
Estratto

Estratto da un prodotto in vendita su **ShopWKI**, il negozio online di Wolters Kluwer Italia

Vai alla scheda →

Wolters Kluwer opera nel mercato dell'editoria professionale, del software, della formazione e dei servizi con i marchi: IPSOA, CEDAM, Altalex, UTET Giuridica, il fisco.



Wolters Kluwer

Capitolo I

INTELLIGENZA ARTIFICIALE E DIRITTO

Sommario: 1. Intelligenza artificiale: un'introduzione storica 2. Origini dell'intelligenza artificiale applicata al diritto 3. Intelligenza artificiale: tentativi di definizione del fenomeno 4. La regolamentazione dell'intelligenza artificiale: gli interventi negli Stati Uniti e Cina 4.1. Segue. Le proposte sovranazionali 5. Il contesto europeo: il percorso verso l'AI Act 6. Il Regolamento UE n. 2024/1689 di regole armonizzate per l'intelligenza artificiale (AI ACT) 6.1. Definizioni, scopo ed ambito di applicazione 6.2. Sistemi di AI proibiti: le pratiche vietate di intelligenza artificiale 6.3. Sistemi di AI ad alto rischio: definizione e disciplina 6.4. Gli obblighi di trasparenza 6.5. Le misure a sostegno dell'innovazione 6.6. *Governance*, applicazione e sanzioni 7. Intelligenza artificiale e proprietà intellettuale 7.1. Segue. Le soluzioni interpretative più recenti e i casi giudiziari 8. Intelligenza artificiale e protezione dei dati personali 8.1. I rapporti tra AI Act e GDPR 9. La disciplina nazionale: il disegno di legge in Italia in materia di intelligenza artificiale

I. INTELLIGENZA ARTIFICIALE: UN'INTRODUZIONE STORICA

Un'indagine sull'intelligenza artificiale deve, necessariamente, definire l'oggetto su cui focalizzare la propria analisi.

Per far ciò appare necessario ripercorrere quelle che sono state le varie tappe dell'evoluzione scientifica e tecnologica che hanno portato ai risultati che consentono, oggi, di costruire sistemi così avanzati che interagiscono attraverso applicazioni *software*, sembrando quasi dotati della capacità di sviluppare un pensiero autonomo.

La storia dell'intelligenza artificiale è strettamente legata all'evoluzione della conoscenza dell'uomo in vari settori: la filosofia, la matematica, l'economia, le neuroscienze, la psicologia, l'ingegneria informatica, la cibernetica e la linguistica¹.

In tutti questi ambiti, gradualmente, si è giunti a comprendere sempre di più come rappresentare la conoscenza e come realizzare dei sistemi informatici, modellati sul cervello umano, che riuscissero ad elaborarla modellando questo nostro fantastico organo.

Storicamente la nascita del concetto di intelligenza artificiale è fatta risalire ad un lavoro pubblicato nel 1943² in cui veniva proposto un modello a rete di neuroni artificiali in cui, a seconda dello stato di ciascuno di essi, che poteva variare sulla base degli stimoli propagati da quelli adiacenti, era possibile calcolare ogni funzione computabile (rifacendosi alla teoria della computazione di Alan Turing) potendo anche implementare tutti gli operatori logici della logica formale.

Il primo computer basato sul concetto di reti neurali fu costruito nel 1950, da Marvin Minsky e Dean Edmonds e venne da loro denominato SNARC. Minsky, che può essere considerato uno dei padri dell'intelligenza artificiale, concentrò poi il suo lavoro di ricerca sulla computazione universale delle reti neurali ed aveva come mentore von Neumann, considerato uno dei matematici più influenti del secolo scorso.

¹ Per un'analisi dell'apporto di ciascuna di queste branche del sapere all'evoluzione dell'intelligenza artificiale vd. S. Russell, P. Novig, *Intelligenza artificiale. Un approccio moderno*, Milano, 2021, pagg. 8 ss.

² W. S. McCulloch, W. Pitts, *A logical calculus of the ideas immanent in nervous activity*, in *The bulletin of mathematical biophysics*, 1943, 5, pagg. 115 - 133.

Ma la vera svolta concettuale arrivò con la pubblicazione da parte di Alan M. Turing, nel 1950, del saggio *Computing Machinery and Intelligence*, in cui il grande scienziato avanzò concetti quali l'apprendimento automatico e per rinforzo, gli algoritmi genetici e il famigerato test di Turing³.

Turing nel suo saggio suggeriva, con una visione lucida di quello che in effetti poi sarebbe accaduto nel futuro, che sarebbe stato più efficiente implementare degli algoritmi di apprendimento da insegnare alla macchina piuttosto che cercare di tentare di codificare la conoscenza della stessa attraverso la logica simbolica.

Ma la nascita del termine “intelligenza artificiale” si deve a John McCarthy che riuscì a riunire al Dartmouth College di Hannover nel 1956 i ricercatori statunitensi interessati a questo tema (in totale una decina, tra cui Minsky e Claude Shannon) in una conferenza con l'obiettivo di dimostrare che era possibile costruire una macchina in grado di simulare la conoscenza umana.

