GIUSTIZIA INSIEME

Diritto e innovazione

La digitalizzazione della giustizia

Giuristi forensi e nuove tecnologie

di Santo Di NuovoMariavittoria CatanzaritiGianluigi CiacciElio GuarnacciaMario Valentini

Carlo Amenta

26 maggio 2025

Sommario: 1. L'intelligenza artificiale tra percezioni soggettive e regolazioni normative *(a cura di Santo Di Nuovo)* – 2. L'AI Act alla prova delle sfide globali: potenzialità e limiti di un modello regolatorio (a cura di Mariavittoria Catanzariti) – 3. Protezione dei dati personali e Intelligenza Artificiale) a cura di Gianluigi Ciacci – 4. Intelligenza Artificiale e azione amministrativa. L'articolo 30 del codice dei contratti pubblici (a cura di Elio Guarnaccia) – 5. I progetti di legge italiani per la disciplina dell'Intelligenza Artificiale (a cura di Mario Valentini) – 6. Due osservazioni (a cura di Carlo Pennisi) – 7. Conclusioni (a cura di Angelo Costanzo).

1. L'intelligenza artificiale tra percezioni soggettive e regolazioni normative *(a cura di Santo Di Nuovo)*

Una recente rassegna sul "diritto digitale guidato dall'intelligenza artificiale" [2] riassume i vantaggi dell'I.A. che possono migliorare i metodi forensi tradizionali: analizzare vasti insiemi di dati, identificare modelli complessi e automatizzare compiti ripetitivi. Al tempo stesso però evidenzia le sfide etiche e legali proposte dall'impiego dell'I.A.: tra esse, la parzialità delle catene algoritmiche, l'ammissibilità delle prove generate dall'IA in ambito giudiziario, le preoccupazioni sulla privacy degli utenti. Man mano che l'interazione tra le capacità dell'IA e le competenze umane si evolve – conclude l'autore – i professionisti del diritto devono rimanere vigili nell'affrontare le sfide associate, assicurando che le considerazioni tecniche ed etiche siano

integrate nelle nuove metodologie proposte dall'I.A. per mantenere il necessario equilibrio tra il progresso tecnologico e il mantenimento di standard etici nelle pratiche forensi.

In questa introduzione accennerò all'atteggiamento dell'utente umano verso le innovazioni basate su A.I., fonte spesso di confusione e incertezza. Esso oscilla tra l'entusiasmo per gli indubbi vantaggi e la paura di perdere il controllo delle operazioni che gli agenti intelligenti possono svolgere in autonomia. C'è chi pensa all'uso della I.A. generativa come utile aiuto per sintetizzare in tempi brevi una grande mole di dati, ma anche per ottimizzare le relazioni o le sentenze (o farle scriverle del tutto?). All'opposto ci sono i timori, derivati da spunti letterari e cinematografici, sull'eccessivo potere attribuito agli agenti artificiali, e sulla possibilità di "eterogenesi dei fini" per cui l'I.A. programmata per certi scopi poi potrebbe perseguirne altri, andando fuori controllo.

Per superare questa dicotomia – poco produttiva se radicalizzata – occorre un aumento delle conoscenze critiche sull'I.A. e le sue applicazioni; conoscenze che sono però molto complesse, per cui si finisce per affidarsi ai "tecnici" considerando le tecnologie come una "scatola nera" di cui si vedono gli esiti senza conoscerne i principi e il funzionamento.

Certo è utile che gli operatori abbiano consapevolezza dei problemi di uso, anche se non possono avere conoscenza di come la tecnologia funziona tecnicamente. Del resto, è quello che avviene quando si usano software di videoscrittura o di calcolo senza conoscere gli algoritmi che sono alla base del loro funzionamento. Quando si usa la realtà virtuale o un robot (anche quello che aiuta in cucina o nelle pulizie, o nella domotica, o nella guida dei veicoli), ma anche lo smartphone che ci accompagna in ogni momento della nostra vita, non occorre sapere come è programmata la rete neurale che ne costituisce la "mente" artificiale. Sappiamo però a che cosa servono questi strumenti "intelligenti", come possono aiutarci, e dobbiamo essere consapevoli di quali sono i loro limiti e i rischi di un cattivo uso.

