contesto degli standard e degli errori algoritmici (Sezione 4), per poi collocare queste novità nel contesto della responsabilità civile (Sezione 5). Alcune considerazioni conclusive (Sezione 6) riassumono i punti focali.

### 3.2. Proposta *AI Act* e amministrazione della giustizia

#### 3.2.1. *Le attività di assistenza dei sistemi di IA all'autorità giudiziaria*

L'amministrazione della giustizia rappresenta uno dei settori all'interno dei quali ricavare i sistemi di IA ad alto rischio ai sensi della Proposta, secondo il rimando operato all'Allegato III dall'art. 6, co. 2. In particolare, ogni settore così individuato contiene l'elenco dei sistemi di IA ad alto rischio. Per quanto qui interessa, il settore numero 8, denominato "Amministrazione della giustizia e processi democratici", consta della sola lettera *a*), relativa ai "sistemi di IA destinati ad assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei

---

<sup>(6)</sup> Per una panoramica completa di questi approcci, v. S. J. RUSSELL, P. NORVIG, (2005), *Intelligenza artificiale. Un approccio moderno* (Vol. 1).

fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti" (7).

La Proposta mira ad introdurre un insieme proporzionato ed efficace di regole vincolanti per i sistemi di IA avvalendosi di un approccio basato sul rischio. La tipologia e il contenuto delle regole sono dunque adattate all'intensità e alla portata dei rischi che possono essere generati dai sistemi di IA (cons. 14). Pertanto, alcune pratiche di Intelligenza Artificiale sono del tutto vietate in quanto a rischio eccessivamente elevato (Titolo II). Differentemente, i sistemi di IA a cui è ascritto un "alto rischio" possono essere immessi sul mercato o messi in servizio al ricorrere di determinati requisiti e all'assolvimento di obblighi per gli operatori pertinenti (Titolo III). Per altri sistemi di IA, non considerati ad alto rischio ma a rischio limitato, vengono prescritti obblighi di trasparenza (Titolo IV). Infine, non sono previste indicazioni per tutti i sistemi non rientranti nei primi tre gruppi, il cui rischio è ritenuto minimo.

Tra i settori predefiniti di cui all'Allegato III, l'alto rischio concerne il pregiudizio alla salute, alla sicurezza o ai diritti fondamentali delle persone, alla luce della finalità sottesa all'uso del sistema di IA, tenendo conto sia della gravità del possibile danno sia della probabilità che si verifichi (cons. 32). Al momento, come accennato, l'elenco di cui al n. 8 è costituito dalla mera lettera *a*). La norma cita l'autorità giudiziaria quale soggetto destinatario dell'assistenza di un sistema di IA. Per autorità giudiziaria parrebbe intendersi la magistratura come terzo potere dello Stato, in quanto esercente la funzione giurisdizionale (8).

Ai sensi dell'art. 102 Cost., la funzione giurisdizionale è esercitata anzitutto da magistrati ordinari, nelle materie civile e penale, dislocati in Tribunali, Corti d'Appello e Corte di Cassazione. Accanto ai magistrati con funzioni giudicanti, vi sono quelli con funzioni requirenti, o

---

(7) Si segnala che, per quanto concerne la giustizia penale, rileva anche il settore numero 6 dell'All. III ("Attività di contrasto") e la presenza della *Risoluzione del Parlamento europeo del 6 Ottobre 2021 sull'Intelligenza Artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale* (2020/2016(INI)), non oggetto di analisi nel presente contributo. Sui profili specifici, v. però il Capitolo 5 e il Capitolo 7 di questo volume. Invece, sulla relazione con altri tipi di impiego di strumenti di IA nel processo, V. § 1.1. in questo volume.

(8) Questa interpretazione si ferma all'attività dell'autorità giudiziaria che vengono citate nel testo. Adrebbero fornita assistenza.



## CAPITOLO 4

**BLOCKCHAIN-BASED SMART CONTRACTS E  
E-JUSTICE NELLA PROPOSTA AI ACT**di *Chantal Bomprezzi*

**SOMMARIO:** 4.1. Introduzione. — 4.2. Funzionamento di *blockchain* e *smart contract*. — 4.3. *Smart contract* e *e-Justice*. — 4.4. *Smart contract* e *AI Act*. — 4.5. *Blockchain* e conformità ai requisiti dell'*AI Act*. — 4.6. Incompatibilità tra *blockchain* e *AI Act*: la decentralizzazione. — 4.7. (*Segue*) L'immutabilità. — 4.8. (*Segue*) L'anonimato. — 4.9. Conclusioni.

**4.1. Introduzione**

La *blockchain*, diffusasi inizialmente con le cosiddette “criptovalute” <sup>(1)</sup>, ha avuto uno sviluppo esponenziale tanto da essere stata definita “*disruptive*” <sup>(2)</sup>. Innumerevoli possono essere le applicazioni di *blockchain* <sup>(3)</sup>. Le piattaforme più avanzate consentono il caricamento di *smart contracts*, programmi informatici autoeseguibili con cui automatizzare operazioni e processi <sup>(4)</sup>.

---

<sup>(1)</sup> Su *blockchain* e criptovalute si rimanda a A. M. GAMBINO, C. BOMPRESZI, *Blockchain e criptovalute*, in G. FINOCCHIARO, V. FALCE (a cura di), *Fintech: diritti, concorrenza, regole – Le operazioni di finanziamento tecnologico*, Zanichelli, Bologna, 2019, pp. 267 ss.

<sup>(2)</sup> M. SWAN, *Blockchain, Blueprint for a New Economy*, O'Reilly, Sebastopol (CA, USA), 2015, p. VII rappresenta la blockchain come “the next major disruptive technology and worldwide computing paradigm (following the mainframe, PC, Internet, and social networking/mobile phones) with the potential for reconfiguring all human activity as pervasively as did the Web”.

<sup>(3)</sup> Su *blockchain* può essere potenzialmente caricato qualsiasi dato o informazione; pertanto, essa è adottabile per i più svariati utilizzi, su cui, per una panoramica, v. EUROPEAN COMMISSION, JOINT RESEARCH CENTRE, *Blockchain now and tomorrow – assessing multidimensional impacts of distributed ledger technologies*, 2019, reperibile qui: <https://ec.europa.eu/jrc/en/facts4efuture/blockchain-now-and-tomorrow> (ult. visita 3 ottobre 2022).

<sup>(4)</sup> Ispetto alle piattaforme il cui funzionamento è limitato al mero scambio di criptovalute, le *blockchain* concepite anche per *smart contract* sono più tecnicamente

La peculiarità di *blockchain*, che rappresenta la ragione dell'interesse suscitato alla medesima da parte sia delle istituzioni <sup>(5)</sup> che dei privati <sup>(6)</sup>, si rinviene nel suo particolare funzionamento che, anche grazie alla fusione tra tecnologie preesistenti quali i sistemi distribuiti e la crittografia asimmetrica, dovrebbe garantire un elevatissimo livello di protezione da interventi di modifica successivi non autorizzati (tanto da essere considerata sostanzialmente immutabile), la trasparenza e la tracciabilità delle operazioni che in essa hanno luogo.