Il frutto di quella riunione fu la creazione del *Logic Theorist*, un sistema per la risoluzione dei problemi matematici creato da Newell e Simon. Essi poi, basandosi sull'ipotesi che denominarono “**sistema fisico dei simboli**” crearono il *General Problem Solver*, che cercava di imitare l'approccio degli esseri umani nel pensiero. Si trattava, quindi, di un approccio simbolico secondo il quale, alla macchina venivano fornite delle “regole di ragionamento” attraverso la logica simbolica ed essa riusciva a risolvere dei problemi in determinati campi.

Un metodo diverso fu adottato da Arthur Samuel, che programmò nel 1956 un **software automatico per il gioco della dama** attraverso tecniche simili a quelle che oggi vengono definite *reinforcement learning*, con le difficoltà derivanti dalle limitate capacità computazionali dei computer di allora.

Dal 1958 al 1966 si assistette ad una netta divisione tra coloro che ricercavano soluzioni teoriche ai problemi attraverso la logica formale e coloro che cercavano soluzioni pratiche per far funzionare i programmi. Così McCarthy definì il linguaggio di programmazione Lisp, destinato ad essere utilizzato nei successivi 30 anni per implementare programmi di intelligenza artificiale, mentre Minsky al MIT svolgeva ricerche con i propri studenti occupandosi di domini limitati, i c.d. **micromondi**, in cui venivano implementati programmi *software* specifici per risolvere compiti ristretti e ben definiti (tra cui i primi progetti di visione artificiale).

Nei 10 anni successivi, ossia fino al 1973, ci si accorse però che, mentre i programmi di intelligenza artificiale riuscivano a sembrare abbastanza efficienti nel risolvere problemi semplici, all'aumentare della complessità i risultati erano fallimentari. Il problema principale risiedeva nell'approccio formalistico che si era adottato, cercando di codificare le regole di ragionamento e facendo svolgere alla macchina una serie di tentativi per la risoluzione di un determinato problema. Ciò non teneva conto della complessità che i problemi possono assumere nel momento in cui aumentano le variabili da considerare, non essendo sufficiente aumentare le capacità computazionali dell'*hardware* della macchina, ma dovendo, evidentemente, adottare un approccio diverso nella costruzione dell'algoritmo (il c.d. problema della “**esplosione combinatoria**”). Si trattava dei c.d. metodi deboli, perché, seppur non limita-

³ A. M. Turing, *Computing Machinery and Intelligence*, in *Mind*, 59, 236, 1950. A. M. Turing, *Calcolatori e intelligenza*, in D. R. Hofstadter, D. C. Dennett (a cura di) *L'io della mente*, Milano, 1985, pagg. 61-100.

ti ad un singolo dominio, non riuscivano a risultare efficienti all'accrescere della complessità.

Questi risultati non confortanti ebbero la conseguenza di far calare l'interesse da parte dei governi, con conseguente taglio dei finanziamenti alla ricerca sull'intelligenza artificiale.

Dal 1969 fino al 1986 prese piede un diverso metodo volto a costruire dei modelli di programmi molto potenti, ma con una competenza verticale su domini di conoscenza ristretti. Si tratta di quelli che furono denominati “**sistemi esperti**”, in cui si tentava di inserire ogni possibile conoscenza di un determinato dominio programmando direttamente le varie possibili casistiche che si potevano presentare. Quello che ottenne più successo commerciale fu R1 (1982), che aiutava la configurazione di sistemi informatici, e modelli analoghi già nel 1988 venivano utilizzati da alcune case farmaceutiche.

Tutto ciò portò alla rapida diffusione di linguaggi informatici per la rappresentazione della conoscenza e del ragionamento, tra cui i più famosi sono il Prolog e il Planner. Anche alcuni governi ripresero il loro interesse per l'intelligenza artificiale, ma dopo un periodo di entusiasmo le difficoltà nella costruzione e governo di sistemi esperti per domini complessi, compresi i limiti degli stessi derivanti dall'incapacità di gestire l'incertezza o di apprendere dall'esperienza - ed il fallimento di molte aziende che si erano dedicate alla costruzione di questi tipi di sistemi - diedero l'avvio a quello che fu chiamato “l'inverno dell'IA”.

Nella seconda metà degli anni '80 dello scorso secolo, il sostanziale insuccesso dei c.d. sistemi esperti determinò un cambiamento di approccio nell'affrontare i problemi di automazione. Da una parte, fu perfezionato l'algoritmo di apprendimento basato sulla retropropagazione, sviluppato nei primi anni '60 del 1900, mentre parallelamente si cominciò ad affrontare le tecniche di apprendimento delle macchine con approcci non più simbolici, quindi basati su logiche booleane, ma probabilistici.

Negli stessi anni prese piede anche un metodo più sperimentale, fissando dei problemi di *benchmark* condivisi con la creazione di *dataset* comuni per testare le soluzioni⁴. Nel 1988 fu pubblicato il volume di Judea Pearl con cui vennero introdotte nuove metodologie per utilizzare il ragionamento probabilistico nella teoria delle decisioni dell'intelligenza artificiale, con lo sviluppo delle prime reti bayesiane. A ciò si aggiunsero i contributi che mettevano in connessione l'apprendimento per rinforzo con la teoria dei processi decisioni di Markov, che vennero presto applicati alla robotica ed al controllo dei processi.