Lo stesso vale per l'I.A. applicata al diritto, che peraltro include temi molto diversi tra loro:

- raccolta e analisi di big data

- automatizzazione di procedure con o senza controllo dell'operatore umano

- rilevamento di malware o di disfunzioni nei sistemi

- ottimizzazione delle reti organizzative e della condivisione di pratiche

- generazione di testi

- protezione, o indebita appropriazione, dei dati

Ognuno di questi aspetti comporta problemi diversi: tecnici (di usabilità, di accettabilità, di generalizzabilità a contesti diversi), etici e normativi. Va in ogni caso assicurata la controllabilità dell'agente artificiale per garantire le comunità di riferimento che verranno coinvolte negli usi applicativi – nell'ambito del diritto: magistrati, personale ausiliario, avvocati, periti, investigatori, ecc. – affinché gli scopi e gli esiti siano compatibili con il funzionamento e il benessere della comunità sociale. In linea con l'obiettivo ribadito dagli orientamenti etici per l'I.A. della Commissione Europea**[3]** (da cui è poi derivato l'*IAct* del 2024 in attesa di applicazione anche nel nostro Paese): creare una cultura dell'IA affidabile, che permetta a tutti di sfruttarne i vantaggi in un modo che garantisca il rispetto dei nostri valori fondamentali: i diritti fondamentali, la democrazia e lo Stato di diritto.

2. L'AI Act alla prova delle sfide globali: potenzialità e limiti di un modello regolatorio (a cura di Mariavittoria Catanzariti)

Il Regolamento EU 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 sulla AI (cosiddetto AI Act) entrato in vigore lo scorso agosto rappresenta il primo *corpus iuris* in materia di intelligenza artificiale a firma del legislatore europeo. L'UE rinsalda il suo collaudato ruolo di *first mover* regolatorio digitale, inaugurato con Regolamento Generale sulla protezione dei dati personali (GDPR), che conferma la costruzione di un modello giuridico ispirato alla compatibilità tra libertà economiche e diritti fondamentali.

I capisaldi di questo regolamento sono essenzialmente quattro: l'approccio antropocentrico fondato sulla dignità della persona, la gradualità del rischio dei sistemi di intelligenza artificiale, l'ampia portata materiale e territoriale del regolamento europeo e l'elenco dei sistemi ad alto rischio. L'architettura giuridica complessiva, tuttavia, lascia adito a non poche criticità, alcune delle quali sono oggetto delle brevi riflessioni svolte di seguito.

Sotto il primo profilo occorre precisare che il Regolamento era stato preceduto nel 2019 dalle Linee guida etiche per una intelligenza artificiale affidabile, che avevano svolto una funzione uniformatrice e preparatoria rispetto ai principi applicabili all'uso dei sistemi di intelligenza artificiale – tra i quali trasparenza, robustezza, qualità e protezione dei dati. Il controllo umano sulle decisioni automatizzate è stato inteso come baluardo della autodeterminazione informativa

in contrasto a pratiche manipolatorie. Tuttavia, gli strumenti di effettiva realizzazione del controllo umano si risolvono in meccanismi di autocertificazione obbligatoria per i sistemi di intelligenza artificiale ad alto rischio ad opera di produttori, sviluppatori e utilizzatori – sulla falsariga del modello di responsabilità da prodotto – e di adesione a codici di condotta per i sistemi non ad altro rischio. Rispetto alle violazioni dell'AI Act, infatti, non è prevista alcun tipo di interlocuzione da parte dell'individuo, né tampoco rimedi giurisdizionali specifici, salvo la possibilità di presentare un reclamo a un'autorità di vigilanza del mercato o il diritto a ottenere dall'utilizzatore spiegazioni chiare e significative sul ruolo dell'uso sistema AI nella procedura decisionale.

Con riguardo alla gradualità del rischio, l'art. 5 del Regolamento vieta l'uso dei sistemi che comportano un rischio inaccettabile, prevedendo per le imprese un obbligo di conformità entro sei mesi dall'entrata in vigore. Si tratta di sistemi utilizzati per pratiche di manipolazione, sfruttamento e controllo sociale e previsti dall'art. 5 del Regolamento, come i sistemi che utilizzano tecniche subliminali manipolatorie, che sfruttano la vulnerabilità di soggetti, che valutano o classificano le persone in base a un social scoring, che effettuano valutazioni sul rischio di commissione di reati, che ampliano banche dati di riconoscimento facciale mediante tecniche di scraping, che inferiscono emozioni personali sul luogo di lavoro e nei luoghi di istruzione, che compiono categorizzazione biometrica con finalità discriminatoria o remota in spazi accessibili al pubblico e tranne che per finalità di contrasto tassativamente previste. Anche rispetto a tali sistemi, se è vero che essi costituiscono pratiche vietate, non è chiaro che tipo di rimedi individuali specifici renda disponibili il Regolamento. Al momento l'unica norma applicabile sembrerebbe quella di cui all'art. 22 GDPR in ordine al diritto alla decisione umana, sulla quale di recente la Corte di Giustizia si è espressa delineando le caratteristiche del significato di decisioni automatizzate produttive di effetti giuridici e includendo tra esse la profilazione (C-634/21, Schufa Holding (Scoring), 7 dicembre 2023). Sembrerebbe piuttosto che la centralità dell'approccio antropocentrico si risolva in una valutazione a monte circa l'inaccettabilità del rischio che non pone l'individuo al centro di un contesto mutevole nel quale possono variare le situazioni pregiudizievoli a seconda degli interessi meritevoli ma preconfeziona una sorta di obbligazione di risultato.