Il presente contributo si interroga sul rapporto tra *smart contract* basati su *blockchain* e Proposta *AI Act* qualora tali soluzioni vengano adottate nell'ambito *e-Justice*. In particolare, dopo un preliminare approfondimento circa il funzionamento tecnico (§ 4.2) e una panoramica sugli utilizzi attuali della tecnologia e i vantaggi astrattamente apportabili al sistema giustizia (§ 4.3), lo studio si interroga sull'applicabilità della Proposta agli *smart contract* rispetto alla definizione di sistema di Intelligenza Artificiale *ivi* fornita (§ 4.4). Successivamente, viene affrontato il tema della *compliance* di tali sistemi rispetto ai requisiti richiesti per i sistemi di IA ad alto rischio (§ 4.5) e ci si sofferma sui ritenuti profili di incompatibilità. Su quest'ultimo punto, i tre aspetti maggiormente critici, a ciascuno dei quali viene dedicato un

---

evolte. Per approfondimenti, v. C. BOMPRESZI, *Implications of Blockchain-Based Smart Contracts on Contract Law*, Nomos, Baden-Baden (Germany), 2021, pp. 40 ss.

<sup>(5)</sup> In Europa, 30 Stati hanno firmato la *European Blockchain Partnership* per cooperare sul tema, reperibile qui: <https://digital-strategy.ec.europa.eu/en/policies/blockchain-partnership> (ult. visita 03 ottobre 2022). Una *European Blockchain Services Infrastructure* (EBSI) è stata creata per sviluppare servizi pubblici digitali transfrontalieri basati su *blockchain*, reperibile qui: <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home> (ult. visita 03 ottobre 2022). Nel febbraio del 2018 la Commissione europea ha lanciato, in collaborazione con il Parlamento europeo, lo *European Blockchain Observatory and Forum*, reperibile qui: <https://www.eublockchainforum.eu/> (ult. visita 3 ottobre 2022); all'interno di quest'ultimo vengono organizzati eventi e prodotti report di approfondimento. L'Italia ha costituito un gruppo di esperti per elaborare una strategia nazionale, reperibile qui: <https://www.mise.gov.it/index.php/it/consultazione-blockchain> (ult. visita 3 ottobre 2022). Anche sul piano internazionale sono sorte svariate iniziative, come l'istituzione di *Atrium*, una piattaforma di scambio e apprendimento all'interno della comunità delle Nazioni Unite, reperibile qui: <https://atrium.network/> (ult. visita 03 ottobre 2022); un'altra iniziativa è rappresentata dal *Global Blockchain Policy Centre* dell'OCSE, reperibile qui: <https://www.oecd.org/daf/blockchain/> (ult. visita 3 ottobre 2022).

<sup>(6)</sup> L'Unione europea sta all'uopo mettendo a disposizione cospicui fondi per sostenere gli investimenti, la cui notizia è reperibile qui: <https://digital-strategy.ec.europa.eu/en/policies/blockchain-funding> (ult. visita 3 ottobre 2022).

apposito paragrafo, si ascrivono alla decentralizzazione (§ 4.6), all'immutabilità della tecnologia (§ 4.7) e alla condizione di anonimato degli utenti (§ 4.8).

## 4.2. Funzionamento di *blockchain* e *smart contract*

Gli *smart contract* elaborano le istruzioni contenute nel codice informatico secondo la logica “se X, allora Y” (7), dove con X si intendono gli *input* esterni, e con Y i relativi *output*. L'autoeseguibilità degli *smart contract* discende dall'idoneità a compiere azioni in vece dell'uomo potenzialmente in ogni ambito, tra cui anche, ma non esclusivamente, quello contrattuale (8).

Gli *smart contract* possono essere caricati ed eseguiti in *blockchain*, ma la loro origine è antecedente (9). Gli *smart contract blockchain-based*, d'altro canto, possono beneficiare delle peculiarità di *blockchain* (10).

La *blockchain* è un *database* distribuito e decentralizzato (11). Il sistema distribuito si pone in alternativa al classico modello *client-*

---

(7) P. CUCCURU, *Blockchain ed automazione contrattuale, riflessioni sugli smart contract*, in *Nuova giur. Civ.*, 2017, 1: 107-119; Id., *Beyond Bitcoin: an early overview on smart contracts* in *International Journal of Law and Information Technology*, 2017, 25: 179-195.

(8) F. DI GIOMMO, *Smart contract e (non-)diritto. Il caso dei mercati finanziari*, in *Nuovo Dir. Civ.*, 2019, 1: 257-295. L'espressione “*smart contract*” è stata coniata dall'informatico Nick Szabo negli Anni '90, che definiva “*a computerized transaction protocol that executes the terms of a contract*”. L'idea alla base delle teorie di Szabo era quella di demandare interamente l'attività contrattuale, tra cui l'esecuzione, a dei *software*, ritenuti più affidabili dell'uomo. Con l'invenzione della *blockchain* si è riacceso l'interesse nei confronti degli *smart contracts* in quanto essa appare come la realizzazione concreta di quanto precedentemente ipotizzato da Nick Szabo. V. N. SZABO, *Formalizing and Securing Relationships on Public Networks*, 1997, reperibile qui: <https://firstmonday.org/ojs/index.php/fm/article/view/548> (ult. visita 03 ottobre 2022).

(9) G. HILEMAN, M. RAUCHS, 2017 *Global Blockchain Benchmarking Study*, 2017, reperibile qui: <https://ssrn.com/abstract=3040224> (ult. visita 3 ottobre 2022).

(10) LO EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM, in un report del 27 settembre 2019 dal titolo *Legal and Regulatory Framework of Blockchains and Smart Contracts* (reperibile qui: <https://www.eublockchainforum.eu/reports>, ult. visita 03 ottobre 2022), dà la seguente definizione di *smart contract*: “*In the blockchain context, it generally means computer code that is stored on a blockchain and one or more parties can access that. These programs are often self-executing and make use of blockchain properties like tamper-resistance, decentralised processing, and the like*” (p. 22).

(11) Più diffusamente sul funzionamento della tecnologia *blockchain*, vedi, in ambito italiano: S. COMELLINI, M. VASAPOLLO, *Blockchain, criptovalute, I.C.O. e smart contract*, Maggioli, Santarcangelo di Romagna, 2019; L. M. PERUGINI, *Distributed ledger technologies e sistemi di blockchain: digital currency, smart contract e altre applicazioni*,

*server*, in cui le informazioni transitano da un centro (il *server*) e si diramano mediante i *download* dei *client*; piuttosto, esse sono replicate in una serie di computer (detti “nodi”), che ne rendono la perdita meno probabile. Inoltre, la duplicazione del dato non è effettuata centralmente a partire da un *master node*, ma l’aggiornamento avviene in contemporanea grazie alla condivisione di un apposito protocollo. Tale decentralizzazione è atta a scongiurare il rischio di errori di duplicazione delle informazioni scambiate, con più elevate prestazioni in termini di trasparenza ed efficienza (sia dal punto di vista economico che temporale) <sup>(12)</sup>.