Dal punto di vista teorico, quindi, si potrebbe sostenere che il quadro per la costruzione di sistemi di intelligenza artificiale era abbastanza delineato già dalla fine degli anni '80 del novecento; la vera spinta alla ricerca applicata venne però dal diffondersi del *world wide web* e dalla sempre maggior disponibilità di dati ed informazioni di vario genere (testi, audio, immagini, video) con l'emergere della necessità di individuare nuove soluzioni algoritmiche per risolvere i problemi derivanti dall'enorme mole di dati da esaminare - come, ad esempio, la necessità di trovare algoritmi

⁴ Sono di questo periodo la creazione del repository di UC Irvine per l'apprendimento automatico, LibriSpeech per il riconoscimento vocale, il MNIST per i test sulla scrittura manuale, ImageNet e COCO per il riconoscimento di immagini, SQUAD per il linguaggio naturale.

efficienti di disambiguazione - e l'opportunità, dall'altra parte, di poter utilizzare tale numerosità di dati proprio per migliorare le prestazioni dei sistemi attraverso i meccanismi di apprendimento già teorizzati negli anni precedenti.

Negli anni '90 del Novecento vennero quindi presentate le prime reti neurali convoluzionali⁵, ossia la possibilità di realizzare l'apprendimento automatico utilizzando molteplici livelli di elementi computazionali semplici e regolabili, il c.d. *deep learning*.

Il vero successo di tale approccio, però, si è rivelato solamente dopo quasi 20 anni, quando metodi di *deep learning*, che richiedono risorse *hardware* più potenti e grandi quantità di dati, hanno portato a prestazioni parificabili a quelle umane nel campo del riconoscimento vocale e nel riconoscimento visivo.

In tale contesto è stato rilevato⁶ che un ruolo preponderante nella ricerca e nella proposizione e sviluppo di sistemi di intelligenza artificiale lo ha ricoperto Google, unendo e divulgando le evoluzioni compiute in questo settore anche tramite eventi e notizie che sono balzati alle cronache dei giornali⁷.

D'altra parte, anche tali successi non riuscivano ancora a convincere del tutto i critici, che sottolineavano la limitatezza dell'ambito di applicazione dei sistemi di intelligenza artificiale essendo ancora in grado di fornire risultati efficienti solo per compiti ben definiti e specifici. Il definitivo superamento di tali critiche si deve ai ricercatori di Google, che nel 2017 pubblicarono un articolo scientifico dal titolo "*Attention is all you need*"⁸ con cui fu introdotto il meccanismo dei c.d. *transformer*, basato, semplificando i concetti, sull'idea di far analizzare dal sistema di intelligenza artificiale, nell'ambito del riconoscimento del linguaggio naturale, non le singole parole nella successione in cui vengono formulate, ma tutto il contesto di significato tramite l'esame dell'intera frase.

L'effetto di tale approccio innovativo è quello di aver "*dato il via a un'era completamente nuova: l'ascesa dell'AI generativa. Oggi il trasformatore è alla base della maggior parte delle applicazioni all'avanguardia dell'IA in fase di sviluppo. Non solo è incorporato in Google Search e in Google Translate, per i quali è stato originariamente inventato, ma alimenta anche tutti i modelli linguistici di grandi dimensioni, compresi quelli dietro*

⁵ Y. LeCun, Y. Bengio, *Convolutional networks for images, speech, and time series*, in *The handbook of brain theory and neural networks*, 1995.

⁶ S. Da Empoli, *L'economia di ChatGPT*, Milano, 2023, pagg. 7 ss.

⁷ Così già nel 2010 Google aveva annunciato che i propri prototipi di macchine a guida autonoma erano stati in grado di percorrere 350 miglia, e poi nel 2016 il sistema AlphaGo, sviluppato dall'azienda DeepMind precedentemente acquistata da Google, riuscì a battere il campione coreano di Go replicando il successo di alcuni anni prima di Watson, sistema di intelligenza artificiale sviluppato da IBM, contro il campione di scacchi Kasparov.

Nel maggio 2018, nel corso della I/O Conference di Google, l'amministratore della società Sundar Pichai presentò Google Duplex, annunciando che l'intelligenza artificiale avrebbe avuto nel futuro un ruolo determinante «quanto l'elettricità». Il sistema emulava un assistente vocale che interagiva con un essere umano, fissando un appuntamento per una prestazione in un salone di bellezza. La presentazione, oltre a suscitare stupore ed ammirazione, sollevò i primi problemi etici in considerazione del fatto che nel dialogo l'assistente vocale utilizzava degli intercalari tipicamente umani, inducendo il proprio interlocutore a ritenere che la conversazione fosse svolta da un essere umano e non da una macchina.

⁸ A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A.N. Gomez, L. Kaiser, I. Polosukhin, *Attention is all you need*, 2017, disponibile all'indirizzo <https://arxiv.org/abs/1706.03762>.

a ChatGPT di OpenAI e Bard di Google. Supporta il completamento automatico sulle nostre tastiere mobili e il riconoscimento vocale tramite altoparlanti intelligenti. Funziona inoltre anche in aree non linguistiche, generando immagini, codice informatico e perfino la struttura di centinaia di milioni di proteine”⁹, trattandosi di un metodo generale idoneo a raccogliere non solo le interazioni tra le parti di una frase, ma anche delle note di una canzone o dei pixel di un’immagine, insomma qualsiasi dato che possa essere ridotto ad una sequenza di bit, pensato quindi per poter assolvere qualsiasi compito.