In relazione all'ampia portata dell'AI Act, va osservato che esso si applica dal punto di vista territoriale e materiale tanto alla immissione sul mercato (distribuzione e uso nel corso di attività commerciali) quanto alla messa in servizio nel mercato UE (fornitura all'utilizzatore per il primo uso) da parte di utilizzatori anche se non stabiliti o ubicati all'interno dell'UE di sistemi di IA o modelli di IA per finalità generali nell'Unione, utilizzatori stabiliti o ubicati all'interno

dell'UE, importatori e distributori di sistemi AI, fabbricanti di prodotti che immettono sul mercato o mettono in servizio un sistema di IA insieme al loro prodotto e con il loro nome o marchio, rappresentanti dei fornitori non stabiliti in UE, persone interessate che si trovano in UE, fornitori e utilizzatori nell'Unione stabiliti o ubicati in un paese terzo, qualora l'*output* prodotto sia utilizzato nell'UE. Si prevede sostanzialmente un ambito di applicazione esteso persino agli output prodotti in Europa, con evidente difficoltà di inquadramento del fatto giuridico nello spazio e nel tempo in ossequio al principio di certezza del diritto, in quanto un output di un sistema di AI può addirittura riferirsi a un'utilizzazione diluita nel tempo dei risultati indipendentemente dalla utilizzazione del sistema stesso in Europa. Tra le deroghe si annoverano la sicurezza nazionale, la difesa e l'uso militare – con evidenti discrasie in ordine al dual use, mentre sono esenti dall'applicazione dell'AI Act le autorità pubbliche di paesi terzi e organizzazioni internazionali.

Ultimo profilo, non di poco conto, riguarda l'elenco di cui all'Allegato III sui sistemi ad alto rischio, considerati legittimi, per i quali vige un obbligo di certificazione, che può essere aggiornato nel tempo dalla Commissione, con ulteriori profili dubbi ancora una volta in ordine alla certezza del diritto. Tra i settori più problematici si evidenziano quelli relativi allo scoring lavorativo e all'accesso alle prestazioni pubbliche essenziali in ordine alla valutazione dell'affidabilità creditizia, nonché quelli relativi all'amministrazione della giustizia e ai processi democratici. In particolare, con riguardo a questi ultimi, appare molto labile la previsione normativa che circoscrive l'applicabilità delle previsioni relative ai sistemi ad alto rischio alla sola attività di supporto alla decisione giudiziale, identificato nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti, ma non esprimendosi nettamente sul punto e lasciando ampio spazio alla interpretazione.

Le perplessità sono dunque molteplici a fronte di un successo regolatorio indiscutibile che tuttavia invita all'esercizio della consapevolezza.

3. Protezione dei dati personali e Intelligenza Artificiale) a cura di Gianluigi Ciacci

Lo sviluppo di un'attenzione "diffusa" per l'IA, conseguenza anche del moltiplicarsi delle sue applicazioni nella quotidianità degli utenti (si pensi ad esempio agli assistenti virtuali nei cellulari o in *device* casalinghi, ed all'"esplosione" dei *chatbot* e dell'intelligenza artificiale generativa), oltre a portarla al di fuori della discussione tra esperti, ha fatto nascere un dibattito sulla necessità di trovare un equilibrio fra due opposte esigenze:

– non rallentare, o addirittura bloccare, il progresso del settore, e quindi le conseguenze positive dello stesso (e poi sì, anche l'enorme business da essa resa possibile direttamente, per il valore in sé dell'IA e, indirettamente, per la ricchezza prodotta dalle sue applicazioni);

– impedire che tale progresso avvenga in danno dei suoi utenti.

Dicotomia che raggiunge una forte criticità, da una parte, proprio nel momento in cui dal suo sviluppo dipendono enormi interessi economici ("aumentando la posta in gioco"); e, dall'altra, quando il danno agli utenti riguarda i loro dati personali: in questo secondo caso soprattutto a causa della presenza di una normativa forte, rappresentata dal Regolamento UE 27 aprile 2016, n. 679 (il c.d. GDPR), finalizzata proprio a prevenire, o comunque limitare, tale danno. Infatti questa disciplina applicata ai sistemi di I.A. incontra diversi problemi, che rendono il rispetto degli obblighi da essa dettati estremamente complesso per i titolari di trattamento che usano, in diverse realtà, tali sistemi.

Per risolvere tali difficoltà applicative, ci si deve muovere dall'analisi del contesto normativo che oggi regolamenta l'I.A. e le sue applicazioni, attraverso la conoscenza approfondita della disciplina in materia di protezione dei dati personali, per poi arrivare a "tracciare" la strada da seguire.

