

Cyber | Security | Defence spazia tra le tecnologie e i contesti coinvolti nel complesso mondo della sicurezza informatica, più comunemente la cyber-security, analizzandone in maniera trasversale i diversi ambiti di applicazione, interazione e sviluppo, e trattando tutti gli elementi correlati: tecnici, tecnologici, organizzativi, economici, politici, giuridici, sociali e umani.

I testi proposti hanno sia un taglio didattico e tecnico-pratico che saggistico e divulgativo, e sono destinati a molteplici interlocutori: istituti e università, enti e aziende di settore, appassionati e cultori della materia | #_7

MASSIMO MONTANILE

Dall'algoritmo al silicio

Comprendere l'intelligenza artificiale

prefazione di Nicola Bernardi

postfazione di Roberto Randazzo

con una nota di Claudio Santo Malavenda e di Francesco Montanile

UNIVERSITÀ

*A Flavia, Daniele, Francesco e a Lucrezia,
che siete la mia direzione, la mia misura, il mio passo.
Che possiate sempre scegliere, non subire.
E costruire il vostro futuro con cuore,
intelligenza e meraviglia.
«Faber est suae quisque fortunae» (Sallustio).*

We can only see a short distance ahead, but we can see plenty there that needs to be done.¹

A.M. Turing

1. «Possiamo vedere solo poco davanti a noi, ma possiamo vedere tante cose che bisogna fare». A.M. Turing, *Computing Machinery and Intelligence in Mind*, New Series, vol. 59, n. 236. (October 1950), pp. 433-460.

Indice

p.	15	Prefazione di Nicola Bernardi
	19	Introduzione
	23	Capitolo 1
		<i>L'architettura algoritmica</i>
	1.1.	Introduzione, 23
	1.2.	Cos'è il machine learning, 24
	1.3.	Programmazione tradizionale vs apprendimento automatico, 27
	1.4.	Componenti fondamentali, 29
	1.5.	Esempi reali di machine learning, 35
	1.6.	Tipi di apprendimento, 35
	1.7.	I modelli principali, 40
	1.8.	Algoritmi fondamentali, 44
	1.9.	Sintesi del capitolo, 50
	1.10.	Transizione al capitolo 2, 51
	53	Capitolo 2
		<i>L'architettura software</i>
	2.1.	Introduzione, 53
	2.2.	Framework di sviluppo, 53
	2.3.	Le pipeline IA: dal dato all'inferenza, 54
	2.4.	Validazione, testing e inferenza, 55
	2.5.	MLOps e gestione del ciclo di vita dei modelli, 56
	2.6.	Esempi pratici di architettura software per l'IA, 56
	2.7.	Caso d'uso metodologico, 59

- 2.8. Sintesi del capitolo, 63
- 2.9. Transizione al capitolo 3, 64
- p. 65 Capitolo 3
L'architettura di sistema
 - 3.1. Introduzione, 65
 - 3.2. Deployment cloud vs edge, 65
 - 3.3. Orchestrazione e runtime IA, 67
 - 3.4. Scalabilità, affidabilità e costi energetici, 68
 - 3.5. Caso d'uso metodologico, 69
 - 3.6. Sintesi del capitolo, 74
 - 3.7. Transizione al capitolo 4, 75
- 77 Capitolo 4
Firmware e microarchitettura
 - 4.1. Introduzione, 77
 - 4.2. Acceleratori hardware, 77
 - 4.3. Compilatori per l'inferenza, 79
 - 4.4. Ottimizzazioni per modelli embedded e real-time, 80
 - 4.5. Caso d'uso metodologico, 81
 - 4.6. Sintesi del capitolo, 85
 - 4.7. Transizione al capitolo 5, 87
- 89 Capitolo 5
L'architettura fisica
 - 5.1. Introduzione, 89
 - 5.2. Co-design hardware/software, 89
 - 5.3. Architetture neuromorfiche, 90
 - 5.4. FPGA e ASIC per l'IA, 91
 - 5.5. Sostenibilità e sovranità tecnologica, 92
 - 5.6. Caso d'uso metodologico, 96
 - 5.7. Sintesi del capitolo, 99
 - 5.8. Transizione al capitolo 6, 99