I risultati di tale nuovo approccio sono stati visibili agli occhi del pubblico dal mese di dicembre 2022 fino ai giorni nostri, in particolare da quando OpenAI, l’azienda statunitense che ha sviluppato uno dei Large Language Model più evoluti del settore (denominato GPT, ossia *Generative Pre-trained Transformer*), lo ha reso disponibile sia per creare applicazioni tramite interfacce API (*Application Programming Interface*) sia direttamente tramite la messa a disposizione del proprio *chatbot* denominato **ChatGPT**.

A tale iniziativa si sono susseguiti, quasi con cadenza settimanale, annunci relativi a nuovi modelli di intelligenza artificiale sempre basati su tecnologia *transformer* rilasciati sul mercato sia con licenze open-source sia con licenze commerciali (LLama di Facebook, Mistral dell’omonima azienda francese, Bard e poi Gemini di Google, Falcon rilasciato dal governo degli Emirati Arabi, Claude di Anthropic, per citare i più conosciuti) con l’effetto di far sempre più emergere, tra i governi e le istituzioni di vario livello, spesso colti di sorpresa da una così rapida evoluzione, la necessità di introdurre una regolamentazione dei sistemi di intelligenza artificiale con approcci ed interessi diversi che si riflettono nelle scelte di politica legislativa ad oggi compiute.

2. ORIGINI DELL’INTELLIGENZA ARTIFICIALE APPLICATA AL DIRITTO

Nel corso degli anni ‘60 e ‘70 del 1900 le nuove possibilità introdotte dei “sistemi esperti” fecero avvicinare al mondo ancora embrionale dell’intelligenza artificiale alcuni giuristi, che, partendo da un approccio di natura filosofica, applicarono poi i principi dei “sistemi esperti” alla ricerca giuridica, facendo così nascere di fatto la categoria del diritto nota come **informatica giuridica**.

Studiosi quali Vittorio Frosini, Ettore Giannantonio, Renato Borruso, si impegnarono¹⁰ per coniugare i principi dell’intelligenza artificiale con le ricerche evolute basate sulle banche dati giuridiche¹¹.

Grazie al lavoro di questi veri e propri pionieri del diritto dell’informatica (o, meglio dell’informatica giuridica come venne chiamata all’epoca) si riuscì a creare uno straordinario esperimento di proto-intelligenza artificiale in uno dei settori più tradizionali e tradizionalisti del mondo giuridico; la Corte Suprema di Cassazione.

⁹ S. Da Empoli, *op. cit.*, pagg. 17 ss.

¹⁰ Sulla storia del C.E.D. si veda R. Borruso, *Computer e diritto*, Milano, 1988, tomo II, pagg. 175 ss.

¹¹ A. Viola, *Diritto e intelligenza artificiale nel pensiero di Vittorio Frosini*, *Informatica e diritto*, XLII Annata, Vol. XXV, 2016, n. 1, pagg. 215-227.

Fortemente voluto da un gruppo di intraprendenti magistrati (tra cui lo stesso Renato Borruso, Alessandro Falcone, Vittorio Novelli e Ugo Berni Canani) tra gli anni '60 e '70, il Centro prese ad organizzare, in modo automatizzato (con il sistema dell'*information retrieval*), le massime della Corte di Cassazione e i documenti giuridici in generale dando vita al sistema *Italgire find*¹².

In particolare, i creatori della banca dati della Cassazione denominata "Italgire" hanno, per primi nel mondo, sperimentato con uno speciale dizionario della lingua italiana nel 1969 chiamato **Thesaurus**, concepito espressamente in funzione del computer e come parte integrante di esso, allo scopo di consentire automaticamente sia la lemmizzazione delle parole (cioè la possibilità di risalire dalle parole declinate o coniugate rinvenute nei testi ai lemmi indicati per la ricerca degli utenti), sia il riconoscimento delle parole sinonime e (più o meno) specifiche.

L'uso del Thesaurus costituirebbe, quindi, il primo serio passo di "intelligenza artificiale" realizzata col computer in ambito non numerico¹³.

Furono questi gli anni in cui i sistemi esperti nel campo del diritto presero l'avvio.

Tra gli studiosi italiani che colsero questa novità vi sono senz'altro G. Sartor e G. Taddei Elmi¹⁴.

Sartor definì l'intelligenza artificiale come una "*scienza intesa a sviluppare modelli computazionali del comportamento intelligente, e quindi a far sì che gli elaboratori possano eseguire compiti che richiederebbero intelligenza da parte dell'uomo*"¹⁵.

3. INTELLIGENZA ARTIFICIALE: TENTATIVI DI DEFINIZIONE DEL FENOMENO

Qualsiasi legislatore che intenda porre una disciplina positiva di un fatto o di un fenomeno che si presenta nella realtà deve necessariamente e preliminarmente individuare il perimetro della regolamentazione, definendo quale sia l'oggetto della stessa così da porre un quadro certo tra ciò che rientra nel perimetro delle norme e ciò che invece è escluso dalle stesse ed eventualmente disciplinato altrove.

Le tecnologie alla base dei sistemi di intelligenza artificiale e, probabilmente, la novità del fenomeno rendono però già difficoltosa tale ricostruzione "pre-giuridica" e ciò emerge chiaramente dalle tante e in parte diverse definizioni che vengono riportate nelle proposte regolamentari avanzate da più parti.

Il sintagma "intelligenza artificiale", infatti, coniato nel 1955 dal professore di

¹² G. Oberto, *Il c.e.d. della Suprema Corte di Cassazione*; http://www.distretto.torino.giustizia.it/documentazione/D_1949.pdf.