Così, con riferimento alle prime norme dettate per le macchine intelligenti, la loro analisi dimostra come siano sempre presenti riferimenti, più o meno specifici, alla tutela delle informazioni relative agli individui: riferimenti che ribadiscono e sottolineano l'importanza del rispetto dei diritti fondamentali dell'individuo, in particolare quello alla protezione dei suoi dati personali, anche nella realtà delle applicazioni dell'I.A.. Situazione che pone il contrasto indicato non tanto e non solo nella dicotomia "applico/non applico", ma anche nella più ampia scelta tra "rispetto/non rispetto" la legge: e allora non si può certo ritenere ammissibile la rinuncia alla legalità, e nella specie a tale protezione.

Provando allora ad immaginare le possibili soluzioni a tale contrasto, le "cose da fare", indichiamo tre differenti ambiti.

Innanzitutto, dal punta di vista dei "*player*" del settore, cioè da un lato i produttori/fornitori di sistemi di I.A., dall'altro gli utilizzatori di tali sistemi (comunque tutti "titolari del trattamento" se questi vengono applicati ad informazioni relative a dati personali), questi devono essere portati ad adeguarsi obbligatoriamente e in maniera corretta ed effettiva al sistema della protezione dei dati personali introdotto dal Regolamento 2016/679, ognuno nell'ambito della propria attività di trattamento di tali dati.

Con riferimento poi agli utenti delle macchine intelligenti, occorre sviluppare il più possibile una tutela "dal basso", cioè posta in essere dagli stessi interessati che, in maniera più o meno consapevole, cedono i loro dati ai *player* citati: tutela che deve partire dalla loro corretta ed efficace informazione e formazione, in generale sulla realtà digitale in cui vivono, ma anche in particolare su quella del trattamento dei dati personali, sugli utilizzi che se ne fanno nei sistemi di intelligenza artificiale, e quindi sulle modalità della loro tutela. Portandoli in questo modo a realizzare che non possono più essere solo passivi fruitori della sempre più pervasiva innovazione tecnologica, né d'altro canto "tecno-entusiasti" senza alcun senso critico: ma che devono diventare "tecno-consapevoli", capaci così di gestire tale innovazione, e dunque di proteggere i propri diritti fondamentali, non ultimo per evitare di essere gestiti da essa.

Infine, si ritiene necessario potenziare il più possibile anche la tutela "dall'alto", sia a livello normativo, realizzando discipline che non si limitino solo a semplici richiami o ad affermazioni generali di principio, ma che individuino regole certe ed efficaci; sia rispetto alle Autorità di controllo (nel nostro Paese il Garante per la protezione dei dati personali), in particolare potenziandole e rendendole maggiormente operative. Dando quindi a queste ultime la possibilità di fornire un concreto ausilio per la realizzazione di quanto appena riportato: e dunque di condurre all'adeguamento alla disciplina normativa, in maniera qualitativamente migliore, i citati "*player*" del settore e, allo stesso tempo, di rendere consapevoli il maggior numero possibile di interessati.

Soluzioni sicuramente ambiziose, e allo stesso tempo di difficile realizzazione, e comunque non in tempi brevi. Ma occorre capire innanzitutto che, a fronte della repentina evoluzione delle macchine intelligenti, sempre più potenti ed invasive della nostra sfera privata, non si può non fare qualcosa per giungere alla soluzione del contrasto tra sviluppo dell'I.A. e protezione dei dati. E questo avendo ben chiaro che il problema in realtà si pone su un livello più alto di quanto possa sembrare: in particolare quello tra la limitazione, o addirittura la rinuncia a un diritto fondamentale dell'individuo per l'importanza (economica) del settore, il cui sviluppo può comunque avere indubbi vantaggi per tutti noi, ed in ogni caso è oramai impossibile fermare.

Per questo motivo la soluzione sembra essere fondamentalmente quella di un "salto culturale", giuridico e tecnologico, finalizzato a portare al 100% di successo il sistema di protezione dei dati personali, quale contrappeso e limite rispetto agli innovativi (e di moda) sistemi di intelligenza artificiale. Sfruttando in questo modo le utilità che possono apportare alla nostra vita, senza doverne subire necessariamente gli aspetti negativi .

4. Intelligenza Artificiale e azione amministrativa. L'articolo 30 del codice dei contratti pubblici (a cura di Elio Guarnaccia)

La digitalizzazione della pubblica amministrazione, avviata normativamente nel 1997 con il decreto legislativo che ha disciplinato per prima volta in Europa la firma digitale, vive un periodo di profonda maturazione, sia in conseguenza dell'ormai piena attuazione del codice dell'amministrazione digitale, il decreto legislativo 82 del 2005, sia, proprio con riferimento agli appalti pubblici, alla luce dell'intera digitalizzazione del ciclo di vita dei contratti pubblici voluta dal decreto legislativo 36 del 2023.