p. 101	Capitolo 6
	<i>Governance, sicurezza ed etica dell'IA</i>
	6.1. Introduzione, 101
	6.2. Governance dell'IA: principi, normative e responsabilità, 101
	6.3. Sicurezza: proteggere modelli, dati e decisioni, 102
	6.4. Etica dell'IA: una tecnologia che riflette chi la crea, 105
	6.5. Caso d'uso metodologico, 106
	6.6. Sintesi del capitolo, 109
	6.7. Transizione al capitolo conclusivo, 110
113	Conclusioni
121	Appendice
127	Bibliografia
131	Note autoriali
137	Postfazione di Roberto Randazzo
139	Gli autori

Prefazione

L'intelligenza artificiale non è più una promessa tecnologica proiettata nel futuro, ma una realtà già presente, silenziosa e pervasiva, che rivoluziona sia la vita dei singoli individui che il funzionamento delle organizzazioni pubbliche e private, attraversando i processi decisionali, incidendo sui diritti delle persone e ridefinendo il modo stesso in cui il valore viene creato, misurato e distribuito.

Considerando che l'intelligenza artificiale si “nutre” di dati, un libro che si pone l'obiettivo di farne un quadro esaustivo non può evitare di affrontare i temi della privacy e della protezione dei dati personali, altrimenti sarebbe un'opera incompiuta.

Infatti, ogni sistema di intelligenza artificiale è prima di tutto un sistema di trattamento dei dati. Informazioni raccolte, selezionate, raffinate, etichettate, combinate, riutilizzate. Dati che spesso raccontano storie di persone: comportamenti, preferenze, abitudini, fragilità. Dati che, una volta trasformati in modelli, producono inferenze, classificazioni, previsioni e decisioni che non si limitano a descrivere la realtà, ma contribuiscono a plasmarla.

È da questa consapevolezza che nasce il legame profondo, strutturale e non contingente tra intelligenza artificiale e protezione dei dati personali.

Per troppo tempo il dibattito sull'IA si è mosso su due binari paralleli: da un lato l'entusiasmo tecnologico, dall'altro la comprensibile preoccupazione di carattere giuridico. Da una parte chi “costruisce” sistemi intelligenti, dall'altra chi prova a contenerne gli effetti.

Questo libro compie un'operazione diversa e più matura: mostra che l'intelligenza artificiale non può essere governata *a valle*, ma deve essere compresa *a monte*, nei suoi strati costitutivi – dall'algoritmo all'hardware – se si vuole davvero parlare di responsabilità, trasparenza e tutela dei diritti fondamentali.

Dal punto di vista di chi si occupa di protezione dei dati, questa operazione è tutt'altro che accademica, e richiede un approccio multidisciplinare e interdisciplinare che coinvolga esperti in grado di analizzare il fenomeno dell'IA dalle varie prospettive.

Il Regolamento UE 2016/679 (GDPR) varato dal legislatore nel 2016 non è mai stato una normativa “tecnologica” in senso stretto, ma, prevedendo in modo lungimirante gli sviluppi delle nuove tecnologie già all'epoca, è stato concepito per disciplinare la gestione di banche dati automatizzate, su cui vengono adottate decisioni, che producono effetti giuridici o comunque significativamente impattanti sulle persone. L'intelligenza artificiale ha semplicemente reso esplicito ciò che era già implicito: non esiste governance dei dati senza comprensione della tecnologia che li utilizza.

L'IA introduce infatti una discontinuità rispetto al software tradizionale: non si limita a eseguire istruzioni predeterminate, ma apprende dai dati e generalizza.

Questo elemento, noto come machine learning, è ciò che rende i sistemi intelligenti straordinariamente potenti, ma anche opachi, difficili da spiegare, talvolta imprevedibili. Ed è proprio qui che le categorie classiche della protezione dei dati (liceità, minimizzazione, limitazione della finalità, esattezza, accountability) incontrano le loro sfide più complesse.