Il vocabolo “*blockchain*” deriva dal raggruppamento in blocchi delle attività registrate (denominate “transazioni”), posizionati in ordine cronologico attraverso strumenti di marcatura temporale (*timestamp*). Ogni blocco è identificato da un *hash*, una stringa alfanumerica univoca, e include anche l’*hash* del blocco precedente, fino a formare una concatenazione di blocchi; il significato letterale di *blockchain* è, infatti, “catena di blocchi”. Questa particolare conformazione protegge il sistema da manipolazioni successive, poiché ogni tentativo di modifica di un *hash* si ripercuoterebbe anche sui successivi, rendendo

---

Key editore, Milano, 2018; M. NICOTRA, F. SARZANA DI SANT’IPPOLITO, *Diritto della blockchain, Intelligenza Artificiale e IoT*, Ipsos, Assago (MI), 2018. In ambito internazionale: I. BASHIR, *Mastering blockchain*, Packt, Birmingham – Mumbai, 2018; M. SWAN, *Blockchain, Blueprint for a New Economy*, op. cit.; A. WRIGHT, P. DE FILIPPI, *Decentralized Blockchain Technology and The Rise of Lex Cryptographia*, 2015, reperibile qui: <http://papers.ssrn.com/abstract=2580664> (ult. visita 3 ottobre 2022).

<sup>(12)</sup> Il recente Regolamento (UE) 2022/859 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo a un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito e che modifica i regolamenti (UE) n. 600/2014 e (UE) n. 909/2014 e la direttiva 2014/65/UE definisce la “tecnologia a registro distribuito (DLT)” come “una tecnologia che consente il funzionamento e l’uso dei registri distribuiti” (art. 2, par. 1, n. 1) e il “registro distribuito” come “un archivio di informazioni in cui sono registrate le operazioni e che è condiviso da una serie di nodi di rete DLT ed è sincronizzato tra di essi, mediante l’utilizzo di un meccanismo di consenso” (art. 2, par. 1, n. 2); con “meccanismo di consenso” si intendono “le regole e le procedure con cui si raggiunge un accordo, tra i nodi di rete DLT, sulla convalida di un’operazione” (art. 2, par. 1, n. 3) e con “nodo di rete DLT” “un dispositivo o un’applicazione informatica che è parte di una rete e che detiene una copia completa o parziale delle registrazioni di tutte le operazioni eseguite tramite il registro distribuito” (art. 2, par. 1, n. 4). Il Regolamento è uno dei tre atti normativi del c.d. *Digital Finance Package*, un pacchetto di misure volte a regolare il fenomeno *blockchain* nel settore finanziario: <https://eur-lex.europa.eu/legal-content/it/TXT/?uri=CELEX:32022r0859>.

Termine estratto capitolo

## CAPITOLO 5

**MECHANICAL JUDGEMENT: UN PROCESSO IN ACTION  
DI AUTOMAZIONE DELLA DECISIONE PENALE?**di *Vittorio Manes, Alessandra Santangelo*

**SOMMARIO:** 5.1. Premessa. — 5.2. Profili di metodo. — 5.3. Verso una “nuova” disciplina europea. — 5.4. Diritto interno e innovazioni normative. — 5.4.1. IA e *policing*: profili attuativi e criticità. — 5.4.2. (*Segue*) Spunti critici in prospettiva comparata sull’esatta calcolabilità delle fasi investigative. — 5.5. Gli strumenti predittivi e il giudizio penale. — 5.5.1. Il contributo delle nuove tecnologie nella fase interpretativa e di applicazione del diritto. — 5.5.2. Giudizi prognostici e *sentencing*. — 5.6. Errore algoritmico: il problema aperto del riparto di responsabilità.

**5.1. Premessa**

La diffusione dei sistemi intelligenti nella sfera penale ha comportato rilevanti conseguenze che muovono — quanto meno — su due piani simmetrici e opposti <sup>(1)</sup>.

Per un verso, le eccezionali potenzialità della macchina hanno promesso soluzioni innovative per i problemi che “tradizionalmente” affliggono il sistema giustizia. Attenuato l’aggravio imposto dagli eccessivi carichi di lavoro e dalle ipotesi di malfunzionamento organizzativo, gli attori del processo penale appaiono liberi di concentrare i propri sforzi sulla risoluzione delle questioni di fatto o di diritto più complesse, agevolando un più rapido evolversi della cultura giuridica

---

<sup>(1)</sup> Con riguardo al carattere di « autentica rivoluzione » indotta dalle interazioni tra nuove tecnologie e diritto penale, si rinvia a P. SEVERINO, *Intelligenza artificiale e diritto penale*, in U. RUFFOLO (a cura di), *Intelligenza artificiale, il diritto, i diritti, l’etica*, Giuffrè, Milano, 2020, p. 531. Per un’analisi più ampia sul carattere pervasivo della diffusione dei sistemi intelligenti, W. BARFIELD, *Towards a law of artificial intelligence*, in W. BARFIELD, U. PAGALLO (a cura di), *Research handbook on the law of artificial intelligence*, Cheltenham, Elgar, 2018, p. 2 s., ove l’A. richiama le parole di Tony Tether secondo cui « machine learning is the next Internet » (corsivi originali).

della comunità di riferimento. Per altro verso, le spinte nella direzione di una “giustizia digitale” che hanno promosso modelli predittivi a carattere anticipatorio capaci di implementare il livello di certezza sulla scorta della c.d. *actuarial doctrine* <sup>(2)</sup>, appaiono strutturalmente antitetici rispetto alle fondamenta su poggia il diritto penale liberale. Il carattere imminente e, al contempo, ineludibile del progresso tecnologico ha, quindi, imposto alla dottrina — ma gradatamente anche alle sedi istituzionali <sup>(3)</sup> (v. *infra*, § 5.3) — di riaprire il dibattito su fondamento e legittimazione delle sanzioni punitive, inquadrando le scelte di politica criminale relative all’impiego degli strumenti algoritmici in una più generale riflessione sull’identità della sfera penale <sup>(4)</sup>.