¹³ R. Borruso, *Computer e diritto*, Milano, 1988, tomo II, pagg. 199 ss.

¹⁴ G. Taddei Elmi, *I diritti dell'intelligenza artificiale tra soggettività e valore: fantadiritto o jus condendum*, in *Il meritevole di tutela. Studi per una ricerca coordinata* da L. Lombardi Vallauri, Milano, 1990, pag. 685-711; per una *overview* delle problematiche giuridiche del periodo oltreoceano *Artificial Intelligence and Law: Stepping Stones to a Model of Legal Reasoning*, Edwina L. Rissland *The Yale Law Journal*, vol. 99, No. 8 (Jun., 1990), pagg. 1957-1981.

¹⁵ Giovanni Sartor, *Intelligenza artificiale e diritto: un'introduzione*, Milano, 1996, pag. 6.

Stanford John McCarthy¹⁶ in occasione della preparazione dell'incontro nel Dartmouth College dell'estate del 1956, comprende il termine "intelligenza" che già di per sé solleva questioni interpretative e dibattiti circa la reale natura della stessa.

Ai fini del presente testo, però, è necessario delimitare il campo di indagine, epurando dallo stesso tutti quei tentativi definitivi che sono stati prospettati in settori diversi da quello strettamente giuridico e legislativo, concentrando l'analisi sulle differenze e analogie che si ritrovano in atti, provvedimenti e proposte emanate fino ad oggi dagli Stati e dalle organizzazioni internazionali.

Uno dei primi interventi in tal senso è stato quello della Commissione Elettrotecnica Internazionale che opera in seno all'*International Organization for Standardization* (ISO), con l'inserimento nello *standard* ISO/IEC 2382: 2015 (en) *Information technology: Vocabulary* della definizione dell'intelligenza artificiale come "Un campo interdisciplinare, solitamente considerato una branca dell'informatica, che si occupa di modelli e sistemi per lo svolgimento di funzioni generalmente associate all'intelligenza umana, come il ragionamento e apprendimento"¹⁷.

La definizione sopra riportata è stata poi migliorata, tramite la sua suddivisione, nel più recente *standard* ISO/IEC 22989: 2022 (en) denominato *Information technology - Artificial intelligence - Artificial intelligence concepts and terminology* che al punto 3.1.3 definisce il termine "Artificial Intelligence" come una disciplina volta a "la ricerca e lo sviluppo di meccanismi ed applicazioni di AI Systems" chiarendo al punto 3.1.4 che un *AI System* deve ritenersi un "sistema ingegnerizzato che genera output come contenuti, previsioni, raccomandazioni o decisioni per un dato insieme di obiettivi definiti dall'uomo"¹⁸.

Nel 2018 il Dipartimento della difesa degli Stati Uniti pubblicava un documento intitolato *Summary of the 2018 Department of Defense AI Strategy: Harnessing AI to Advance Our Security and Prosperity*¹⁹ in cui l'intelligenza artificiale viene definita "La capacità delle macchine di eseguire compiti che normalmente richiedono l'intelligenza umana - ad esempio, riconoscere schemi, imparare dall'esperienza, trarre conclusioni, fare previsioni o agire - sia in forma digitale che come software intelligente alla base di sistemi fisici autonomi."²⁰.

Sempre nello stesso anno l'Autorità per la protezione dei dati personali norvegese pubblicava un *report*²¹ sui rapporti tra intelligenza artificiale e normativa in materia di protezione dei dati personali, in cui veniva introdotto il concetto di sistemi

¹⁶ Il Prof. McCarthy utilizzava il termine intelligenza artificiale per indicare la scienza e l'ingegneria di realizzare macchine intelligenti.

¹⁷ Traduzione dell'autore. Nel testo originale «*An interdisciplinary field, usually regarded as a branch of computer science, dealing with models and systems for the performance of functions generally associated with human intelligence, such as reasoning and learning.*».

¹⁸ Traduzione dell'autore. Nel testo originale «*engineered system that generates outputs such as content, forecast, recommendations or decisions for a given set of human-defined objectives.*».

¹⁹ Il documento è consultabile a questo link <https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF>

²⁰ Traduzione dell'autore. Nel testo originale «*The ability of machines to perform tasks that normally require human intelligence — for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action - whether digitally or as the smart software behind autonomous physical systems.*».

²¹ Consultabile su <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>.

informatici in grado di imparare dalle proprie esperienze e di risolvere problemi complessi in situazioni diverse, per sottolineare come molto spesso tali sistemi siano alimentati da dati personali, che consentono loro di imparare e diventare intelligenti.

Un'ulteriore tentativo di inquadramento del fenomeno veniva fornita nel 2018 dal governo federale tedesco, il quale nella propria *National AI Strategy*²² aggiungeva un ulteriore elemento rispetto alle definizioni fino ad allora coniate: è introdotta la **distinzione tra intelligenza artificiale “forte” e “debole”**, secondo la quale la prima ha capacità intellettuali pari a quella degli esseri umani, se non addirittura superiori, mentre i sistemi di intelligenza artificiale debole si concentrano sulla soluzione di problemi specifici utilizzando metodi matematici e informatici, essendo in grado di auto-ottimizzarsi. A tal fine, gli aspetti dell'intelligenza umana risulterebbero mappati e descritti formalmente e i sistemi sono progettati per simulare e supportare il pensiero umano.