Come si valuta la qualità di un dato in un sistema che apprende? Come si garantisce la correttezza di una decisione automatizzata quando il modello evolve nel tempo? Come si rende effettivo il diritto alla spiegazione – o, più correttamente, alla comprensione – in presenza di architetture profonde e distribuite? Come si governa il rischio quando l'errore non è più un bug, ma una probabilità statistica?

Le risposte a queste domande non possono essere esclusivamente giuridiche. Richiedono una alfabetizzazione tecnica che, per gli addetti ai lavori dell'IA e della privacy, non è opzionale. Ed è qui che il valore di questo libro emerge con particolare chiarezza.

Dall'algoritmo al silicio non è un manuale per programmatori né un trattato divulgativo superficiale. È un testo che accompagna il lettore attraverso i diversi livelli dell'intelligenza artificiale, mostrando come ogni scelta – algoritmica, software, sistemistica, hardware – abbia conseguenze dirette sulla sicurezza, sull'affidabilità e sulla governabilità dei sistemi. Per chi si occupa di

data protection, questo significa acquisire gli strumenti per dialogare realmente con chi progetta e implementa l'IA, superando la sterile contrapposizione tra “tecnici” e “giuristi”.

La protezione dei dati personali, nell'era dell'intelligenza artificiale, non può ridursi a un esercizio di compliance documentale. Deve diventare parte integrante della progettazione dei sistemi, secondo una logica di data protection by design and by default che oggi si intreccia inevitabilmente con la AI governance.

Il GDPR, l'AI Act, il Data Governance Act e il Data Act non sono compartimenti stagni, ma tasselli di un unico disegno europeo: costruire un ecosistema digitale in cui l'innovazione non sia ottenuta al prezzo dei diritti fondamentali.

In questo senso, comprendere l'intelligenza artificiale non è solo una competenza tecnica, ma una responsabilità professionale, sia per chi lavora nelle aziende, nelle pubbliche amministrazioni, nella consulenza, nella sicurezza informatica, nella protezione dei dati, sia per chi è chiamato a valutare rischi, redigere valutazioni d'impatto, definire policy, progettare processi, assumere decisioni che avranno effetti concreti sulla vita delle persone.

Questo libro offre una preziosa chiave di lettura: mostra che l'IA non è una “scatola nera” inevitabile e misteriosa, ma un sistema costruito da esseri umani, con scelte precise, compromessi, limiti e possibilità di controllo. E ci ricorda che ogni sistema intelligente riflette, nel bene e nel male, la cultura di chi lo progetta e di chi lo governa.

Per queste ragioni il libro non si rivolge solo a chi vuole imparare *come funziona* l'intelligenza artificiale, ma anche a chi avvisa l'importanza e sente l'urgenza di capire *come governarla*. È un invito a superare l'approccio passivo all'innovazione e a riappropriarsi di una visione critica, consapevole e responsabile della tecnologia.

In un'epoca in cui l'intelligenza artificiale rischia di diventare una delega cieca, decisionale, organizzativa, persino morale, la conoscenza resta l'unico vero strumento di libertà per gli individui, e di competitività per i professionisti.

E, per chi si occupa di protezione dei dati, resta anche il presupposto imprescindibile per tutelare efficacemente la dignità, l'autonomia e i diritti delle persone nell'ecosistema della nuova civiltà digitale.

Nicola Bernardi
presidente di Federprivacy

Introduzione

Negli ultimi anni l'intelligenza artificiale è entrata nelle nostre vite in modo silenzioso ma pervasivo. La utilizziamo ogni giorno, spesso senza accorgercene: quando chiediamo a un assistente vocale di ricordarci un impegno, quando guardiamo un film suggerito da una piattaforma, quando scriviamo un messaggio e il telefono completa le nostre frasi. È un cambiamento che si muove veloce, troppo veloce, e che in Italia rischiamo di subirlo passivamente, come fossimo semplici consumatori di strumenti sviluppati altrove.

Questo libro nasce dal desiderio di contribuire a un cambio di paradigma: dall'uso inconsapevole dell'AI alla sua comprensione profonda, affinché studenti, professionisti e appassionati possano diventare non soltanto utilizzatori, ma creatori di intelligenza artificiale.