E infatti, il corpus normativo attualmente vigente in materia di appalti pubblici, ha inteso prevedere in modo generalizzato e vincolante per tutte le pubbliche amministrazioni la digitalizzazione di tutti gli step del procedimento di approvvigionamento pubblico, ossia programmazione, progettazione, pubblicazione, affidamento ed esecuzione. E ciò non in esecuzione di nuove direttive comunitarie, ma sulla scorta del cd. principio del risultato, nel quadro della spinta voluta dal PNRR per la ripresa del nostro paese dopo la pandemia, e comunque in piena conformità con i principi, gli strumenti e le regole imposti dal codice dell'amministrazione digitale nel settore della transizione digitale della PA.

Ed è proprio un articolo del codice contratti pubblici, l'articolo 30, l'unica norma di legge vigente del nostro ordinamento giuridico, che si occupa di intelligenza artificiale. E lo fa esprimendo una preferenza verso la scelta delle stazioni appaltanti di *"automatizzare le proprie attività ricorrendo a soluzioni tecnologiche, ivi incluse l'intelligenza artificiale e le tecnologie di registri distribuiti".*

Ma questa preferenza viene espressa mantenendo fermo l'ormai consolidato rapporto di strumentalità tra uso dell'informatica e efficienza dell'azione amministrativa, specificando infatti che l'adozione di applicativi di AI deve essere in ogni caso volta a *"migliorare l'efficienza"*, così come d'altronde ritroviamo all'art. 3bis della legge n. 241\90, laddove già il legislatore del 2005 sanciva che *"le amministrazioni pubbliche agiscono mediante strumenti informatici e telematici ... per conseguire maggiore efficienza nella loro attività".*

La norma in commento, dunque, disciplina espressamente le regole che le stazioni appaltanti devono seguire per inglobare nelle piattaforme di approvvigionamento digitale -la via maestra per l'espletamento delle gare d'appalto, segnata dall'art. 25 del codice- specifici applicativi di

intelligenza artificiale.

In particolare, il comma 2 prevede che, nell'acquisto di soluzioni di AI, le stazioni appaltanti devono prioritariamente assicurare *"la disponibilità del codice sorgente"*, inclusa la relativa documentazione ed ogni altro elemento utile a comprenderne le logiche di funzionamento.

È evidente dunque l'esigenza del legislatore di garantire alla PA committente maggiore trasparenza e conoscibilità possibile dell'algoritmo, che al tal fine opera un'evidente inversione di tendenza rispetto all'art. 68 CAD, che invece, nel prevedere l'acquisto da parte delle pubbliche amministrazioni di programmi informatici, i cd. *software* -nel cui ambito devono annoverarsi le soluzioni algoritmiche e automatizzate- indicava come soluzione preferibile il *"software sviluppato per conto della pubblica amministrazione"*, relegando al terzo posto, dopo il riutilizzo di software, il software a codice sorgente aperto.

Ma l'art. 30 si spinge oltre: recependo la giurisprudenza amministrativa già stratificatasi sul punto, essa infatti prevede quali debbano essere le caratteristiche necessarie che devono avere i provvedimenti amministrativi formati con l'intelligenza artificiale: a) conoscibilità e comprensibilità, b) non esclusività, c) non discriminazione.

Si tratta, dunque, di una norma primaria di grande portata. E ciò anche perché la sua formulazione di fatto la fa diventare paletto normativo da seguire per qualsiasi procedura di acquisto pubblico di intelligenza artificiale, e per di più a prescindere dall'utilizzo a cui l'AI verrà destinata dalla pubblica

5. I progetti di legge italiani per la disciplina dell'Intelligenza Artificiale (a cura di Mario Valentini)

Introduzione

Il Disegno di Legge (DDL) sull'Intelligenza Artificiale, presentato al Senato il 20 maggio 2024, ha l'obiettivo di bilanciare le opportunità offerte dalle nuove tecnologie con i rischi legati al loro uso improprio. Questo provvedimento, composto da 27 articoli e suddiviso in 6 capi, affronta una serie di temi cruciali per la regolamentazione dell'IA in Italia. Tra questi, si trovano i principi e le finalità dell'IA, le disposizioni di settore, la strategia nazionale, la tutela degli utenti, il diritto

d'autore, le disposizioni penali e quelle finanziarie.

Il DDL è stato approvato dal Senato il 20 marzo 2025 e attende ora la discussione alla Camera dei deputati. Un concetto chiave del disegno di legge è l'autonomia: l'IA è vista come uno strumento che coadiuva le decisioni umane senza sostituirle, promuovendo lo sviluppo di sistemi comprensibili e tecnologicamente avanzati. Questo approccio vuole garantire che le decisioni automatizzate siano sempre controllate dall'autodeterminazione umana.

1. Dalle prescrizioni etiche allo sviluppo economico

Gli articoli 3, 4 e 5 stabiliscono le prescrizioni etiche e operative per l'IA in Italia, concentrandosi su dignità umana, sicurezza e trasparenza, e promuovendo lo sviluppo economico.