Mentre in quel periodo anche altre istituzioni pubblicavano studi e rapporti sull'utilizzo dell'intelligenza artificiale²³, un tassello importante per una definizione comune di tali sistemi veniva posto nel novembre 2019 dall'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) con la pubblicazione del paper dal titolo “*Scoping the OECD AI Principles*” in cui, dopo aver introdotto una descrizione di un sistema di intelligenza artificiale²⁴, viene proposta la seguente definizione “*Un sistema di intelligenza artificiale è un sistema basato su una macchina che è in grado di influenzare l'ambiente facendo raccomandazioni, previsioni o decisioni per un determinato insieme di obiettivi. Lo fa utilizzando input/dati di macchina e/o umani per: i) percepire ambienti reali e/o virtuali; ii) astrarre tali percezioni in modelli manualmente o automaticamente; e iii) utilizzare le interpretazioni dei modelli per formulare opzioni per i risultati.*”²⁵.

Ad onor del vero tale pubblicazione era stata preceduta da una serie di documenti dell'8 aprile 2019 realizzati dal Gruppo di Alti Esperti sull'Intelligenza Artificiale nominato dalla Commissione Europea in seguito alla Raccomandazione n. 2018/C 252/25 del 16 febbraio 2017 denominata *Civil Rules in Robotics* del Parlamento Europeo, in cui, pur non individuando una specifica definizione dei sistemi di intelligenza artificiale, i parlamentari europei sollecitavano la Commissione ad avviare degli studi e delle azioni al fine di proporre una regolamentazione del fenomeno nell'Unione Europea, anche in considerazione delle divergenze tra i vari ordinamenti degli Stati membri e dei rischi, sotto il profilo civilistico, che l'introduzione

²² Consultabile al link https://www.ki-strategie-deutschland.de/home.html?file=files/downloads/Nationale_KI-Strategie_engl.pdf.

²³ Vd. il rapporto “*European Ethical Charter on the use of Artificial Intelligence in Judicial Systems and their Environment*” pubblicato dalla Commissione europea per l'efficienza della giustizia del Consiglio di Europa del 3-4 dicembre 2018, consultabile al link <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>.

²⁴ Ripresa da S. Russell, P. Novig, *Intelligenza artificiale. Un approccio moderno*, cit.

²⁵ Traduzione dell'autore. Nel testo originale “*An AI system is a machine-based system that is capable of influencing the Environment by making recommendations, predictions or decisions for a given set of Objectives. It does so by utilising machine and/or human-based inputs/data to: i) perceive real and/or virtual environments; ii) abstract such perceptions into models manually or automatically; and iii) use Model Interpretations to formulate options for outcomes.*».

e l'utilizzo diffuso di tali sistemi avrebbero potuto porre.

Il Gruppo di Alti Esperti nel produrre i documenti richiesti dalla Commissione²⁶ pubblicava un *report* preliminare denominato *A definition of AI: main capabilities and scientific disciplines*²⁷, allo scopo di fornire la definizione di intelligenza artificiale che sarebbe stata poi referenziata negli ulteriori atti²⁸. In tale *report* viene proposta una definizione assai ampia con il tentativo di ricomprendere tutti gli aspetti del fenomeno, e che vede rientrare nella stessa tutti i “*Sistemi software (ed eventualmente anche hardware) progettati dall'uomo che, dato un obiettivo complesso, agiscono nella dimensione fisica o digitale percependo l'ambiente circostante attraverso l'acquisizione di dati, interpretando i dati strutturati o non strutturati raccolti, ragionando sulla conoscenza o elaborando le informazioni derivate da questi dati e decidendo le azioni migliori da intraprendere per raggiungere l'obiettivo prefissato. I sistemi di IA possono utilizzare regole simboliche o apprendere un modello matematico, e possono anche adattare il loro comportamento analizzando come l'ambiente è influenzato dalle loro azioni precedenti.*

*In quanto disciplina scientifica, l'IA comprende diversi approcci e tecniche, come l'apprendimento automatico (di cui l'apprendimento profondo e l'apprendimento per rinforzo sono esempi specifici), il ragionamento automatico (che include la pianificazione, programmazione, rappresentazione della conoscenza e ragionamento, ricerca e ottimizzazione), e la robotica (che comprende il controllo, la percezione, i sensori e gli attuatori, nonché l'integrazione di tutte le altre tecniche nei sistemi cyber-fisici).”*²⁹.

In seguito a tali primi tentativi di fornire una definizione quanto più esaustiva dell'intelligenza artificiale di per sé e dei sistemi basati su tale tecnologia all'interno di documenti e *report* strategici o di indirizzo, vari Paesi nel mondo hanno avviato delle procedure volte a promulgare atti aventi forza di legge, introducendo definizioni a volte non coincidenti o parziali su tale fenomeno.

Così il 20 maggio 2020 il Senato e la Camera degli Stati Uniti d'America pro-

²⁶ In particolare, le *Linee Guida etiche per una intelligenza artificiale affidabile*, le *Raccomandazioni sulle politiche ed investimenti per una AI affidabile*, la c.d. ALTAI ossia *Assessment List for Trustworthy AI* e le *Considerazioni settoriali sulle raccomandazioni politiche e di investimento*.

²⁷ Disponibile al link <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>.