La mia storia personale si intreccia con questa sfida. Quando, alla fine degli anni '70, iniziai a frequentare l'Università di Salerno, il corso di laurea in scienze dell'informazione era una fucina di idee e di pionieri. Dal 1979 al 1983 ebbi il privilegio di studiare i primi mattoncini di quella che allora era chiamata "intelligenza artificiale", in anni in cui i computer occupavano interi locali e il futuro digitale era ancora un territorio da esplorare. Mi laureai a soli ventidue anni, *magna cum laude*, con una tesi di ricerca sugli Algoritmi di approssimazione per problemi NP-Completi: un lavoro che mi permise di intravedere, con entusiasmo e stupore, le potenzialità immense degli algoritmi applicati a problemi reali.

Quel seme ha guidato tutta la mia vita professionale. Ho avuto la fortuna di lavorare in realtà di eccellenza come Olivetti, Telecom Italia ed Elettronica Group, vivendo dall'interno le trasformazioni che hanno segnato la storia industriale e tecnologica del nostro Paese. Esperienze che mi hanno insegnato

quanto sia importante non limitarsi a adottare soluzioni esterne, ma sviluppare capacità progettuali autonome, creando innovazione radicata nella nostra cultura e nel nostro tessuto sociale.

Oggi, come co-direttore della collana *Cyber Security, Data Protection & Digital Innovation* di *tab* edizioni, porto avanti con convinzione questa idea: diffondere una cultura digitale che non si esaurisca nell'uso di strumenti già pronti, ma che sappia promuovere consapevolezza, responsabilità e capacità di costruzione. La collana intende valorizzare contributi che, come questo libro, aiutino a comprendere e a governare le tecnologie emergenti, coniugando rigore scientifico e impegno etico.

Il percorso che propongo in queste pagine è top-down: parte dalle architetture algoritmiche e arriva fino agli strati più profondi dell'hardware, mostrando come ogni livello – software, sistemi, firmware, architettura fisica – contribuisca a dare forma a quell'intelligenza che oggi ci affascina e ci spaventa.

Ma c'è un aspetto che non possiamo dimenticare: l'intelligenza artificiale non è solo una questione tecnica. È anche un terreno in cui si giocano valori etici e sociali: la tutela della privacy, la trasparenza delle decisioni automatizzate, l'impatto sull'occupazione, la sostenibilità energetica. Governare l'IA significa anche scegliere come vogliamo che influenzi le nostre vite e quelle delle generazioni future.

Il mio auspicio è che questo libro diventi una guida, ma anche uno stimolo: che chi lo legge non si limiti ad apprendere nozioni, ma acquisisca consapevolezza e strumenti pratici per creare. Perché l'Italia ha bisogno di tornare a essere protagonista dell'innovazione, e l'intelligenza artificiale rappresenta una delle frontiere più decisive – e più delicate – del nostro futuro.

Questo libro nasce, prima di tutto, per gli studenti del corso "Introduzione all'intelligenza artificiale e alle tecnologie informatiche". È a loro che ho pensato mentre trasformavo le slide, gli esempi e le discussioni d'aula in un testo più ampio, capace di accompagnare passo dopo passo nella comprensione dei meccanismi che governano l'IA.

A loro è dedicato l'invito a non limitarsi a osservare ciò che l'intelligenza artificiale fa, ma a interrogarsi su come lo fa, perché lo fa e quali conseguenze produce. Lo scopo non è imparare a usare qualche strumento di moda, ma capire i principi che ne stanno alla base, per poterli poi applicare, modificare e persino superare.

Il libro si rivolge anche a chi lavora o desidera lavorare nel mondo della tecnologia e della consulenza, a chi si occupa di data protection, cybersecurity, auditing o governance digitale. Professionisti che avvertono il bisogno di coniugare competenze tecniche e sensibilità etica, perché l'intelligenza artificiale non è solo un insieme di algoritmi, ma un sistema di decisioni che può influenzare la vita delle persone.