2. Salute, lavoro e giustizia: il Capo II del DDL Intelligenza artificiale

Il Capo II del DDL riguarda l'uso dell'IA in sanità, lavoro e giustizia, migliorando efficienza e trasparenza. L'articolo 7 disciplina l'uso dell'IA nel settore sanitario, mentre l'articolo 10 regola l'uso dell'IA nel settore lavorativo.

3. Difesa e sicurezza nazionale

Il DDL prevede l'uso dell'IA nella difesa e sicurezza nazionale per monitorare minacce, proteggere dati e gestire emergenze informatiche. Include strumenti per il disaster recovery e il miglioramento della cybersicurezza. L'articolo 6 esclude le attività di IA legate alla sicurezza nazionale dalla normativa generale. I sistemi di IA destinati all'uso pubblico devono essere installati su server ubicati in Italia per garantire la sicurezza dei dati sensibili.

4. Strategia e governance

Il DDL assegna la governance dell'IA ad AgID e ACN, una decisione contestata da alcune associazioni per i diritti digitali che preferivano un'autorità indipendente. Il Garante della Privacy ha evidenziato la mancanza di un ente autorizzato per i sistemi di identificazione biometrica in tempo reale e si è candidato per questo ruolo. Le opposizioni propongono la creazione di vari osservatori e commissioni, tra cui un Osservatorio sui Diritti Digitali a Palazzo Chigi, una commissione per l'uso dell'IA in ambito giudiziario, una commissione dati, analisi e la ricerca clinica presso il Ministero della Salute.

5. Investimenti nell'IA

L'articolo 21 delinea gli investimenti nei settori dell'IA, cybersicurezza e calcolo quantistico. Il governo ha previsto un fondo da 1 miliardo di euro, gestito da Cdp Venture Capital Sgr, per

sostenere lo sviluppo dell'IA in Italia. Questo fondo è destinato sia alle PMI che alle grandi aziende per favorire ricerca e innovazione. Tuttavia, l'apertura del fondo a investitori stranieri ha suscitato dibattiti sulla tutela dell'industria nazionale e il controllo strategico delle tecnologie emergenti.

6. Sistema sanzionatorio

L'articolo 25 del DDL apporta modifiche al Codice penale, inasprendo le pene per reati commessi mediante l'uso dell'IA. Le aggravanti sono previste quando l'IA costituisce un mezzo insidioso, ostacola la difesa pubblica e privata, o peggiora le conseguenze del reato. Viene introdotto il reato di "Illecita diffusione di contenuti generati o alterati con sistemi di IA" (articolo 612-quater), punendo chi causa danni ingiusti, diffondendo immagini, video o voci falsificati o alterati senza consenso, utilizzando l'IA.

Il DDL Intelligenza Artificiale è stato approvato lo scorso 20 marzo 2025 al Senato e si attende ora la sua discussione alla Camera dei deputati.

6. Due osservazioni (a cura di Carlo Pennisi)

Dal punto di vista sociologico si tratta di due questioni connesse, sul piano culturale, tecnico e normativo.

La prima riguarda un aspetto del carattere performativo che rivestono gli strumenti di cui si parla rispetto alle decisioni in cui vengono coinvolti, sia che si propongano in forma di piattaforme, di software o di chatbot. Ciascuno di questi strumenti, in effetti, sembra andare oltre la predisposizione delle alternative decisionali, la contestuale riduzione e moltiplicazione degli ambiti di interrogazione o di applicazione. Ciascuno di essi deriva infatti da un processo di digitalizzazione della realtà e della sua rappresentazione (testuale o iconica) che, in attesa degli sviluppi operativi della logica quantistica, implica selezioni, classificazioni, tipizzazioni e generalizzazioni volte ad adeguare al carattere binario dell’universo digitale ciascuna delle dimensioni di realtà interessate; volte a rendere “discrete” dimensioni della realtà che devono spesso la propria identità al loro carattere continuo (comunicazioni, interazioni, emozioni, sentimenti, i loro processi e gli esiti).

In questo senso, il carattere performativo di tali strumenti si realizza anche, pur suscitando meno attenzione e dibattito, sul piano cognitivo, sul piano della determinazione dei contenuti sui quali si esercita la decisione alla quale vengono dedicati questi strumenti (definizioni,

imputazioni, previsioni, acquisti, ma anche formulazioni di testi).

Nell'ambito della pratica giuridica il ruolo cognitivo di questi strumenti non può essere sottovalutato. Può comportare che l'attribuzione di significato normativo, ad una prescrizione la cui fattispecie sia derivata da processi di quel tipo, sfugga alla normatività che le deriva dalla sua qualificazione giuridica e venga piuttosto derivata dallo stato di fatto digitalmente predefinito – molta della logica "evidence based" non sfugge a questo rischio. La performatività sul cognitivo compiuta dal digitale può così risultare una sottrazione di potere normativo all'ordinamento a favore di un passaggio che si rivela certamente di potere ma la cui autorità, la cui legittimazione istituzionale, rimane ancora da verificare.