D’altro canto, nell’alternativa tra modello “forte” e “debole” di Intelligenza Artificiale <sup>(5)</sup>, non si può ignorare la proposta di sostituire il giudice persona fisica con una “*machina sapiens*” <sup>(6)</sup>, così da assicurare, in un contesto che pare altamente incerto e imprevedibile <sup>(7)</sup>,

---

<sup>(2)</sup> In senso critico, si veda, inter alia, J. M. EAGLIN, *Technologically Distorted Conceptions of Punishment*, in Wash. U. L. Rev., 2019, p. 485 ss., B. E. HARCOURT, *Against Prediction. Profiling, Policing and Punishing in an Actuarial Age*, Chicago, 2007, *passim*, nonché A. ASHWORTH-L. ZEDNER, *Preventive Justice*, Oxford, 2015, p. 132 s., precisando gli autori che « probabilistic assessments continue to form the basis for dichotomous decisions within the court room, not least whether to impose a fixed term or an indeterminate and therefore potentially grossly disproportionate sentence ».

<sup>(3)</sup> Solo si pensi al *Group of Experts on Artificial Intelligence and Criminal Law*, istituito a opera dello *European Committee on Crime Problems*, proprio allo scopo di raccordare e confrontare le iniziative normative e di regolazione adottate dagli ordinamenti europei per raccordare nuove tecnologie e giustizia penale: per approfondire, si rinvia alle considerazioni formulate *infra*, § 5.3.

<sup>(4)</sup> C. BURCHARD, *L’Intelligenza Artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in Riv. It. Dir. e proc. Pen., 4, 2019, p. 1938, ove l’A. osserva che « [l]a pressione [...] sorge in ogni caso quando si guardano i postulati normativi celati dell’IA, postulati normativi che sono facilmente mascherati da molte superficiali trame giustificative (più efficace ed efficiente; più obiettiva, neutrale e coerente). In questo senso, la scienza penalistica deve aprirsi alla teoria sociale o politica e prendere posizione su questioni fondamentali (in particolare sull’importanza sociale della fiducia e dell’apertura al futuro) ».

<sup>(5)</sup> Sulla distinzione in questione, si veda anzitutto J. SEARLE, *Minds, Brains, and Programs*, in *Behavioral and Brain Science*, 1980, 417.

<sup>(6)</sup> Per una disamina delle ragioni poste a fondamento di una simile opzione, si rinvia a M. LUCIANI, *La decisione giudiziaria robotica*, in *Rivista AIC*, 2018, 873.

<sup>(7)</sup> Si consideri che il problema ha raggiunto uno stadio di complessità tanto avanzato da persuadere gli indecisi sull’opportunità di introdurre *ex novo* il principio di riserva di codice, nel tentativo di razionalizzare e contenere l’ipertrofia punitiva: esaminando la proposta della Commissione Pagliaro, nonché i successivi progetti delle

ragionevoli margini di calcolabilità all'intervento punitivo <sup>(8)</sup>. Consumata la crisi dell'ideale "legalistico" del *nullum crimen* <sup>(9)</sup>, è (ormai) piuttosto condiviso il processo di dissoluzione della legalità — o, meglio, della centralità un tempo riservata alla riserva di legge <sup>(10)</sup> — nella prevedibilità della sanzione penale <sup>(11)</sup>. A fronte della necessità di

---

commissioni Grosso e Pisapia, C.E. PALIERO, *La "riserva di codice" messa alla prova: deontica "idealistica" versus deontica realista*, in *Criminalia*, 2019, 34. Con riguardo ai vantaggi che derivano dalla riserva di codice rispetto al proliferare di livelli semantici inconferenti tra codificazione e legislazione complementare, si veda C. SOTIS, *Vincolo di rubrica e tipicità penale*, in *Riv. It. Dir. e proc. Pen.*, 2017, 1365. La migliore dottrina, del resto, aveva già puntualmente osservato la tendenza legislativa che aveva reso « il precetto [...] inattuabile per un avvicinarsi e affollarsi di fonti che continuamente rinviano ad altre fonti »: F. SGUBBI, *Il diritto penale incerto ed efficace*, in *Riv. It. Dir. e proc. Pen.*, 4, 2001, 1194. All'opposto, norme penali selettive, in grado di attingere le sole aggressioni intollerabili, consentirebbero di meglio giustificare il *self-restraint* imposto ai giudici nell'interpretazione della legge penale. Sul punto, si veda M. DONINI, *Teoria del reato*, Cedam, Padova, 1996, 238.

<sup>(8)</sup> Con riguardo alla distinzione tra calcolabilità e prevedibilità, si rinvia a G. ZACCARIA, *Figure del giudicare: calcolabilità, precedenti, decisione robotica*, in *Riv. Dir. Civ.*, 2, 2020, p. 277 ss.

<sup>(9)</sup> Da tempo, invero, la scienza penale descrive la crisi della legalità quale contraltare « della più generale crisi della democrazia »: G. FIANDACA, *Principio di legalità e diritto penale*, in *Quad. fior.*, II, 36, 2007, p. 1276, nonché ID., *Crisi della riserva di legge e disagio della democrazia rappresentativa nell'età del protagonismo giurisdizionale*, in *Criminalia*, 2011, p. 88. Per approfondire, con riguardo ai fattori endogeni che hanno esacerbato il fenomeno, si veda; con riguardo, poi, alle cause esogene, C. CUPELLI, *La legalità delegata. Crisi e attualità della riserva di legge nel diritto penale*, ESI, Napoli, 2012, p. 279 ss., C. GRANDI, *Riserva di legge e legalità penale europea*, Giuffrè, Milano, 2010, p. 48 ss., nonché in prospettiva convenzionale a V. MANES, *L'evoluzione del rapporto tra Corte e giudici comuni nell'attuazione del "volto costituzionale" dell'illecito penale*, in V. MANES, V. NAPOLEONI, *La legge penale illegittima. Metodo, itinerari e limiti della questione di costituzionalità in materia penale*, Giappichelli, Torino, 2019, p. 42 ss.

<sup>(10)</sup> In argomento, F. PALAZZO, voce *Legalità (dir. Pen.)*, in S. CASSESE (diretto da), *Dizionario di diritto pubblico*, Giuffrè, Milano, IV, 2006, p. 3379. Con particolare riguardo ai contraccolpi subiti nel tempo dal sistema delle fonti penali, M. GALLO, *Le fonti rivisitate. Appunti di diritto penale*, Giappichelli, Torino, 2017, p. 106 ss., C.E. PALIERO, *Il diritto liquido. Pensieri post-delmasiani sulla dialettica delle fonti penali*, in *Riv. It. Dir. e proc. Pen.*, II, 2014, p. 1126, ove l'A. analizza il tramonto dell'utopia codicistica, nonché G. INSOLERA, *Il diritto penale complementare*, in U. CURI-G. PALOMBARINI (a cura di), *Diritto penale minimo*, Donzelli, Roma, 2002, 63.