È pensato inoltre per docenti, ricercatori e formatori, che vogliono disporre di uno strumento capace di collegare la dimensione accademica con quella operativa, in linea con gli standard internazionali come la ISO/IEC 42001¹, che introduce un modello di gestione responsabile dell'intelligenza artificiale.

Infine, questo libro è rivolto a chiunque sia animato da curiosità e passione: a chi sente che l'IA non è un mistero riservato agli esperti, ma un linguaggio che tutti possiamo imparare a parlare. Perché comprendere l'intelligenza artificiale non significa solo saper programmare una macchina: significa imparare a riconoscere, nel dialogo tra l'uomo e la tecnologia, le tracce più profonde della nostra intelligenza naturale.

Desidero infine esprimere la mia gratitudine agli studenti, che con le loro domande e osservazioni hanno reso vivo e dinamico il percorso da cui questo testo è nato; agli autorevoli professionisti che mi hanno ispirato con il loro esempio e con le loro competenze; e ai colleghi e intellettuali, anche di discipline non tecniche, con cui ho avuto il privilegio di confrontarmi in questi anni.

Molti dei loro suggerimenti ho cercato di comprenderli e inglobarli, consapevole che altri – forse i più profondi – non sono riuscito a recepirli in pieno. Se il testo risulta efficace, è merito anche di questi incontri; se non lo è abbastanza, è per i limiti che restano miei e che continuerò a esplorare con la stessa curiosità con cui ho iniziato questo viaggio.

Nota dei contributori

Questo volume nasce come progetto corale, arricchito da voci e prospettive differenti.

1. UNI CEI ISO/IEC 42001:2024 – Tecnologie informatiche – Intelligenza artificiale – Sistema di gestione. Requisiti per un sistema di gestione dell'IA (versione in italiano).

A completamento del testo principale, il libro include contributi autorevoli che ampliano lo sguardo sulla complessità dell'intelligenza artificiale nel mondo contemporaneo.

- *Prefazione*: Nicola Bernardi, presidente Federprivacy;
- *Nota autoriale*: Claudio Santo Malavenda, esperto di sistemi critici, difesa, C5I e automazione avanzata;
- *Nota autoriale*: Francesco Montanile, Network and System Engineer specializzato in sicurezza delle infrastrutture digitali, sistemi di osservazione intelligenti e comunicazioni avanzate.

Il loro intervento non solo completa il senso del libro, ma ne rafforza la vocazione: offrire strumenti di comprensione e non soltanto di utilizzo, con uno sguardo critico, multidisciplinare e profondamente umano.

Capitolo 1

L'architettura algoritmica

1.1. Introduzione

Nel presente volume i termini IA e AI sono utilizzati come sinonimi. Entrambi indicano la medesima disciplina: IA, acronimo italiano di *intelligenza artificiale*, e AI, corrispondente inglese di *Artificial Intelligence*.

Tale equivalenza terminologica riflette l'uso consolidato nella letteratura scientifica e nei principali standard tecnici e normativi – in particolare ISO/IEC 22989:2022¹, che definisce terminologia e concetti fondamentali nel dominio dell'IA e adotta AI quale forma abbreviata ufficiale.

L'impiego parallelo dei due acronimi risponde dunque a una duplice esigenza: mantenere coerenza con la tradizione linguistica italiana e, allo stesso tempo, garantire pieno allineamento con lo stato dell'arte internazionale in ambito accademico, industriale e regolatorio.

L'intelligenza artificiale, nella sua forma moderna, non nasce da una singola scoperta, ma dall'incontro graduale di matematica, informatica, neuroscienze, statistica e filosofia. È un campo giovane, eppure profondamente radicato nelle domande antiche dell'umanità:

- Come apprendiamo?
- Come riconosciamo ciò che vediamo?
- Come prendiamo decisioni?

1. ISO/IEC. *Artificial Intelligence – Concepts and terminology (ISO/IEC 22989:2022)*. Geneva: International Organization for Standardization, 2022.