La seconda questione ha a che fare con quello che si dice "uso consapevole" di queste tecnologie, quale strumento di prudenza e di difesa dalle loro eventuali distorsioni. Al di là dell'auspicio, questa indicazione di solito fa riferimento alla consapevolezza relativa all'oggetto di cui si parla, ossia ancora i software, il loro funzionamento e le loro regole. È una prospettiva comprensibile dal punto di vista professionale. Poiché si tratta di strumenti, la responsabilità nel loro uso impone prudenza e conoscenza, quindi informazione e formazione continua.

Tuttavia, l'aspetto della consapevolezza sul quale occorre richiamare l'attenzione, anche rispetto a quanto già osservato, ha a che fare con la specifica dimensione riflessiva dell'esercizio professionale. Un approccio professionale nei confronti della tecnologia impone anche un atteggiamento autocontrollato sulla professione che sorregga e dia contenuto al carattere, appunto, "strumentale" della tecnologia rispetto ai fini, al quadro normativo ed empirico nel cui ambito si realizza l'esercizio professionale.

Tale carattere strumentale, tuttavia, rimane tale solo sino a quando l'uso della tecnologia risulta decidibile. Su questa decidibilità si conserva, professionalmente, il carattere di strumento della tecnologia. Interrogarsi soltanto sulla semplice "utilità" delle tecnologie che si propongono alle pratiche professionali, sul risparmio di tempo, sulle loro potenzialità economiche, può celare, paradossalmente, proprio il loro carattere strumentale, ossia il fatto che vengono scelte e adoperate in vista di un obiettivo, di un fine che, professionalmente non può essere solo individuale. E celare il loro carattere strumentale significa divenirne "utenti", ossia operatori "configurati" dalle regole e dalle decisioni del software.

Ora, se nell'uso quotidiano questa configurazione da *utente* molte volte risulta inevitabile (con tutte le conseguenze che la ricerca ha messo in luce), nell'uso professionale finisce col risultare contraddittoria proprio con la dimensione professionale della pratica entro cui si realizza il

ricorso al software. Perché, in effetti, non si è soli dinanzi a questi strumenti, e meno che mai lo si è da professionisti. Anche solo la disponibilità del loro uso è frutto di una o più decisioni già prese da altri – e capire in quale veste sarebbe già informativo.

Ma, soprattutto, la decisione di adoperarli è compiuta nell'ambito di un esercizio di ruolo che non può essere concepito esclusivamente sul piano individuale e psicologico (come talvolta rischia di fare generalizzando la problematica della relazione uomo-macchina). In quest'ambito, la decisione di servirsi di tecnologia, e il modo in cui lo si fa, è parte di una pratica che possa dirsi professionale nella misura in cui è configurata dall'ordinamento entro il quale quel ruolo assume senso e identità. Questa condizione non è esclusivamente normativa, ma si specifica in molteplici dimensioni: l'organizzazione pubblica di cui si è parte o con la quale si è in relazione, le prassi procedimentali e processuali nelle quali si opera, le scelte deontologiche e regolatorie dell'ordine professionale al quale si appartiene, le pratiche di studio consolidate, le relazioni con il cliente. Ciascuna di queste dimensioni operative e normative interagisce con tutte le altre e definisce nel concreto la selettività specifica, di fatto e normativa, in cui si realizza l'uso dei software che si rendono disponibili al professionista.

Da questo punto di vista, la consapevolezza non riguarda più soltanto l'oggetto ma, appunto, il suo carattere strumentale rispetto agli obiettivi, ai fini e, va detto, rispetto ai valori, ai quali è orientato ciascuno degli ambiti normativi e di pratiche entro i quali assume senso l'esercizio professionale. In altri termini, la consapevolezza riguarda anche il quadro di istituzioni sociali e giuridiche che danno senso, orientamento normativo e valore all'esercizio professionale, perché è solo in riferimento a queste dimensioni che si definisce in senso proprio il carattere strumentale nell'uso della tecnologia.

Tale consapevolezza, motore della riflessività della pratica professionale, assume rilevanza in due direzioni inseparabili. Per un verso, rende progressivamente chiare le sfide ed i cambiamenti necessari nel quadro istituzionale e normativo che orienta l'esercizio professionale, sul piano dei fini e dei loro rapporti con i mezzi disponibili. Per un altro verso sollecita il professionista a mantenere soltanto strumentale il proprio rapporto con la tecnologia, rapportandone gli usi che gli sono possibili ai fini ed al quadro istituzionale entro cui si muove.

La tecnologia trasforma le professioni, gli ordinamenti, i ruoli e le pratiche non per una propria forza, ma attraverso l'uso che se ne compie e, soprattutto, attraverso modalità che riescono o meno a salvaguardare ciascuno degli obiettivi specifici dei livelli di senso, empirici e normativi,

entro cui il professionista esercita il proprio ruolo.