²⁸ Tale definizione è stata poi ripresa anche dall'Agenzia Europea per i diritti fondamentali nella pubblicazione *Getting the future right. Artificial Intelligence and Fundamental Rights* del 2020 in cui venivano esaminate le sfide ed i rischi per i diritti fondamentali posti da tale nuova tecnologia. Il testo del documento è disponibile al link https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-artificial-intelligence_en.pdf.

²⁹ Traduzione dell'autore. Nel testo originale «*Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.*

As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)», vd. High-level Expert Group on Artificial Intelligence, *A definition of AI: main capabilities and scientific disciplines*, 2019, pag. 6.

ponevano una norma volta a comprendere l'evoluzione dei sistemi di intelligenza artificiale per massimizzarne i benefici verso la società e promuovere un clima di investimenti e innovazione al fine di assicurare la competitività della nazione³⁰.

La definizione contenuta in tale provvedimento, che non è mai assunto allo stato di legge federale, è abbastanza ampia e recita:

“a. Tutti i sistemi artificiali che eseguono compiti in circostanze variabili e imprevedibili, senza una significativa supervisione umana, o che possono imparare dall'esperienza e migliorare le proprie prestazioni. Tali sistemi possono essere sviluppati in software per computer, hardware fisico o altri contesti non ancora contemplati. Possono risolvere compiti che richiedono percezione, cognizione, pianificazione, apprendimento, comunicazione o azione fisica simili a quelli umani. In generale, quanto più il sistema è simile all'uomo nel contesto dei suoi compiti, tanto più si può dire che utilizza l'intelligenza artificiale.

b. Sistemi che pensano come gli esseri umani, come le architetture cognitive e le reti neurali.

c. Sistemi che agiscono come gli esseri umani, come i sistemi in grado di superare il test di Turing o altri test comparabili attraverso l'elaborazione del linguaggio naturale, la rappresentazione della conoscenza, il ragionamento automatico e l'apprendimento.

d. Un insieme di tecniche, compreso l'apprendimento automatico, che cercano di approssimare un compito cognitivo.

e. Sistemi che agiscono razionalmente, come agenti software intelligenti e robot che raggiungono gli obiettivi attraverso la percezione, la pianificazione, il ragionamento e l'apprendimento, la comunicazione, il processo decisionale e l'azione.”³¹.

La norma, inoltre, distingueva, come la strategia nazionale tedesca, tra “intelli-

³⁰ Si tratta della proposta di legge S.3771 denominata *Fundamentally Understanding the Usability and Realistic Evolution of Artificial Intelligence Act of 2020* consultabile all'indirizzo internet <https://www.congress.gov/bills/116th-congress/senate-bill/3771/text>.

Nel 2019 il Presidente degli Stati Uniti aveva emanato uno specifico provvedimento, Executive Order 13859 of February 11, 2019, dal titolo *Maintaining American Leadership in Artificial Intelligence* con cui venivano individuate una serie di azioni per aumentare le capacità produttive e conoscitive degli Stati Uniti in tale settore, attraverso investimenti economici, piani di azione rivolti alla formazione ed attrazione di talenti, aumento della *cybersecurity* dei sistemi, senza però fornire una definizione specifica di intelligenza artificiale.

A tale provvedimento seguiva un ulteriore Executive Order n. 13960 del 3 dicembre 2020 dal titolo *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government* volto ad incentivare l'uso affidabile dei sistemi di intelligenza artificiale da parte delle istituzioni, al cui interno, però, non è stata inserita alcuna definizione relativamente alla tecnologia. Interessante notare, invece, l'utilizzo dell'aggettivo “*Trustworthy*” che riprende il termine contenuto nei documenti prodotti dal Gruppo di Alti Esperti nominato dalla Commissione Europea.

³¹ Traduzione dell'autore. Nel testo originale «*a. Any artificial systems that perform tasks under varying and unpredictable circumstances, without significant human oversight, or that can learn from their experience and improve their performance. Such systems may be developed in computer software, physical hardware, or other contexts not yet contemplated. They may solve tasks requiring human-like perception, cognition, planning, learning,*

genza artificiale generale” intesa come un sistema di intelligenza artificiale futuro e immaginario che mostra un comportamento apparentemente intelligente almeno pari a quello di una persona in tutta la gamma di comportamenti cognitivi, emotivi e sociali, e “intelligenza artificiale ristretta” quale un’intelligenza artificiale rivolta ad aree applicative specifiche, come la riproduzione di giochi strategici, la traduzione linguistica, i veicoli a guida autonoma e il riconoscimento facciale o di altre immagini.

Nello stesso anno, sempre negli USA, veniva approvato il *National Artificial Intelligence Initiative Act of 2020* riferito come 15 U.S.C. 9401 il cui paragrafo 3 contiene la definizione oramai ufficiale dell’ordinamento statunitense sull’intelligenza artificiale, per cui “*Con il termine “intelligenza artificiale” si intende un sistema basato su una macchina in grado, per un determinato insieme di obiettivi definiti dall’uomo, di fare previsioni, raccomandazioni o decisioni che influenzano ambienti reali o virtuali. I sistemi di intelligenza artificiale utilizzano input basati sulla macchina e sull’uomo per:*

- (A) *percepire ambienti reali e virtuali;*
- (B) *astrarre tali percezioni in modelli attraverso l’analisi in modo automatizzato; e*
- (C) *utilizzare l’inferenza del modello per formulare opzioni di informazione o di azione.”*³².