<sup>(11)</sup> Con particolare riguardo alla genesi "europea" della prevedibilità, A. BERNARDI, *Il principio di legalità dei reati e delle pene nella Carta europea dei diritti: problemi e prospettive*, in *Riv. It. Dir. Pubb. Com.*, 4, 2002, p. 681 ss., F. PALAZZO, *Legalità e determinatezza della legge penale: significato linguistico, interpretazione e conoscibilità*

definire il profilo di una “nuova” legalità <sup>(12)</sup>, pertanto, le potenzialità inedite dei processi algoritmici non hanno mancato di destare interesse quale rimedio capace di implementare la stabilità del diritto <sup>(13)</sup> e risolvere — peraltro, in termini potenzialmente definitivi — *bias* e incertezze riconducibili al giudizio del giudice-persona fisica.

Su tale scenario, nondimeno, insistono le critiche di quanti sostengono che i vantaggi in termini di calcolabilità del diritto punitivo non siano in alcun modo proporzionati al sacrificio delle garanzie personali che assistono la sfera penale: «il sistema penale», in particolare, «è un sistema personocentrico e personologico, pensato per l'uomo ed affidato al giudizio dell'uomo, come tale *fallibile* ma pur sempre *controllabile* secondo un determinato *iter* argomentativo e i criteri che lo guidano» <sup>(14)</sup>. D'altronde, si obietta, non è escluso che possa giungersi alla definitiva scomparsa del diritto penale, a fronte del

---

della *regula iuris*, in G. VASSALLI (a cura di), *Diritto penale e giurisprudenza costituzionale*, ESI, Napoli, 2006, p. 73, mettendo l'accento sull'indebolirsi della componente politica del *nullum crimen* in ragione della prospettiva individual-garantistica preferita in relazione ai requisiti qualitativi della legalità europea. Quanto, poi, alle diverse accezioni di cui il principio si compone nella giurisprudenza della Corte di Strasburgo, si rinvia, *inter alia*, a M. DONINI, *Fattispecie o case law? La "prevedibilità del diritto" e i limiti alla dissoluzione della legge penale nella giurisprudenza*, in *Questione giustizia*, 4, 2018, 101; F. MAZZACUVA, *Art. 7*, in G. UBERTIS, F. VIGANÒ (a cura di), *Corte di Strasburgo e giustizia penale*, II ed., Giappichelli, Torino, 2022, 301, nonché, D. PERRONE, *Nullum crimen sine iure. Il diritto penale giurisprudenziale tra dinamiche interpretative in malam partem e nuove istanze di garanzia*, Giappichelli, Torino, 2019, 212, osservando come i diversi indirizzi seguiti dai giudici di Strasburgo nell'interpretazione dei requisiti qualitativi di cui all'art. 7 CEDU siano da imputare alla «manipolazione strumentale della prevedibilità secondo le contingenti istanze di giustizia sostanziale del caso concreto».

<sup>(12)</sup> Si tratta di una nozione ormai piuttosto consolidata su cui, *inter alia*, F. PALAZZO, *Interpretazione penalistica e armonizzazione europea nell'attuale momento storico*, in *Ars interpretandi*, 2, 2016, p. 79; P. GROSSI, *Oltre la legalità*, Laterza, Roma-Bari, 2020, in particolare p. 79 ss.; V. MAIELLO, *La legalità della legge nel tempo del diritto dei giudici*, ES, Napoli, 2020, p. 15; M. VOGLIOTTI, *La nuova legalità penale e il ruolo della giurisdizione, Spunti per un confronto*, in *Sistema penale*, 3, 2020, p. 63, secondo cui è in tale contesto valorizzato il piano dell'effettività del diritto in relazione «alla concreta esperienza giuridica, ai significati che gli enunciati normativi assumono a contatto con i multiformi e cangianti fatti della vita».

<sup>(13)</sup> Sull'esigenza di calcolabilità e affidamento d'ispirazione weberiana in relazione alla funzione nomofilattica della Corte di legittimità, si rinvia a N. IRTI, *Per un dialogo sulla calcolabilità giuridica*, in A. CARLEO (a cura di), *Calcolabilità giuridica*, Il Mulino, Bologna, 2017, p. 22 s.

<sup>(14)</sup> V. M. ... *Giudice al binario tecnologico*

Termine estratto capitolo



## CAPITOLO 6

INTELLIGENZA ARTIFICIALE, AMMINISTRAZIONE  
E TUTELA DEI DIRITTI

di Marco Dugato, Donato Vese (\*)

**SOMMARIO:** 6.1. Introduzione e struttura della ricerca. — Parte I. - *Profili sostanziali*. — 6.2. Intelligenza artificiale e tassonomia in ambito pubblico. — 6.3. L'analisi costi-benefici nell'implementazione di algoritmi nel procedimento amministrativo. — 6.4. Il problema della trasparenza e della motivazione degli atti prodotti dagli algoritmi. — 6.5. Il bisogno di un'Intelligenza Artificiale che metta al centro la persona. — Parte II. - *Profili processuali*. — 6.6. Intelligenza artificiale e giudizio amministrativo. — 6.6.1. Algoritmi: tassonomia e trattamento processuale. — 6.6.2. Funzionamento del processo amministrativo e applicazione degli algoritmi. — 6.6.3. Il rispetto dei principi posti a base dell'ordinamento giuridico. — 6.6.3.1. Principio di strumentalità del ricorso all'informatica. — 6.6.3.2. Principio di trasparenza e conoscibilità. — 6.6.3.3. Principio di imputabilità. — 6.6.3.4. Principio di non esclusività della decisione algoritmica. — 6.6.3.5. Principio di non discriminazione algoritmica. — 6.7. Conclusioni.

**6.1. Introduzione e struttura della ricerca**

L'Intelligenza Artificiale (AI) sta rivoluzionando radicalmente la nostra società. Il passaggio dal capitale finanziario a quello digitale <sup>(1)</sup>, nel senso di detenere *big data* e informazioni di massa per scopi *governativi* — in termini *foucaultiani* <sup>(2)</sup> — ed economici <sup>(3)</sup> si realizza

---

(\*) La ricerca è frutto di un lavoro comune degli autori, tuttavia al dr. Donato Vese vanno attribuiti il paragrafo 6.1. "Introduzione e struttura della ricerca" e l'intera Parte I sui Profili sostanziali, vale a dire i paragrafi 6.2., 6.3., 6.4. e 6.5. e le conclusioni 6.7. Al Prof. Marco Dugato va attribuita l'intera Parte II sui profili processuali, vale a dire i paragrafi 6.6., 6.6.1., 6.6.2., 6.6.3., 6.6.3.1., 6.6.3.2., 6.6.3.3., 6.6.3.4., 6.6.3.5., e le conclusioni 6.7.

<sup>(1)</sup> M. FERRARIS, *Documanità*, Roma-Bari, Laterza, 2021.