7. Conclusioni (a cura di Angelo Costanzo)

L’espressione «intelligenza artificiale» (coniata durante il convegno di Dartmouth nel 1956), mentre esprime correttamente la natura artificiale dei sistemi che vengono così denominati, inganna circa le sue vere capacità.

Converrebbe, allora, abituarsi a riconsiderare i diversi strumenti offerti dalla cosiddetta *intelligenza artificiale*, dando loro nomi aderenti alle variegate realtà in cui si articolano.

In generale, potremmo parlare di forme di «razionalità algoritmica a base elettronico-silicea». Oppure nel caso di sistemi che, con strumenti matematici scoprono schemi in miriadi di dati e poi trasformano i risultati nel linguaggio simbolico o nel linguaggio scritto usare (ma forse non avrebbe successo...) l’espressione, da qualcuno proposta, «sintetizzatori di schemi antropoglossi».

Il diritto guidato dall'intelligenza artificiale offre nuove risorse e comporta nuovi impegni per i giuristi, specialmente in relazione alla IA generativa.

Infatti, è evidente che chi usa questi strumenti, sebbene non possa avere la conoscenza che appartiene agli esperti del settore, dovrebbe comunque essere nella condizione di comprendere i meccanismi di funzionamento.

Fondamentale è comprendere quali sono gli scarti fra i criteri che si utilizzano quando ci si serve della sola intelligenza umana e quelli sulla base dei quali funzionano gli strumenti offertigli dalla IA.

Il modello giuridico che regge il cosiddetto *AI Act* europeo enfatizza, fra i suoi punti essenziali, un’approccio antropocentrico alla IA e si preoccupa della compatibilità tra la libertà economica nella produzione e nel diffusione dei nuovi strumenti e il rispetto dei diritti fondamentali. In questa prospettiva, delinea i rischi accettabili e quelli inaccettabili.

Tuttavia, restano da definire concretamente i percorsi attraverso i quali gli enti (privati o pubblici) che svilupperanno i sistemi saranno in grado di comprendere per tempo se e come il loro impegno di risorse umane e economiche riceverà il lasciapassare dalle autorità preposte al

controllo del settore.

Inoltre, rimane ardua la soluzione del problema della efficacia delle regole europee rispetto ai sistemi provenienti dall'esterno dell'Unione.

Occorrerà vedere, ancora, con quali diverse declinazioni le legislazioni nazionali specificheranno i contenuti delle regolamentazione europea.

In Italia, il disegno di legge sulla IA, in corso di approvazione, ribadisce il principio che le decisioni automatizzate devono essere sempre controllate dal decisore umano nei settori della salute, della lavoro e della giustizia. Prefigura una disciplina derogatoria per le attività di IA connesse alla sicurezza nazionale dalla normativa generale. Assegna la governance dell'IA ad Agi e ACN. Prevede un fondo per sostenere favorire in Italia la ricerca e l'innovazione in materia.

Intanto, nel mercato, gli enormi interessi economici in campo possono condurre a situazioni che travalicano gli interessi degli utenti, particolarmente per quel che riguarda la protezione dei loro dati personali, che va sempre ricordato si realizza anzitutto attraverso la *tecno-consapevolezza* da parte degli utenti.

In questo ambito, in Italia, l'azione del Garante per la protezione dei dati personali andrebbe potenziata e resa più diffusamente conoscibile dal pubblico.

Gli strumenti della IA offrono sempre più rilevanti possibilità di utilizzo alla Pubblica amministrazione, che costituisce la sede nella quale la loro implementazione e i loro controllo possono essere ottimali.

Per altro verso, nello svolgimento delle professioni, gli strumenti di IA possiedono una forza performativa che deriva da una *digitalizzazione* delle rappresentazioni della realtà che incide della determinazione dei contenuti delle decisioni raggiunte (anche) tramite questi strumenti: per esempio, questo può produrre distorsioni nella interpretazione delle norme e, quindi, una dislocazione dei poteri normativi a agenti non legittimati.

Inoltre, in vari modi gli strumenti della possono modificare i profili delle professioni intellettuali nei diversi settori giuridici, in che implica scelte deontologiche e regolatorie che non andrebbero lasciate ai singoli professionisti, ma esercitate dagli ordini professionali in relazione ai valori sociali ai quali si ispirano le professioni.

[1] Incontro del 4 marzo 2025 promosso dal Centro di ricerca sulla giustizia dei minori e della famiglia “Enzo Zappalà” dell’Università di Catania.

[2] R. T. Yadav, AI-Driven Digital Forensics. *International Journal of Scientific Research & Engineering Trends*, Vol. 10 (2024), Issue 4, pp. 1673-1681.

[3] European Commission. *Ethics guidelines for trustworthy AI*, 2019. **https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai**.