Nel 2021 il Regno Unito ha approvato il *National Security and Investment Act* inserendo all’Allegato 3 una definizione di intelligenza artificiale - quasi analoga a quella appena sopra riportata presente nella normativa USA - allo scopo di includere in tale regolamentazione le acquisizioni effettuate da società estere di imprese britanniche che operano in tale settore, al fine di valutarne l’impatto sull’economia ed eventualmente esercitare i poteri di veto governativi³³. La definizione è più stringata di quelle sopra esaminate, e considera intelligenza artificiale “*la tecnologia che consente la programmazione o l’addestramento di un dispositivo o di un software per:*

- i) *percepire ambienti attraverso l’uso di dati,*
- ii) *interpretare i dati utilizzando un’elaborazione automatica progettata per approssimare le capacità cognitive; e*

communication, or physical action. In general, the more human-like the system within the context of its tasks, the more it can be said to use artificial intelligence.

b. Systems that think like humans, such as cognitive architectures and neural networks.

c. Systems that act like humans, such as systems that can pass the Turing test or other comparable test via natural language processing, knowledge representation, automated reasoning, and learning.

d. A set of techniques, including machine learning, that seek to approximate some cognitive task.

e. Systems that act rationally, such as intelligent software agents and embodied robots that achieve goals via perception, planning, reasoning, learning, communicating, decision-making, and acting.».

³² Traduzione dell’autore. Nel testo originale “*The term “artificial intelligence” means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to*

(A) perceive real and virtual environments;

(B) abstract such perceptions into models through analysis in an automated manner; and

(C) use model inference to formulate options for information or action.». Il testo del provvedimento legislativo è consultabile al link <https://www.congress.gov/bill/116th-congress/house-bill/6216/text>.

³³ Il testo della norma è segnatamente dell’Allegato 3 è consultabile al link <https://www.legislation.gov.uk/uksi/2021/1264/schedule/3>.

iii) *formulare raccomandazioni, previsioni o decisioni, al fine di raggiungere un obiettivo specifico;*³⁴.

Il 2021 è anche l'anno in cui la Commissione Europea presenta la *“Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce norme armonizzate sull'intelligenza artificiale (Atto sull'intelligenza artificiale) e che modifica alcuni atti legislativi dell'Unione”*.

Nel mese di aprile 2024, dopo le modifiche introdotte dal Parlamento europeo nel 2023, è stato pubblicato il Regolamento UE n. 2024/1689, che definisce all'art. 3, par. 1, n. 1, un sistema di IA come *“ un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali.”*.

Nell'ambito dei sistemi di intelligenza artificiale così definiti il testo individua la sottocategoria dei sistemi di intelligenza artificiale per finalità generali (*general purpose AI system, o GenAI*) ossia quei sistemi basati su un modello di intelligenza artificiale per scopi generali (*general purpose AI Model*)³⁵, che hanno la capacità di servire una varietà di scopi sia per l'uso diretto sia per l'integrazione in altri sistemi di IA.

La varietà delle definizioni sopra riportate rispecchia la difficoltà terminologica di includere, in una singola nozione, un insieme di tecnologie o approcci metodologici - anche tra loro assai diversi - che conducono al medesimo risultato di far ritenere che l'autonomia del sistema nel raggiungere determinati risultati sia il sintomo di una sorta di “intelligenza” della macchina.

Il problema dell'insufficienza del bagaglio semantico di cui siamo dotati per poter compiutamente esprimere le sfumature che possono connotare l'intelligenza umana è stato messo in risalto³⁶ per sottolineare come Alan Turing, con il noto test, cercò di superare tale insufficienza proponendo una metodologia incentrata sui risultati che i sistemi dell'intelligenza artificiale possono produrre³⁷.

³⁴ Traduzione dell'autore. Nel testo originale *«artificial intelligence» means technology enabling the programming or training of a device or software to:*

(i) perceive environments through the use of data;

(ii) interpret data using automated processing designed to approximate cognitive abilities; and

(iii) make recommendations, predictions or decisions;

with a view to achieving a specific objective;».

³⁵ La definizione di «modello di IA per scopi generali» è relativa a un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato da una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato (art. 2, par. 1, n. 63).

³⁶ G. D'Acquisto, *Intelligenza Artificiale*, Milano, 2021, pagg. 2 ss.

³⁷ G. D'Acquisto così sintetizza la metodologia di Turing: *«La sua idea è di abbandonare l'ambiguità del linguaggio e di concentrarci unicamente sui risultati che una macchina può produrre. Per farlo, egli assume l'esistenza di una macchina ipotetica (una macchina che in quel momento neppure esisteva che faccia “qualcosa” per rispondere a delle domande che le sono sottoposte, in modo che l'osservatore umano che le formula possa interpretare le risposte ottenute, giuste o sbagliate che siano, come il frutto di un pensiero. Una specie di imbroglio, ma che fa rientrare la questione nell'alveo tradizionale del metodo scientifico. Se quell'imbroglio funziona, e l'osservatore umano*

Estratto

Estratto da un prodotto in vendita su **ShopWKI**, il negozio online di Wolters Kluwer Italia

Vai alla scheda →

Wolters Kluwer opera nel mercato dell'editoria professionale, del software, della formazione e dei servizi con i marchi: IPSOA, CEDAM, Altalex, UTET Giuridica, il fisco.



Wolters Kluwer