<sup>(2)</sup> M. FOUCAULT, *Naissance de la Biopolitique, Cours au Collège de France*, 1978-1979, Seuil, Gallimard, 2004, p. 236, dove è chiarito come "[o]n peut faire de la

con l'ascesa della società "algoritmica" (4). In questa tipologia di società, la *burocrazia weberiana* (5) e la *razionalità limitata* di Herbert Simon (6) sembrano appartenere ad un lontano passato, sostituite definitivamente dall'efficienza di sofisticati meccanismi di apprendimento automatico, come gli algoritmi.

Dietro la complessità della *black box* (7) si nasconde una nuova era di *sorveglianza orwelliana* (8) da parte degli Stati e delle *big company* private che possiedono le tecnologie di AI. Mentre la mancanza di trasparenza e di prevedibilità dello Stato automatizzato (9) fa inesorabilmente crollare ogni forma di protezione nell'ordine costituzionale (10), il *panopticon* di Bentham (11) si realizza in tutta la sua potenza e violenza. In un tale ambito giuridico, ogni diritto fondamentale in gioco è potenzialmente minacciato dal nuovo "capitale di dati".

In questo scenario, la presente ricerca esplora l'applicazione dell'Intelligenza Artificiale all'amministrazione pubblica, a partire dall'analisi della tassonomia dei principali strumenti dell'AI che trovano applicazione nell'ordinamento giuridico. L'implementazione degli algoritmi nel procedimento amministrativo viene esaminata alla luce

---

même façon l'analyse des soins médicaux, et d'une façon générale de toutes les activités concernant la santé des individus, qui apparaissent ainsi comme étant autant d'éléments à partir desquels le capital humain va pouvoir premièrement être amélioré, deuxièmement être conservé et utilisé le plus longtemps possible"; si v. anche K. BERKER, *Biosecurity: securing circulations from the microbe to the macrocosm*, in *The Geographical Journal*, 181(4), 2015, pp. 357-365.

(3) M. BUNZ, *Die stille Revolution: Wie Algorithmen Wissen, Arbeit, Öffentlichkeit und Politik verändern, ohne dabei viel Lärm zu machen*, Suhrkamp, Berlin 2012.

(4) M. SCHULENBURG, R. PEETERS (a cura di), *The Algorithmic Society: Technology, Power, and Knowledge*, London, Taylor & Francis, 2021.

(5) M. WEBER, *Economia e Società. L'economia in rapporto agli ordinamenti e alle forze sociali*, Roma, Donzelli, 2003.

(6) H. A. SIMON, *Economics, Bounded Rationality and the Cognitive Revolution*, Aldershot, Elgar, 1992.

(7) J. WARD, *Black Box Artificial Intelligence and the Rule of Law*, in *Law and Contemporary Problems*, 84, 3, 2021, p. 1 ss.

(8) G. ORWELL, *Nineteen Eighty-four a Novel*, Harmondsworth, Penguin in Association with Secker & Warburg, 1954.

(9) C. COGLIANESE, D. LEHR, *Transparency and Algorithmic Governance*, in *Administrative Law Review*, 71, 1, 2019, 1, p. 9 ss.

(10) A. REICHMAN, A. SIMONCINI, G. DE GREGORIO, G. SARTOR, H. W. MICKLITZ, O. POLLICINO (a cura di), *Constitutional Challenges in the Algorithmic Society*, Cambridge, Cambridge University Press, 2021.

(11) J. BENTHAM, M. FOUCAULT, M. PERROT, G. FUKU. *Panopticon, ovvero, la casa d'ispezione*. 2 ed., Venezia, Marsilio, 1997.

dell'analisi costi-benefici per comprendere gli effetti che tali strumenti producono nella sfera dell'amministrazione, mentre la necessità di (ri)mettere la persona umana al centro del dibattito sull'uso dei sistemi di Intelligenza Artificiale è argomentata nella conclusione della Parte I dell'articolo.

La ricerca si concentra sui profili di tutela dei diritti nei confronti dei meccanismi di AI nella Parte II. A questo scopo, viene offerta una tassonomia degli algoritmi in relazione al trattamento processuale e al funzionamento del giudizio amministrativo. L'esame dei principi posti alla base dell'ordinamento giuridico, fra cui la strumentalità del ricorso all'informatica, la trasparenza, la conoscibilità, l'imputabilità, la non esclusività e discriminazione degli algoritmi costituiscono le basi portanti di questa seconda parte della ricerca.

## Parte I. - *Profili sostanziali*

### 6.2. Intelligenza artificiale e tassonomia in ambito pubblico

Nel pieno della “Quarta Rivoluzione Industriale” <sup>(12)</sup> le tecnologie informatiche, basate sull'uso dell'Intelligenza Artificiale, pongono alla scienza giuridica vecchi e nuovi interrogativi <sup>(13)</sup>, mettendo alla prova sia le capacità di risposta del sistema <sup>(14)</sup>, sia le tradizionali ed attuali categorie concettuali <sup>(15)</sup> per seguire l'evoluzione della realtà che muta con ritmi tanto frenetici quanto imprevedibili <sup>(16)</sup>.

---

<sup>(12)</sup> M. ZUAZUA, *The Fourth Industrial Revolution Will Change Production forever. Here's how*, in *World Economic Forum*, 18 gennaio 2019; L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo* (2014), trad. it., Raffaello Cortina, Milano 2017.

<sup>(13)</sup> B. ROMANO, *Algoritmi al potere. Calcolo giudizio pensiero*, Giappichelli, Torino, 2018.

<sup>(14)</sup> F. CAPRIGLIONE, *Diritto ed economia. La sfida dell'Intelligenza Artificiale*, in *Riv. trim. dir. ec.*, suppl. 3, 2021, p. 4 ss.

<sup>(15)</sup> G. ALPA, *L'Intelligenza Artificiale. Il contesto giuridico*, Modena, Mucchi, 2021.

<sup>(16)</sup> F. MATTASSOGLIO, *Algoritmi e regolazione: mito o realtà*, in A. ANTONUCCI, M. DE POLI, P. URBANI (a cura di), *I luoghi dell'economia. Le dimensioni delle sovranità*, Torino, Giappichelli, 2019, p. 57 ss. Gli algoritmi, anche di tipo non deterministico, sono già utilizzati nell'assunzione di decisioni amministrative sebbene manchi in alcuni ordinamenti una norma di legge che ammetta espressamente tale possibilità. Si v. P. G. OTRANTO, *Riflessioni in tema di decisione amministrativa, Intelligenza Artificiale e legalità*, in *Federalismi.it*, 7, 2021, pp. 1-19.

In ambito pubblico <sup>(17)</sup>, le potenzialità dell'Intelligenza Artificiale hanno, di fatto, indotto a guardare con interesse alla prospettiva dell'*e-government*, in un'ottica di semplificazione, volta a migliorare l'efficienza organizzativa della pubblica amministrazione <sup>(18)</sup>, nonché ad implementare i processi democratici e a rafforzare il sostegno delle politiche a tutela dell'interesse generale <sup>(19)</sup>. La transizione verso l'*e-government* fa, dunque, presagire quella che sarà probabilmente la più profonda trasformazione dei processi organizzativi e decisionali garantendo livelli sempre più elevati di efficienza, imparzialità, economicità e trasparenza nei rapporti tra libertà individuali e autorità, quantomeno sulla carta <sup>(20)</sup>.