Per decenni l'informatica si è basata su regole rigide, istruzioni fisse, logiche deterministiche. Ma la realtà – con tutte le sue sfumature, eccezioni, ambiguità – raramente segue schemi così prevedibili. Il machine learning nasce proprio qui: nel tentativo di costruire sistemi capaci non solo di eseguire istruzioni, ma di imparare dall'esperienza.

In questo capitolo entriamo nel cuore algoritmico dell'intelligenza artificiale: il livello dove si forma ciò che le macchine chiamano “conoscenza”. Capiremo perché il machine learning rappresenta un cambio di paradigma rispetto alla programmazione tradizionale, e quali sono le componenti essenziali che permettono a un sistema di apprendere dai dati. Esploreremo i diversi tipi di apprendimento, i modelli più utilizzati oggi e gli algoritmi matematici che rendono possibile la trasformazione delle informazioni in previsioni, classificazioni, decisioni.

Questo non è solo un capitolo tecnico: è un passaggio culturale. Perché ogni algoritmo racconta un modo diverso di interpretare il mondo. E prima di costruire applicazioni, strumenti o sistemi intelligenti, è fondamentale comprendere il principio da cui tutto nasce:

Un sistema artificiale è intelligente nella misura in cui sa imparare.

1.2. Cos'è il machine learning

Quando parliamo di intelligenza artificiale, spesso immaginiamo macchine capaci di “pensare” come noi. In realtà, almeno nella maggior parte dei casi, ciò che chiamiamo IA oggi è soprattutto machine learning: un insieme di metodi e tecniche che permettono a un sistema informatico di imparare dai dati e migliorare le proprie prestazioni nel tempo, senza essere esplicitamente programmato per ogni possibile scenario.

Per comprendere cosa significhi davvero, possiamo partire dalla visione tradizionale dell'informatica: per decenni abbiamo scritto software basati su regole fisse – *if this, then that*.

L'algoritmo informatico «è fondamentalmente una sequenza di istruzioni che sono eseguite secondo il verificarsi o meno delle condizioni che vengono

generate a ogni passaggio in modo non ambiguo»². Se fosse accaduto una certa condizione, il computer avrebbe eseguito un'azione definita dal programmatore. Nulla di più, nulla di meno.

Il machine learning ribalta questa logica.

Invece di dire al computer “come” deve prendere una decisione, gli mostriamo esempi, dati, esperienze. A partire da essi, il sistema costruisce da solo – attraverso modelli matematici – una rappresentazione interna dei fenomeni, riconosce schemi ricorrenti, effettua previsioni o classificazioni.

In altre parole, il machine learning permette al computer di passare dall'essere un esecutore perfetto all'essere un osservatore, interprete e, in una certa misura, generalizzatore.

Un cambiamento culturale, prima ancora che tecnologico.

Questa transizione non è soltanto un'evoluzione tecnica: è un cambio di paradigma.

Oggi non chiediamo più alla macchina: “Esegui questa istruzione”, ma: “Osserva questi esempi, trova una struttura nascosta nei dati e applicala ai casi futuri”.

Il computer diventa così un modello statistico dinamico, capace di adattarsi ai cambiamenti del contesto – una caratteristica impossibile da ottenere nei sistemi rigidi della programmazione tradizionale.

Una definizione semplice e rigorosa

Possiamo quindi definire il machine learning³ come:

La capacità di un sistema di migliorare automaticamente la propria performance nell'eseguire un compito, grazie all'esperienza accumulata attraverso i dati.

2. P. Benanti, S. Maffettone, *Noi e la macchina. Un'etica per l'era digitale*, LUISS University Press, Roma 2024, p. 22.

3. Cfr. Enciclopedia Treccani: «Branca dell'intelligenza artificiale che si occupa dello sviluppo di algoritmi e tecniche finalizzate all'apprendimento automatico mediante la statistica computazionale e l'ottimizzazione matematica», <https://www.treccani.it/vocabolario/machine-learning>.

Postfazione

È con grande interesse e curiosità che ho letto il volume *Dall'algoritmo al silicio: comprendere l'intelligenza artificiale*, sviluppato come ultima fatica editoriale da parte del dottor Massimo Montanile che, oltre a considerarlo un mio carissimo amico, lo ritengo un professionista con una grandissima esperienza professionale in vari settori di avanguardia tecnologica in ambito nazionale e internazionale.