L'*Amministrazione 4.0* <sup>(21)</sup>, protagonista di tale evoluzione, è condizionata dalla contemporanea manifestazione di due fenomeni: da un lato, la notevole dilazione dei riferimenti spazio-temporali, come conseguenza dell'uso continuo delle ICT <sup>(22)</sup>; dall'altro, la progressiva digitalizzazione per effetto dell'utilizzo degli algoritmi nel procedimento amministrativo <sup>(23)</sup>. Quest'ultimo aspetto è quello maggior-

---

<sup>(17)</sup> M. OSWALD, *Algorithm-assisted decision-making in the public sector: framing the issues using administrative law rules governing discretionary power*, in *Phil. Trans. R. Soc.*, 376, 2018, p. 5.

<sup>(18)</sup> Sull'efficienza organizzativa, sia concesso rinviare a D. VESE, *L'efficienza dell'organizzazione amministrativa come massimizzazione dei diritti fondamentali*, in *P.A. Persona e Amministrazione*, 1, 2019, p. 279 ss.

<sup>(19)</sup> COM (2003) 567 definitivo, Comunicazione della Commissione al Consiglio, al Parlamento Europeo, al Comitato Economico e Sociale e al Comitato delle Regioni, "Il ruolo dell'*e-government* per il futuro dell'Europa (Testo rilevante ai fini del SEE)", Bruxelles 26 Settembre 2003.

<sup>(20)</sup> F. RASO, H. HILLIGOSS, V. KRISHNAMURTHY, C. BAVITZ, L. Y. KIM, *Artificial Intelligence & Human Rights: Opportunities & Risks* (September 25, 2018), *Berkman Klein Center Research Publication No. 2018-6*, disponibile all'indirizzo: <https://ssrn.com/abstract=3259344> (ult. visita 17 Ottobre 2022); M. RISSE, *Human Rights and Artificial Intelligence: An Urgently Needed Agenda*, 41 *HUM. RTS. Q.* 1 (2019).

<sup>(21)</sup> La definizione è di D.U. GALETTA, J.G. CORVOLAN, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *www.federalismi.it*, 2019, pp. 1-23.

<sup>(22)</sup> ICT (Information and Communication Technologies) sono le tecnologie riguardanti i sistemi integrati di telecomunicazione (linee di comunicazione cablate e senza fili), i computer, le tecnologie audio-video e relativi *software*, che permettono agli utenti di creare, immagazzinare e scambiare informazioni. Per questa definizione v. *Enciclopedia Treccani*, disponibile *online* al seguente link: [https://www.treccani.it/enciclopedia/ict\\_%28Diagnostica%20e%20comunicazione%29/](https://www.treccani.it/enciclopedia/ict_%28Diagnostica%20e%20comunicazione%29/).

<sup>(23)</sup> Tra gli autori, cfr. G. GAZDAR, *La rivoluzione digitale e il processo amministrativo*, in *www.federalismi.it*, 2019, pp. 1-23.

## CAPITOLO 7

**L'UTILIZZO DI STRUMENTI DI INTELLIGENZA  
ARTIFICIALE NEL CONTRASTO ALLA CRIMINALITÀ  
ORGANIZZATA DI TIPO MAFIOSO**di *Stefania Pellegrini, Sofia Benedetti*

**SOMMARIO:** 7.1. Le nuove frontiere criminali della criminalità organizzata. L'utilizzazione dell'IA. — 7.2. L'utilizzo dei *big data Analytics* e dell'IA da parte delle forze dell'ordine in un'ottica comparata. — 7.3. Quadro normativo di riferimento. — 7.4. Profili di ricerca e profili applicativi. — 7.4.1. Antimafia Digitale, il *case study* della Immobiliare Strasburgo (ANBSC). — 7.4.2. Proton: le potenzialità della realtà virtuale nella lotta alla mafia e al terrorismo. — 7.4.3. L'analisi dei *big data* e dei grafi per l'interruzione delle reti criminali. — 7.4.4. L'analisi dei *big data* per combattere il crimine organizzato e l'infiltrazione nell'economia legale (collaborazione di UNICRI, CERN e DNA).

**7.1. Le nuove frontiere criminali della criminalità organizzata. L'utilizzo dell'IA**

La principale e più pregnante caratteristica della criminalità si riferisce alla sua "liquidità" intensa come capacità di adattamento alle contingenze spazio-temporali della contemporaneità.

Nonostante l'ossessiva necessità di controllare il territorio nella quale agisce in una spasmodica ricerca di acquisizione di potere i sistemi criminali sono stati in grado di compiere un significativo salto di qualità che ha permesso loro di superare i limiti dello spazio geografico. Il tutto è coinciso con l'utilizzo sempre maggiore delle tecnologie che lo sviluppo informatico ha messo a disposizione.

Le agenzie internazionali di polizia hanno da tempo lanciato un allarme rispetto ai "cambiamenti dinamici" nei metodi di contrattazione illecita mediante l'impiego della rete, dall'utilizzo dei *social network*, all'impiego del *darkweb*.

Il traffico e lo spaccio di sostanze stupefacenti ha rappresentato l'ambito di maggior utilizzo delle tecnologie informatiche. Alle piazze

e alle strade sempre più controllate, la criminalità ha risposto organizzando una sorta di *e-commerce*, finalizzato alla vendita a domicilio. I venditori che operano all'interno dei gruppi che utilizzano servizi di messaggia criptata sono stati segnalati anche per l'uso di tecniche di *marketing*, come la promozione di sconti e quantità minime d'ordine, finalizzate all'incremento delle vendite <sup>(1)</sup>.

Il contatto tra *pusher* e clienti avviene mediante *app* di messaggistica criptata. La consegna va a buon fine per mezzo posta e gli acquisti sono effettuati mediante la moneta elettronica: dai PayPal ai bonifici bancari. In questo caso, si tratta di piccole dosi per uso personale e dell'utilizzo del c.d. "web di superficie".

Ciò che più preoccupa è l'espansione del *cybercrime*. Mediante l'accesso a siti tramite sistemi di crittografia sicuri si accede a un mercato nero che consente l'acquisto di droga con un buon margine di sicurezza. Questi sistemi, infatti, rendono estremamente difficoltosa l'identificazione dei soggetti coinvolti ed il tracciamento dei relativi pagamenti, effettuati generalmente in bitcoin o altre criptovalute.

Un'analisi del mercato *darknet* dell'OEDT condotta all'inizio della pandemia ha rivelato un aumento di attività *online*, principalmente legate ai prodotti di cannabis. Lo studio ipotizzava che gli acquirenti consolidati che cercavano la cannabis per uso personale, stessero aumentando le loro attività sulla *darknet* in previsione della chiusura. Uno studio più recente ha analizzato quasi 300 pezzi di *feedback* generati dagli utenti sulle consegne e sulla qualità della droga dalle transazioni sulla *darknet*, basate sulle voci di un sito web dedicato rivolto agli utenti dei criptomercati di droga.

Senza dubbio, il *dark web*, come ambiente nel quale nascono e crescono mercati virtuali nei quali, al di fuori di ogni regolamentazione giuridica e competenza territoriale, si conclude qualunque tipo di accordo commerciale, rappresenta il nuovo terreno di azione della criminalità. È il caso di Silk Road, lanciato nel febbraio 2011 e oggi chiuso, dove — accedendo con *browser* anonimizzati e pagando con transazioni altrettanto anonimizzate — sono stati venduti, tra le altre cose, droghe, pornografia, prodotti contraffatti, documenti falsi e armi.

Per rendersi conto della crescita esponenziale del mercato delle criptovalute, basti considerare la stima accertata da UNODC che ha

---

<sup>(1)</sup> European Monitoring Centre for Drugs and Drugs Addiction, *Impact of Covid-19 on drugs market, use, harms and drugs services in the community and prisons. Results from an EMCDDA trendspotter study*, April 2021.

segnalato una capitalizzazione di questo mercato nell'ordine di 1.800 miliardi di dollari, dal 2014 al 2022. Di questi, 10 miliardi di dollari in criptovalute, nel solo 2020, sono circolati per scopi criminali.

Il fatto che il capitale economico venga oramai accumulato anche in realtà virtuali e in valute virtuali, impone a riflettere sulla necessità di immaginare strumenti di aggressione patrimoniali nel cosiddetto “metaverso” e a ritenere che il futuro delle indagini patrimoniali sarà, in qualche modo, legato alla tecnologia della *blockchain*.

È la stessa Direzione Investigativa Antimafia ad attrarre l'attenzione su questo profilo, ricordando che « le cripto attività rappresentano, dunque, oggi un fenomeno in netta espansione che travalica i confini continentali e che è connotato da un'estesa diffusione di piattaforme che attirano un numero sempre maggiore di professionisti e investitori spinti dall'opportunità di moltiplicare i propri investimenti mediante l'acquisto di criptovalute e di NFT pur se intrisi di elevati profili di rischio » (2).

La cooperazione europea ed internazionale sempre di più si interroga su questo fenomeno che per sua natura è, più che transnazionale, “a-nazionale”, e che pertanto sfida gli strumenti fino ad ora elaborati. Sul piano nazionale, il primo tentativo di avvicinare il mondo delle criptovalute è rappresentato dai D.Lgs. 90/2017 e 125/2019, che hanno tradotto nell'ordinamento interno le previsioni in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio e di finanziamento del terrorismo contenute nella IV e la V Direttiva antiriciclaggio, a loro volta emanate in aderenza agli standard e alle linee guida in materia di valute virtuali diffuse dal FATF-GAFI (3).

Questo pacchetto normativo ha, per la prima volta, elaborato una definizione giuridicamente rilevante di “valuta virtuale”, prevedendo che tutti i soggetti che erogano servizi di piattaforme di scambio di valute virtuali (*exchangers*) e i prestatori di servizi di portafoglio digitale (*wallet service providers*) debbano adempiere ai comuni obblighi anti-riciclaggio, tra i quali quelli di adeguata verifica della clientela, di conservazione dei dati e di invio di segnalazioni di operazioni sospette.

---

(2) Direzione Investigativa Antimafia, *Relazione semestrale al Parlamento*, II semestre 2021, p. 388 ss.

(3) La Financial Action Task Force - *Groupe d'action financière*, è un'organizzazione intergovernativa fondata nel 1989 su iniziativa del G7 per sviluppare politiche di contrasto al riciclaggio di denaro. Nel 2001, il suo mandato è stato ampliato per includere il finanziamento del terrorismo.

Questi operatori sono quindi obbligati ad iscriversi in una sezione speciale del registro dei cambiavalute tenuto presso l'OAM (4). Tuttavia, come ha sottolineato nella sua ultima Relazione semestrale al Parlamento la Direzione Investigativa, « il processo evolutivo del quadro di riferimento europeo in materia di valute virtuali e più in generale di cripto attività non si è peraltro concluso. Nel delineato contesto il 24 settembre 2020, a poca distanza dall'emanazione della citata V direttiva antiriciclaggio, la Commissione europea ha presentato una proposta di Regolamento concernente gli emittenti di cripto attività non garantite e i cosiddetti *stablecoin*, nonché le piattaforme di negoziazione e i portafogli in cui sono detenute le cripto attività e cripto valute. Tale proposta, oggetto di un recente accordo provvisorio tra la Presidenza del Consiglio e il Parlamento europeo, mira a realizzare una cornice normativa per il mercato delle cripto attività dalla quale restano esclusi, per il momento, gli NFT, e si colloca in un più ampio pacchetto sulla finanza digitale teso allo sviluppo di un approccio europeo che tuteli gli investitori e la stabilità finanziaria del sistema preservando, allo stesso tempo, l'innovazione e l'attrattività del nuovo settore » (5).

Tale proposta normativa scaturisce dal lavoro che Europol sta svolgendo sul settore delle criptovalute da ormai alcuni anni, e che è sfociato anche in alcune recenti operazioni di polizia.

Nel settembre 2016, infatti, Europol, Interpol e il Basel Institute on Governance (6) hanno stabilito una *partnership* per creare un gruppo di lavoro stabile finalizzato ad approfondire il tema del riciclaggio di denaro attraverso le criptovalute, ed in particolare ad analizzare e scambiare informazioni riguardanti l'uso delle valute digitali come mezzo di riciclaggio di denaro ed il recupero dei proventi di reato conservati nella stessa forma. Rientra nei compiti del gruppo di lavoro la proposta di occasioni formative per il personale delle forze dell'ordine che necessita di costruire la propria capacità di indagine sui reati in cui sono coinvolte valute virtuali. Le previsioni di obblighi normativi

---

(4) L'OAM, istituito dal D.Lgs. 141/2010, è l'organismo competente in via esclusiva per la gestione degli elenchi degli agenti in attività finanziaria e dei mediatori creditizi. In una sezione speciale dell'elenco dedicato agli agenti in attività finanziaria sono iscritti anche gli agenti che prestano esclusivamente i servizi di pagamento.

(5) Direzione Investigativa Antimafia, Relazione semestrale al Parlamento, II semestre 2021.

(6) Il Basel Institute on Governance, fondato a Basilea nel 2003, è un'organizzazione internazionale di esperti dedicati alla prevenzione e