La domanda che mi sono posto è stata di come abbia potuto affrontare un tema così complesso, estremamente ampio e diffuso quale la struttura e l'architettura dei sistemi di intelligenza artificiale. Tutto questo può apparire come una *Mission Impossible*, cioè un compito estremamente difficile e complesso per tutte le implicazioni che l'argomento comporta.

Nell'utilizzo dei sistemi di intelligenza artificiale, attività oggi molto praticata da operatori e utenti che tuttavia non sempre approfondiscono gli elementi che utilizzano e che vengono messi a loro disposizione dai grandi leader mondiali di AI. La lettura di questo volume può essere di aiuto e approfondimento per un aumento di consapevolezza da parte degli utilizzatori degli strumenti di AI che vengono adoperati. I sistemi di AI sono molto spesso visti come una scatola nera, una cd. black box, ma dietro questi sistemi sono presenti architetture e componenti ben definiti e strutturati che vanno dall'hardware (come scrive l'autore Massimo Montanile chiamandolo silicio) alle applicazioni finali ad esempio Assistenti AI e Chat Bot (testuale o vocale). Nei vari capitoli del volume sono stati esplorati e descritti con notevole dettaglio i vari livelli dell'architettura (definiti Layers) che costituiscono il modo in cui i sistemi di intelligenza artificiale sono progettati, sviluppati, addestrati e distribuiti a grandi livelli. Tra questi cito i livelli principali descritti nel volume:

- livello fisico (hardware e infrastruttura);
- livello di calcolo;
- livello di conoscenza (algoritmi);
- livello di apprendimento;
- livello di rappresentazione;
- livello applicativo (interfaccia AI)

Tenendo conto che l'introduzione dell'intelligenza artificiale nei vari settori del mondo delle professioni e del lavoro non sarà soltanto l'utilizzo di nuove tecnologie o di nuovi strumenti che sicuramente miglioreranno e innoveranno il mondo delle organizzazioni, ma rappresenta una transizione epocale che cambierà il mondo produttivo e sociale. Per tale ragione in ambito europeo è stato introdotto il Regolamento UE 2024/1689 AI ACT, che, nell'Articolo 4, ha introdotto per le imprese, i professionisti e le pubbliche amministrazioni un importante obbligo di alfabetizzazione, volto ad assicurare che tutte le decisioni che riguardano la progettazione, l'implementazione ed il controllo dei sistemi di AI siano assunte da soggetti dotati delle competenze essenziali per comprenderne il funzionamento e i limiti.

Per poter rispondere a questa necessità da parte delle organizzazioni, e dei vari operatori dei sistemi di AI, ecco disponibile questo volume che riassume in maniera dettagliata e completa l'architettura dei sistemi di AI.

Concludo dicendo che ho letto il volume e l'ho apprezzato per la semplicità dell'approccio, tenendo conto della complessità e delle dimensioni degli argomenti affrontati sull'intelligenza artificiale. Ciò è stato reso possibile grazie alla notevole competenza dell'Autore, che ha saputo descrivere i vari argomenti di notevole complessità in maniera da renderli ben strutturati e comprensibili

Roberto Randazzo

Cyber | Security | Defence_Tecnologie e contesti della sicurezza informatica è una collana diretta da Paolo Capodanno e Massimo Montanile.

Ultimi volumi in collana

- #4 Paolo Capodanno, *Etica del mondo digitale* (in corso di pubblicazione)
- #5 Fabrizio Cirilli, *Essere auditor o fare audit? Una vita tra norme, docenze e audit ISO*
- #6 Fabrizio Cirilli, *Implementazione dei sistemi di gestione dalle basi alla certificazione. Progettazione e sviluppo di ISO/IEC 27001 e ISO/IEC 42001 passo dopo passo*
- #7 Massimo Montanile, *Dall'algoritmo al silicio: comprendere l'Intelligenza artificiale*